kaspersky

Kaspersky Security Center 15.1 Windows

目次

Kaspersky Security Center 15.1 のヘルプ

	**新機能** 最新の製品リリースの新機能を確認できます。		**ネットワーク保護の設定** 組織のセキュリティを管理する方法を確認できます。
	**システム要件** サポート対象のオペレーティングシステムとアプリケーションのバージョンを確認できます。		**カスペルスキー製品：定義データベースとソフトウェアモジュールのアップデート** 保護システムの信頼性を維持する方法を確認できます。
	**導入と初期セットアップ** リソースプランニング、管理サーバーのインストール、クライアントデバイスへのネットワークエージェントとセキュリティ製品のインストール、デバイスの管理グループへの統合について説明しています。		**監視とレポート** インフラストラクチャの状況、保護ステータス、統計情報の確認方法について説明しています。Cloud Discovery を使用してクラウドサービスへのアクセスを管理します。
	**ネットワーク接続されたデバイスの検出** 組織ネットワーク上の既存デバイスと新規デバイスの検出方法について説明しています。		**サードパーティのセキュリティ製品からの移行とアンインストールの実施** 競合するアプリケーションをアンインストールする方法を確認できます。
	**カスペルスキー製品：一元管理による導入** カスペルスキー製品の導入		**ディストリビューションポイントと接続ゲートウェイの調整** ディストリビューションポイントの設定方法を説明しています。
	**以前のバージョンの Kaspersky Security Center からのアップグレード** 以前のバージョンから Kaspersky Security Center 15.1 へのアップグレード方法を説明しています。		**導入と設定に関する推奨事項（オンラインヘルプのみ）** アプリケーションの導入、設定、および使用方法についての推奨事項を確認できます。また、アプリケーションの操作に関する一般的な問題を解決する方法についても説明しています。
	**カスペルスキー製品：ライセンスとアクティベーション** カスペルスキー製品を数ステップでアクティベートする方法を確認できます。		**サイジングガイド（オンラインヘルプのみ）** 様々な運用環境で最適なパフォーマンスを実現し維持するには、ネットワークに接続されたデバイスの数、ネットワークのトポロジー、必要な Kaspersky Security Center の機能を考慮する必要があります。
	**SIEM システムへのイベントのエクスポート** 分析のために、SIEM システムへのイベントのエクスポートを設定します。		**脆弱性とパッチ管理** サードパーティ製ソフトウェアの脆弱性を検知して修正する方法を確認できます。
	**クラウド環境での利用** クラウド環境の Amazon Web Services™、Microsoft Azure™、Google™ Cloud Platform で Kaspersky Security Center を導入します。		**よくある質問（英語のみ）** 一般的な問題を解決する方法について説明します。
	**Kaspersky Endpoint Security for Business クイックスタートガイド** Kaspersky Endpoint Security for Business の使用を開始するには、このソリューションをインストールして設定します。Kaspersky Security Center の機能比較を確認して、ネットワーク セキュリティを管理する最適な方法を選択することもできます。		

新機能

Kaspersky Security Center 15.1

Kaspersky Security Center 15.1 にはいくつかの新機能と機能強化が追加されています：

- Cloud Discovery。この機能を使用すると、Windows を実行している管理対象デバイスでのクラウドサービスの使用を監視し、不要と判断されるクラウドサービスへのアクセスをブロックできます。この機能は、Kaspersky Security Center Web コンソールでのみ使用できます。
- ドメインコントローラーポーリングにより、Linux ベースのディストリビューションポイントを介して Samba ドメインコントローラーをポーリングできるようになりました。大規模ドメインのポーリングをサポートするために、追加の改善が行われました。
- Linux ベースの管理対象デバイスのリモート診断を強化しました。
- macOS デバイスのハードウェアインベントリを拡張しました。macOS デバイス上のネットワークエージェントは、MAC アドレスとデバイスのシリアル番号を管理サーバーに送信します。
- SIEM システムへの接続を確認できるようになりました。
- 内部ユーザーのパスワードの最大長が 256 文字に引き上げられました。
- Kaspersky Security Center Windows から Kaspersky Security Center Linux に移行する場合、管理サーバーの証明書と秘密鍵をバックアップコピーから復元することで、管理対象デバイスを Kaspersky Security Center Linux の管理下に切り替えることができるようになりました。
- クリーナーツールまたは klmover ユーティリティを実行してパスワードで保護されたネットワークエージェントを削除すると、アンインストールパスワードの入力を要求されます。
- Kaspersky Security for Windows Server から Kaspersky Endpoint Security for Windows へのアップグレードにおいて、対象デバイスの再起動が不要になりました。
- Linux 上のクライアントデバイスにネットワークエージェントをインストールする際、またはインストール後に、ユーザーをデバイスの所有者として割り当てることができます。
- カスタムスクリプトを使用して管理対象デバイスにソフトウェアをインストールする時に、リモートインストールに関するレポートを受信できるようになりました。
- 管理対象デバイス上で複数のカスタムスクリプトを実行する場合、各スクリプトの優先順位を設定して実行順序を定義できます。スクリプトは、優先度が最も高いものから最も低いものの順に実行されます。
- 拡張ポリシー監査。ポリシーリビジョンの内容を表示し、ポリシーリビジョンをファイルに保存できるようになりました。現在、これらの機能は管理サーバーポリシーとネットワークエージェントポリシーでのみ使用できます。
- 以下を含むユーザーエクスペリエンスの向上：
  - Kaspersky Security Center Web コンソールのセクションをピン留めして、**ピン留め**セクションからすばやくアクセスできるように、メインメニューをカスタマイズできます。
  - テーブルでの作業を最適化しました。各テーブルの既定のビューには、最も頻繁に使用される列が含まれるようになりました。また、現在のページまたはテーブル全体のすべての項目を選択したり、テーブル全体の項目を並べ替えたりできるようになりました。

- レポート配信の設定が改善されました。レポートを送信する最大 20 個のメールアドレスとレポート配信スケジュールを指定できるようになりました。

- Linux ベースの管理対象デバイス上のアカウントからローカル管理者権限を取り消すことができます。これにより、ユーザーアカウントをさらに細かく制御できるようになります。たとえば、1 回限りの割り当ての完了後、ローカル管理者の権限を取り消すことができます。

- Linux ベースの管理対象デバイスでは、たとえば、ユーザーがローカルアカウントのパスワードを忘れた場合や、定期的なパスワードの変更を実行する場合に、ローカルアカウントのパスワードを変更できます。

- ［**ユーザー証明書の管理**］サブセクションでは、インストールするルート証明書を指定できます。これらの証明書は、たとえば、Web サイトまたは Web サーバーの信頼性を検証するために使用できます。

- ネットワーク攻撃のレポート、攻撃デバイスの MAC アドレスとポートが含まれるようになりました。

- 次回 Kaspersky Security Center Web コンソールにサインインしようとした時に、内部ユーザーにパスワードの変更を強制する新しいオプション。

- CEF または LEEF 形式でイベントを SIEM システムにエクスポートする時に、商用ライセンスがチェックされなくなりました。

- あるカスペルスキー製品から別のアプリケーションに移行する時に、現在のアプリケーションがパスワードで保護されている場合は、リモートインストールタスクでアンインストールパスワードを指定できるようになりました。

- Exchange ActiveSync はサポートされなくなりました。

Kaspersky Security Center 14.2

Kaspersky Security Center 14.2 にはいくつかの新機能と機能強化が追加されています：

- 新しいハードニングガイドがリリースされました。このガイドを注意深く読み、セキュリティに関する推奨事項に従って Kaspersky Security Center とネットワークインフラストラクチャを構成することを強く推奨します。

  また、Kaspersky Security Center の最新アップデートをインストールしてください。このアップデートには、ユーザーアカウントの二段階認証などのインフラストラクチャ保護機能が含まれています。

- カスペルスキーのサーバーへのアクセスが自動的に検証されるようになりました。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS を使用します。

- 仮想管理サーバーのユーザー権限を、プライマリ管理サーバーから独立していつでも設定できます。また、プライマリサーバーユーザーに仮想サーバーを管理する権限を割り当てることもできます。

- Kaspersky Security Center が、次の DBMS の使用をサポートするようになりました：

  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x（すべてのエディション）
  - Postgres Pro 14.x（すべてのエディション）
  - MariaDB 10.1、10.4、10.5

- Kaspersky Security Center Web コンソールを使用してファイルにポリシーとタスクをエクスポートしてから、ポリシーとタスクを Kaspersky Security Center Windows または Kaspersky Security Center Linux にインポートできます。

- ［**プロキシサーバーを使用しない**］が次のタスクから削除されました：

  - *管理サーバーのリポジトリへのアップデートのダウンロード*

  - *ディストリビューションポイントのリポジトリにアップデートをダウンロード*

- クラウド環境でクライアントデバイスを保護するために、Kaspersky Security for Windows Server の代わりに Kaspersky Endpoint Security for Windows を導入できます。この機能は、Kaspersky Endpoint Security 12.0 for Windows のリリース後に使用できるようになりました。

- 暗号化鍵の操作は、［**一般的な機能**］：［**暗号化キーの管理**］機能領域のアクセス権によって制限されるようになりました。Kaspersky Security Center のユーザーは、**読み取り**権限がある場合は暗号化鍵をエクスポートでき、**書き込み**権限がある場合は暗号化鍵をインポートできるようになりました。

Kaspersky Security Center 14

Kaspersky Security Center 14 にはいくつかの新機能と機能強化が追加されています：

- 分離されたネットワーク内のサードパーティ製ソフトウェア（Microsoft 製ソフトウェアを除く）のアップデートをインストールして脆弱性を修正できます。このネットワークには管理サーバーと、インターネット接続のない管理対象デバイスが含まれます。この種類のネットワークの脆弱性を修正するには、インターネットアクセスが可能な管理サーバーを使用して必要なアップデートをダウンロードし、分離された管理サーバーにパッチを転送する必要があります。

- モバイルユーザー用の接続プロファイルが、macOS デバイスに追加されました。接続プロファイルを使用すると、macOS デバイスのネットワークエージェントのルールを設定し、同一または異なる管理サーバー（デバイスの位置により異なる）へ接続できます。

- ネットワークエージェントが、Microsoft Windows 10 IoT Enterprise のデバイスへインストールできるようになりました。

- **脅威レポート**の設定で、脅威のリストをフィルタリングし、Cloud Sandbox で検知された脅威のみを表示することが可能になりました。

- Kaspersky Security Center が Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 を管理対象アプリケーションとしてサポートするようになりました。

Kaspersky Security Center Web コンソールにはいくつかの新機能と機能強化が追加されています：

- ［ダッシュボードのみモード］は、ネットワークを管理してはいないが、Kaspersky Security Center でネットワークの保護ステータスを表示する必要がある社員（幹部社員など）に対して設定することができます。ユーザーがこのモードを有効にすると、事前設定されたウィジェットのあるダッシュボードのみが表示されます。このように、すべての管理対象デバイスの保護ステータスや、最近検知された脅威数、またはネットワーク内で頻繁に検知される脅威など、ウィジェットで指定された統計情報を管理できます。

- Kaspersky Security Center Web コンソールがセキュリティ製品として Kaspersky Security for iOS をサポートするようになりました。

- タスクのプロパティで、サブグループおよびセカンダリ管理サーバー（仮想サーバーを含む）にタスクを適用するかどうかを指定できるようになりました。

- Kaspersky Security Center が Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 を管理対象アプリケーションとしてサポートするようになりました。

Kaspersky Security Center 13.2

Kaspersky Security Center 13.2 にはいくつかの新機能と機能強化が追加されています：

- 管理サーバー、管理コンソール、Kaspersky Security Center 13.2 Web コンソールおよびネットワークエージェントを次の新しいオペレーティングシステムにインストールすることができます（詳細については、ソフトウェア要件を参照してください）：
  - Microsoft Windows 11
  - Microsoft Windows 10 21H2（October 2021 Update）
  - Windows Server 2022
- MySQL 8.0 を定義データベースとして使用できます。
- カスペルスキーのフェールオーバークラスターに Kaspersky Security Center を導入し、Kaspersky Security Center の高可用性を実現できます。
- Kaspersky Security Center は IPv4 アドレスと同様に IPv6 アドレスでも動作するようになりました。管理サーバーが IPv6 アドレスのデバイスを持つネットワークを検索できるようになりました。

Kaspersky Security Center 13.2 Web コンソールにはいくつかの新機能と機能強化が追加されています：

- Kaspersky Security Center 13.2 Web コンソールを介して Android を実行しているモバイルデバイスを管理できるようになりました。
- 「マーケットプレイス」が新しいメニューセクションとして使用可能になりました。Kaspersky Security Center 13.2 Web コンソールを使用してカスペルスキー製品を検索できます。
- Kaspersky Security Center は次のカスペルスキー製品をサポートするようになりました：
  - Kaspersky Endpoint Detection and Response Optimum 2.0
  - Kaspersky Sandbox 2.0
  - Kaspersky Industrial CyberSecurity for Networks 3.1

Kaspersky Security Center 13.1

Kaspersky Security Center 13.1 にはいくつかの新機能と機能強化が追加されています：

- SIEM システムとの連携が強化されました。暗号化チャネル（TLS）を使用して、イベントを SIEM システムへエクスポートできるようになりました。この機能は Kaspersky Security Center Web コンソールおよび MMC ベースの管理コンソールで使用できます。
- 管理サーバーでパッチを配布パッケージの形式で受信できるようになりました。パッケージは、今後のバージョンで将来使用することも可能です。
- Kaspersky Endpoint Detection and Response Optimum 用の新規セクション［**Alerts**］が、Kaspersky Security Center 13.1 Web コンソールに追加されました。Kaspersky Endpoint Detection and Response

Optimum が検知する脅威に対する操作で使用する、いくつかの新規ウィジェットも追加されました。

- Kaspersky Security Center 13.1 Web コンソールを使用して、カスペルスキー製品ライセンスの有効期間の終了に関する通知を受信できるようになりました。
- Kaspersky Security Center 13.1 Web コンソールの応答時間が短縮されました。

Kaspersky Security Center 13

Kaspersky Security Center 13 Web コンソールでは、次の機能が追加されています：

- 二段階認証を実装しました。Kaspersky Security Center 13 Web コンソールへの不正なアクセスのリスクを減少させる二段階認証を有効にすることができます。
- NTLM および Kerberos プロトコルを使用したドメイン認証を実装しました（シングルサインオン）。シングルサインオン機能を使用することで、Windows のユーザーは企業のネットワークのパスワードを再入力することなく Kaspersky Security Center 13 Web コンソールで安全な認証を有効にできます。
- Kaspersky Managed Detection and Response で使用するプラグインを設定できるようになりました。これは、インシデントの表示やワークステーションの管理に使用できます。
- 管理サーバーのインストールウィザードで Kaspersky Security Center 13 Web コンソールの設定を指定できるようになりました。
- アップデートやパッチの新しいリリースに関する通知が表示されます。アップデートをすぐにインストールすることも、後でインストールすることもできます。Kaspersky Security Center 13 Web コンソールを介して管理サーバーのパッチをインストールすることができるようになりました。
- 表での作業時に、順番や列の幅を指定したりデータを並べ替えたり、ページサイズを指定したりできるようになりました。
- 名前をクリックしてレポートを開けるようになりました。
- 韓国語で Kaspersky Security Center 13 Web コンソールが利用できるようになりました。
- ［**監視とレポート**］メニューで、カスペルスキーからの通知が新しいセクションとして使用できるようになりました。このセクションには、Kaspersky Security Center のバージョンと、管理対象デバイスにインストールされている管理対象アプリケーションに関連する情報が提供されます。このセクションの情報は、古い通知を削除し、新しい情報を追加することで定期的に更新されます。通知が不要であれば、カスペルスキーからの通知を無効にすることができます。
- ユーザーアカウントの設定を変更した後に追加の認証を実装しました。不正な変更からのユーザーアカウントの保護を有効にすることができます。このオプションが有効になっていると、ユーザーアカウントの編集にはユーザー認証が要求されます。

Kaspersky Security Center 13 で追加された機能は次の通りです：

- 二段階認証を実装しました。管理コンソールへの不正なアクセスのリスクを減少させる二段階認証を有効にすることができます。このオプションをオンにすると、ユーザーアカウントの編集にはユーザー認証が要求されます。KES デバイスの二段階認証を有効または無効に設定できるようになりました。
- HTTP を通して管理サーバーにメッセージを送ることができます。管理サーバーの OpenAPI を使用するための Python ライブラリとリファレンスガイドが利用できるようになりました。
- iOS MDM サーバー証明書の有効期限が切れた後、管理対象 iOS デバイスへのシームレスな切り替えを可能とするために、iOS MDM プロファイルで使用する予備証明書を発行できます。

- マルチテナンシーアプリケーションフォルダーは管理サーバーに表示されなくなりました。

Kaspersky Security Center の概要

このセクションでは、Kaspersky Security Center の目的、主な機能と構成要素、および Kaspersky Security Center の購入方法について説明します。

オンラインヘルプに含まれる情報は、製品に付属するドキュメントに記載されている情報と異なっている場合があります。その場合は、最新の情報はオンラインヘルプの情報です。製品のインターフェイスのリンクをクリックするか、付属ドキュメント内のオンラインヘルプへのリンクをクリックして、オンラインヘルプに移動することができます。オンラインヘルプは、事前の通知なしに更新されることがあります。必要に応じて、オンラインヘルプとオフラインヘルプを切り替えることができます。

Kaspersky Security Center は、組織のネットワークの基本的な管理と保守の一元化を目的として設計されています。組織のネットワークセキュリティのレベルに関する詳細情報にアクセスし、カスペルスキー製品を使用して構築された保護システムのすべてのコンポーネントを設定できます。

Kaspersky Security Center は、組織内でデバイスの保護を担当する企業ネットワーク管理者および従業員を対象としています。

Kaspersky Security Center を使用して、次のことが実現できます：

- 管理サーバーの階層を作成して、組織内、リモートオフィス内、クライアント組織内のネットワークを管理する。

  *クライアント組織*とは、サービスプロバイダーからアンチウイルスによる保護の提供を受ける組織です。

- 管理グループの階層を作成して、いくつかのクライアントデバイスを1つの単位として管理する。
- カスペルスキー製品をベースに構築されたアンチウイルスによる保護システムを管理する。
- オペレーティングシステムのイメージを作成し、ネットワーク経由でクライアントデバイスに導入する。また、カスペルスキー製品や他社のソフトウェア製品をリモートインストールする。
- クライアントデバイスにインストールされたカスペルスキー製品または他社のソフトウェアをリモート管理する（アップデートのインストール、脆弱性の検知および修正など）。
- カスペルスキー製品のライセンスをクライアントデバイスへ一元的に配信し、使用状況を監視したり、ライセンスを更新したりする。
- アプリケーションやデバイスの動作に関する統計情報とレポートを受信する。
- カスペルスキー製品の動作中に発生した緊急イベントに関する通知を受信する。
- モバイルデバイスを管理する。
- デバイスのハードディスクやリムーバブルドライブに保存された情報を暗号化したり、暗号化されたデータへのユーザーのアクセスを管理したりする。
- 組織のネットワークに接続されたハードウェアのインベントリを作成する。
- セキュリティ製品により隔離またはバックアップに移動されたファイルや、セキュリティ製品による処理が延期されたファイルを一元管理する。

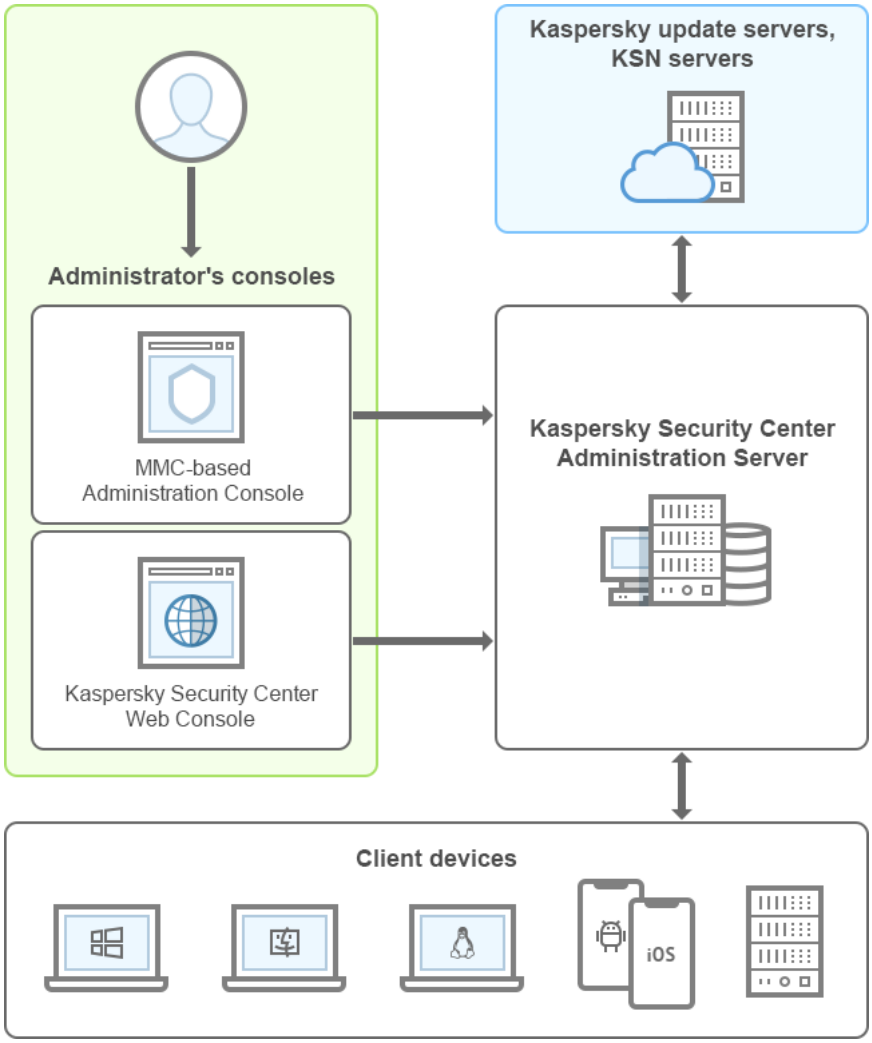
Kaspersky Security Center は、カスペルスキー（例：https://www.kaspersky.co.jp）またはパートナー会社を通じて購入することができます。

カスペルスキーから Kaspersky Security Center を購入した場合は、当社のウェブサイトからアプリケーションをコピーすることができます。アプリケーションのアクティベーションに必要な情報は、支払い手続き完了後にメールで送信されます。

アップデート機能（ウイルス対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

アーキテクチャ

このセクションでは、Kaspersky Security Center のコンポーネントとコンポーネント間の連携について説明します。



Kaspersky Security Center のコンポーネント構成

Kaspersky Security Center は主に次のコンポーネントで構成されています：

- *管理コンソール*（以降「*コンソール*」とも表記）：管理サーバーとネットワークエージェントの管理サービスに対し、ユーザーインターフェイスを提供します。管理コンソールは、Microsoft Management Console（MMC）のスナップインとして実装されます。管理コンソールを使用すると、管理サーバーにインターネット経由でリモート接続できます。

- *Kaspersky Security Center Web コンソール*：Kaspersky Security Center により管理されているクライアント組織のネットワークの保護システムの構築や管理が可能な Web インターフェイスです。

- *Kaspersky Security Center 管理サーバー*（以降「*サーバー*」とも表記）：組織のネットワークにインストールされているアプリケーションおよびその管理方法に関する情報を一元的に保管します。
- *カスペルスキーのアップデートサーバー*：カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。
- *KSN サーバー*：ファイル、Web リソース、ソフトウェアの評価情報が定期的に更新されるカスペルスキーのデータベースを格納するサーバー。KSN を使用することで、カスペルスキー製品がより迅速に新しい脅威に対応します。また、一部の保護コンポーネントのパフォーマンスが向上し、誤検知の可能性が減ります。
- *クライアントデバイス*：Kaspersky Security Center によって保護されているクライアント企業のデバイス。保護する必要がある各デバイスには、カスペルスキーのセキュリティ製品のいずれかがインストールされている必要があります。

システム要件

- 管理サーバーの要件
- Web コンソールの要件
- モバイルサーバーの要件
- 管理コンソールの要件
- ネットワークエージェントの要件

管理サーバーの要件

ハードウェアの最小要件：

- CPU：動作周波数が 1 GHz 以上（64 ビット OS の場合、最小周波数は 1.4 GHz）
- メモリ：4 GB
- 使用可能なディスク容量：10 GB（脆弱性対策とパッチ管理を使用する場合は、100 GB 以上のディスク空き容量が使用可能である必要があります）

クラウド環境での導入の場合、管理サーバーとデータベースサーバーの要件は、物理管理サーバーの要件と同じです（管理するデバイスの数によって異なります）。

ソフトウェア要件：

- Microsoft Data Access Components（MDAC）2.8
- Microsoft Windows® DAC 6.0
- Microsoft Windows Installer 4.5

次のオペレーティングシステムがサポートされています：

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64 ビット
- Windows Server 2016 Standard/Datacenter/Essentials/Server Core（インストールオプション）（LTSB）64 ビット
- Microsoft Windows Server 2019 標準/データセンター/コア 64 ビット
- Microsoft Windows Server 2022 標準/データセンター/コア 64 ビット
- Windows Storage Server 2019 64 ビット

次の仮想化プラットフォームがサポートされています：

- VMware vSphere 6.7
- VMware vSphere 7.0
- Microsoft Hyper-V Server 2019 64 ビット
- Microsoft Hyper-V Server 2022 64 ビット
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x

以下のデータベースサーバーがサポートされます（異なるデバイスにインストール可能）：

- Microsoft SQL Server 2016（すべてのエディション）64 ビット
- Microsoft SQL Server 2017（すべてのエディション）（Windows/Linux 上で実行）64 ビット
- Microsoft SQL Server 2019（すべてのエディション）（Windows/Linux 上で実行）64 ビット（追加の操作が必要）
- Microsoft SQL Server 2022（すべてのエディション）（Windows/Linux 上で実行）64 ビット
- MySQL 5.7 コミュニティ 32 ビット/64 ビット MySQL 8.0 コミュニティ 32 ビット/64 ビット
- MariaDB 10.5（ビルド 10.5.27 以降）32 ビット / 64 ビット
- MariaDB Galera Cluster 10.3 32 ビット / 64 ビット（InnoDB ストレージエンジンを使用）
- PostgreSQL 13.x 64 ビット
- PostgreSQL 14.x 64 ビット
- PostgreSQL 15.x 64 ビット
- Postgres Pro 13.x Windows/Linux 64 ビット
- Postgres Pro 14.x Windows/Linux 64 ビット

詳細と制限事項については、「DBMS の選択」のトピックを参照してください。

SIEM およびその他の情報管理システム：

- HP（Micro Focus）ArcSight ESM 7.0
- IBM QRadar 7.3
- Splunk 7.1

Web コンソールの要件

Kaspersky Security Center Web コンソールサーバー

ハードウェアの最小要件：

- CPU：4 コア、動作周波数が 2.5 GHz
- メモリ：8 GB
- 使用可能なディスク容量：40 GB

管理サーバー証明書の最低要件：

- 証明書署名アルゴリズム SHA-2
- 鍵の長さ 2048 以上

証明書を再発行する必要がある場合は、Kaspersky Security Center ナレッジベースを参照してください。

Kaspersky Security Center Web コンソールサーバーがサポートするオペレーティングシステム

オペレーティングシステム：下記の Microsoft Windows 製品（64 ビット版のみ）	Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials/Server Core Windows Server 2016 Standard/Datacenter/Essentials/Server Core（インストールオプション）（LTSB） Windows Server 2019 Standard/Datacenter/Core Windows Server 2022 Standard/Datacenter/Core Windows Storage Server 2019
仮想化プラットフォーム	VMware vSphere 6.7 VMware vSphere 7.0 Citrix XenServer 7.1 LTSR Citrix XenServer 8.x Parallels Desktop 18 Oracle VM VirtualBox 7.x

クライアントデバイス

クライアントデバイス側で Kaspersky Security Center Web コンソールを使用するために必要なのはブラウザーのみです。

最小画面解像度は 1366x768 ピクセルです。

デバイスのハードウェアおよびソフトウェア要件は、Kaspersky Security Center Web コンソールの操作で使用するブラウザーと同じです。

ブラウザー：

- Google Chrome 128.0.6613.120 以降
- Microsoft Edge 128.0.2739.67 以降
- macOS 上の Safari 17.6
- 「Yandex」ブラウザー 24.7.3.1081 以降
- Mozilla Firefox 延長サポートリリース 115.14.0 以降

モバイルサーバーの要件

iOS モバイルデバイス管理（iOS MDM）サーバー

ハードウェア要件：

- CPU：動作周波数が 1 GHz 以上（64 ビット OS の場合、最小周波数は 1.4 GHz）
- メモリ：2 GB
- 使用可能なディスク容量：2 GB

ソフトウェア要件：Microsoft Windows（サポートされるオペレーティングシステムのバージョンは、管理サーバーの要件によって決まります）

管理コンソールの要件

ハードウェア要件：

- CPU：動作周波数が 1 GHz 以上（64 ビット OS の場合、最小周波数は 1.4 GHz）
- メモリ：512 MB
- 使用可能なディスク容量：1 GB

ソフトウェア要件：

- Microsoft Windows オペレーティングシステム（サポートされるオペレーティングシステムのバージョンは、管理サーバーの要件によって決まります）：
  - Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials 64 ビット
  - Windows Server 2016 Standard/Datacenter/Essentials（LTSB）64 ビット
  - Windows Server 2019 Standard/Datacenter 64 ビット

- Windows Server 2022 Standard/Datacenter 64 ビット
- Windows Storage Server 2019 64 ビット

- Microsoft 管理コンソール 2.0
- Microsoft Windows Installer 4.5
- 次の OS で実行している Microsoft Internet Explorer 11.0：
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows ストレージサーバー 2019
- Microsoft Edge（Microsoft Windows サーバーで実行）2022 Standard

ネットワークエージェントの要件

ハードウェアの最小要件：

- CPU：動作周波数が 1 GHz 以上（64 ビット OS の場合、最小周波数は 1.4 GHz）
- メモリ：512 MB
- 使用可能なディスク容量：1 GB

Linux ベースのデバイスのソフトウェア要件：Perl 言語インタープリターのバージョン 5.10 以降をインストールする必要があります。

ネットワークエージェントがサポートするオペレーティングシステム

オペレーティングシステム： Microsoft Windows	Windows Embedded POSReady 2009（最新の Service Pack）32 ビット Windows Embedded 7 Standard（Service Pack 1）32 ビット / 64 ビット Windows Embedded 8.1 Industry Pro 32 ビット / 64 ビット Windows 10 Enterprise 2015 LTSB 32 ビット / 64 ビット Windows 10 Enterprise 2016 LTSB 32 ビット / 64 ビット Windows 10 IoT Enterprise 2015 LTSB 32 ビット / 64 ビット Windows 10 IoT Enterprise 2016 LTSB 32 ビット / 64 ビット Windows 10 Enterprise 2019 LTSC 32 ビット / 64 ビット Windows 10 IoT Enterprise バージョン 1703 32 ビット / 64 ビット Windows 10 IoT Enterprise バージョン 1709 32 ビット / 64 ビット Windows 10 IoT Enterprise バージョン 1803 32 ビット / 64 ビット Windows 10 IoT Enterprise バージョン 1809 32 ビット / 64 ビット Windows 10 20H2 IoT Enterprise 32 ビット / 64 ビット Windows 10 21H2 IoT Enterprise 32 ビット / 64 ビット Windows 10 IoT Enterprise 32 ビット / 64 ビット Windows 10 IoT Enterprise バージョン 1909 32 ビット / 64 ビット Windows 10 IoT Enterprise LTSC 2021 32 ビット / 64 ビット Windows 10 IoT Enterprise バージョン 1607 32 ビット / 64 ビット Windows 10 TH1 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット / 64 ビット

	Windows 10 TH2 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット / 64 ビット Windows 10 RS1 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット / 64 ビット Windows 10 RS2 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット / 64 ビット Windows 10 RS3 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット Windows 10 RS4 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット Windows 10 RS5 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット Windows 10 RS6 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット Windows 10 19H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット Windows 10 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット Windows 10 20H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット Windows 10 20H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット Windows 10 21H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット Windows 10 21H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット Windows 10 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 ビット/64 ビット Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64 ビット Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 ビット Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 ビット Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 ビット Windows 8 Pro/Enterprise 32 ビット / 64 ビット Windows 8.1 Pro/Enterprise 32 ビット / 64 ビット Windows 7 Home/Pro/Enterprise/Ultimate（Service Pack 1）32 ビット / 64 ビット Microsoft Windows XP Professional（Service Pack 2）32 ビット / 64 ビット（ネットワークエージェントのバージョン 10.5.1781 のみ対応） Windows XP Professional Service Pack 3 以降 32 ビット（ネットワークエージェントバージョン 14.0.0.20023 でサポート） Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32 ビット（ネットワークエージェントバージョン 14.0.0.20023 でサポート） Windows MultiPoint Server 2011 Standard / Premium 64 ビット Windows Server 2008 Standard/Enterprise/Datacenter/Foundation（Service Pack 2）32 ビット / 64 ビット Windows Server 2008 R2 Standard /Datacenter/Enterprise/Foundation/with Service Pack 1 以降 64 ビット Windows Server 2012 Standard/Datacenter/Essentials/Foundation/Server Core 64 ビット Windows Server 2012 Standard/Datacenter/Essentials/Foundation/Server Core 64 ビット Windows Server 2016 Standard/Datacenter/Essentials/Server Core（インストールオプション）（LTSB）64 ビット Windows Server 2019 Standard/Datacenter/Core 64 ビット Windows Server 2019 RS5 Standard/Essentials 64 ビット Windows Server 2022 Standard/Datacenter/Core 64 ビット Windows Server 2022 21H2 Standard/Datacenter 64 ビット Windows Storage Server 2019 64 ビット
オペレーティングシステム：Linux	Debian GNU / Linux 10.x（Buster）32 ビット / 64 ビット Debian GNU/Linux 11.x（Bullseye）32 ビット / 64 ビット Debian GNU/Linux 12（Bookworm）32 ビット/64 ビット Ubuntu Server 18.04 LTS（Bionic Beaver）64 ビット Ubuntu Server 20.04 LTS（Focal Fossa）64 ビット Ubuntu Server 22.04 LTS（Jammy Jellyfish）64 ビット Ubuntu Server 22.04 LTS ARM 64 ビット Ubuntu Server 24.04 LTS (Noble Numbat) 64 ビット CentOS 6.7 以降 32 ビット CentOS 6.x（6.6 まで）32 ビット / 64 ビット CentOS 7.x 64 ビット CentOS ストリーム 8 64 ビット CentOS ストリーム 9 64 ビット CentOS ストリーム 9 ARM 64 ビット Red Hat Enterprise Linux Server 6.x 32 ビット / 64 ビット Red Hat Enterprise Linux Server 7.x 64 ビット

Red Hat Enterprise Linux Server 8.x 64 ビット
Red Hat Enterprise Linux Server 9.x 64 ビット
SUSE Linux Enterprise Server 12（すべての Service Pack）64 ビット
SUSE Linux Enterprise Server 15（すべての Service Pack）64 ビット
SUSE Linux Enterprise Server 15（すべての Service Pack）ARM 64 ビット
openSUSE 15 64 ビット
EulerOS 2.0 SP10 64 ビット
EulerOS 2.0 SP10 ARM 64 ビット
Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.5）64 ビット
Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.6）64 ビット
Astra Linux Special Edition RUSB.10015-16（リリース 1、運用アップデート 1.6）64 ビット
Astra Linux Special Edition RUSB.10015-17（運用アップデート 1.7.3）64 ビット
Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.7）64 ビット
Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.8）64 ビット
Astra Linux Special Edition RUSB.10015-37（運用アップデート 7.7）64 ビット
Astra Linux Special Edition RUSB.10152-02（運用アップデート 4.7）ARM 64 ビット
Astra Linux Common Edition（運用アップデート 2.12）64 ビット
ALT Workstation 10.1 64 ビット
ALT Server 10.1 64 ビット
ALT Education 10.1 64 ビット
ALT SP Server 10 32 ビット / 64 ビット
ALT SP Server 10 ARM 64 ビット
ALT SP Workstation 10 32 ビット / 64 ビット
ALT SP Workstation 10 ARM 64 ビット
ALT Server 10 64 ビット
ALT Server 10 ARM 64 ビット
ALT Workstation 10 32 ビット / 64 ビット
ALT 8 SP Workstation (8.4) ARM 64 ビット
ALT 8 SP Server (8.4) ARM 64 ビット
ALT 8 SP Server（LKNV.11100-01）32 ビット / 64 ビット
ALT 8 SP Server（LKNV.11100-02）32 ビット / 64 ビット
ALT 8 SP Server（LKNV.11100-03）32 ビット / 64 ビット
ALT 8 SP Workstation（LKNV.11100-01）32 ビット / 64 ビット
ALT 8 SP Workstation（LKNV.11100-02）32 ビット / 64 ビット
ALT 8 SP Workstation（LKNV.11100-03）32 ビット / 64 ビット
Mageia 4 32 ビット
Oracle Linux 7 64 ビット
Oracle Linux 8 64 ビット
Oracle Linux 9 64 ビット
Linux Mint 20.x 64 ビット
Linux Mint 21.1 以降 64 ビット
AlterOS 7.5 以降 64 ビット
GosLinux IC6/7.17 64 ビット
GosLinux IC6/7.2 64 ビット
SberOS 3.3.1 64 ビット
Platform V SberLinux OS Server (SLO) 8.8 64 ビット
Platform V SberLinux OS Server (SLO) 8.9.2 64 ビット
RED OS 7.3 ARM 64 ビット
RED OS 7.3 Server 64 ビット
RED OS 7.3 Certified Edition 64 ビット
RED OS 8 Certified Edition 64 ビット
ROSA Enterprise Linux Server 7.9 64 ビット
ROSA Enterprise Linux Desktop 7.9 64 ビット
ROSA COBALT 7.9 64 ビット
ROSA CHROME 12 64 ビット
AlmaLinux 8 以降 64 ビット

	AlmaLinux 9 以降 64 ビット Rocky Linux 8 以降 64 ビット Rocky Linux 9 以降 64 ビット Atlant、Alcyone ビルド、バージョン 2022.02 64 ビット MSVSPHERE 9.2 SERVER 64 ビット MSVSPHERE 9.2 ARM 64 ビット SynthesisM Server 8.6 64 ビット SynthesisM Client 8.6 64 ビット OSnova 2.10 64 ビット Kylin 10 64 ビット EMIAS 1.0 64 ビット Amazon Linux 2 64 ビット MosOS 15.4 Arbat 64 ビット M OS (Moscow Electronic School) 64 ビット
オペレーティングシステム：macOS	macOS Monterey（12.x） macOS Ventura（13.x） macOS Sonoma（14.x）

ネットワークエージェントが、Intel に加えて、Apple シリコン（M1）アーキテクチャをサポートするようになりました。

次の仮想化プラットフォームがサポートされています：

- VMware vSphere 6.7
- VMware vSphere 7.0
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- カーネルベースの仮想マシン（ネットワークエージェントによってサポートされるすべての Linux オペレーティングシステム）

Windows 10 RS4 または Windows 10 RS5 を使用しているデバイスでは、大文字と小文字の区別が有効になっているフォルダーにおいて、一部の脆弱性を Kaspersky Security Center が検知できない可能性があります。

Windows 7、Windows Server 2008、または Windows Server 2008 R2 を実行しているデバイスにネットワークエージェントをインストールする前に、OS Windows 用セキュリティアップデートプログラム KB3063858（Windows 7 用セキュリティアップデートプログラム (KB3063858)、Windows 7 for x64-Based Systems 用セキュリティアップデートプログラム (KB3063858)、Windows Server 2008 用セキュリティアップデートプログラム (KB3063858)、Windows Server 2008 x64 Edition 用セキュリティアップデートプログラム (KB3063858)、Windows Server 2008 R2 x64 Edition 用セキュリティアップデートプログラム (KB3063858)）がインストールされていることを確認してください。

Microsoft Windows XP では、ネットワークエージェントの一部の機能が正常に動作しない可能性があります。

Windows XP 向けのネットワークエージェントは、Microsoft Windows XP でのみインストールまたはアップデートが可能です。Microsoft Windows XP のサポートされているエディションとそれに対応するネットワークエージェントのバージョンは、上記のサポートされているオペレーティングシステムのリストに記載されています。このページから、Microsoft Windows XP に必要なバージョンのネットワークエージェントをダウンロードできます。

Kaspersky Security Center と同じバージョンの Linux 用ネットワークエージェントをインストールすることを推奨します。

Kaspersky Security Center は、同じまたはそれ以降のバージョンのネットワークエージェントを完全にサポートします。

macOS 用ネットワークエージェントは、このオペレーティングシステム用のカスペルスキーのセキュリティ製品と一緒に提供されます。

互換性のあるカスペルスキーのアプリケーションとソリューション

Kaspersky Security Center は、現在サポートされているすべてのカスペルスキー製品とソリューションの一元的な導入、管理をサポートします。以下の表に、MMC ベースの管理コンソールおよび Kaspersky Security Center Web コンソールがサポートするカスペルスキー製品とソリューションを記載しています。製品とソリューションのバージョンを調べるには、製品のサポートライフサイクルページを参照してください。

Kaspersky Security Center がサポートするカスペルスキー製品とソリューションのリスト

カスペルスキー製品またはソリューションの名前	MMC ベースの管理コンソールのサポート対象	Kaspersky Security Center Web コンソールのサポート対象
ワークステーション向け製品		
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Kaspersky Endpoint Security for Linux ARM64 Edition	✓	✓
Kaspersky Endpoint Security for Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security for Windows	✓	✓
Kaspersky Embedded Systems Security for Linux	–	✓
産業用ソリューション向け		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Networks（一元的な導入はサポート対象外です）	✓	✓
モバイルデバイス向け製品		

Kaspersky Endpoint Security for Android	✓	✓
Kaspersky Security for iOS	–	✓
ファイルサーバー向け製品		
Kaspersky Security for Windows Server	✓	✓
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
仮想環境向け		
Kaspersky Security for Virtualization Light Agent	✓	✓
Kaspersky Security for Virtualization Agentless	✓	–
メールおよびコラボレーションサーバー向け		
Kaspersky Security for Microsoft Exchange Servers	✓	–
標的型攻撃を検知するサービス		
Kaspersky Sandbox サーバー	–	✓
Kaspersky Endpoint Detection and Response Optimum	–	✓
Kaspersky Managed Detection and Response	–	✓
KasperskyOS デバイス向け製品		
Kaspersky IoT Secure Gateway	–	✓
KasperskyOS Thin Client	–	✓
評判定義データベース		
Kaspersky Private Security Network	–	✓

Kaspersky Security Center 15.1 の機能のライセンス

Kaspersky Security Center では、いくつかの機能にライセンスが必要です。

次の表は、各ライセンスがカバーする Kaspersky Security Center 機能を示しています。

Kaspersky Security Center の機能を有効にするには、管理サーバーのライセンスを追加して管理サーバーをアクティベートする必要があります。

各管理サーバーにライセンスを手動で追加する必要があります。

ライセンスと Kaspersky Security Center 機能

Kaspersky Security Center の機能	Kaspersky Vulnerability and Patch Management	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security for Business	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise	Kaspersky EDR Optimum
脆弱性の評価	✓	✓	✓	✓	✓	✓	✓
パッチ管理	✓	–	✓	✓	–	✓	✓
ロールベースのアクセス制御	✓	✓	✓	✓	✓	✓	✓
オペレーティングシステムとアプリケーションのインストール	✓	–	✓	✓	–	✓	✓

モバイルデバイス管理（ユーザーの iOS および Android デバイスの管理）	✓	✓	✓	✓	–	–	✓
AWS、Microsoft Azure、Google Cloud などのクラウド環境で作業するためのクラウド環境の設定	–	–	–	–	✓	✓	–
SIEM システムへのイベントのエクスポート：Syslog	✓	✓	✓	✓	✓	✓	✓
SIEM システムへのイベントのエクスポート：IBM の QRadar および Micro Focus の ArcSight	✓	–	✓	✓	–	✓	✓

Kaspersky Security Center のコンポーネントの互換性について

以下の表に、Kaspersky Security Center コンポーネントの互換性に関する情報が記載されています。

Kaspersky Security Center のコンポーネントの互換性

コンポーネント	互換性あり
Kaspersky Security Center 15.1 管理サーバー	• Kaspersky Security Center 15.1 管理サーバー • Kaspersky Security Center 15.1 Web コンソール。 Kaspersky Security Center 管理サーバーと Kaspersky Security Center Web コンソールの両方の最新バージョンを使用することを推奨します。そうしないと、Kaspersky Security Center の機能が制限される可能性があります。Kaspersky Security Center 管理サーバーと Kaspersky Security Center Web コンソールは個別にインストールおよびアップグレードすることができます。この場合、インストールされている Kaspersky Security Center Web コンソールが接続先の管理サーバーのバージョンと互換性があることを確認する必要があります。 • Kaspersky Security Center ネットワークエージェントのバージョン：15.1、15、14.2、14。
Kaspersky Security Center 15.1 Web コンソール	Kaspersky Security Center 管理サーバーのバージョン：15.1 および 14.2。 Kaspersky Security Center 管理サーバーと Kaspersky Security Center Web コンソールの両方の最新バージョンを使用することを推奨します。そうしないと、Kaspersky Security Center の機能が制限される可能性があります。Kaspersky Security Center 管理サーバーと Kaspersky Security Center Web コンソールは個別にインストールおよびアップグレードすることができます。この場合、インストールされている Kaspersky Security Center Web コンソールが接続先の管理サーバーのバージョンと互換性があることを確認する必要があります。 最新バージョンの Kaspersky Security Center Web コンソールと以前のバージョンの Kaspersky Security Center を使用している場合、ドメイン認証中にエラーが発生すると、エラーテキストに既定のメッセージが含まれます。
Kaspersky Security Center 15.1 プライマリ管理サーバー	セカンダリ管理サーバー： • Kaspersky Security Center 14 Windows • Kaspersky Security Center 14.2 Windows • Kaspersky Security Center 15.1 Windows • Kaspersky Security Center 14.2 Linux • Kaspersky Security Center 15 Linux • Kaspersky Security Center 15.1 Linux

Kaspersky Security Center 15.1 セカンダリ管理サーバー	プライマリ管理サーバー： • Kaspersky Security Center 14 Windows • Kaspersky Security Center 14.2 Windows • Kaspersky Security Center 15.1 Windows • Kaspersky Security Center 14.2 Linux • Kaspersky Security Center 15 Linux • Kaspersky Security Center 15.1 Linux

Kaspersky Security Center の比較：Windows ベースと Linux ベース

カスペルスキーは、Windows と Linux の 2 つのプラットフォームのオンプレミスのソリューションとして Kaspersky Security Center を提供しています。Windows ベースのソリューションでは、Windows デバイスに管理サーバーをインストールし、Linux ベースのソリューションには Linux にインストールされるよう設計されたバージョンの管理サーバーをインストールします。このオンラインヘルプには、Kaspersky Security Center Windows に関する情報が含まれています。Linux ベースのソリューションの詳細については、Kaspersky Security Center Linux オンライン ヘルプを参照してください。

以下の表で Windows ベースのソリューションと Linux ベースのソリューションの Kaspersky Security Center の主要な機能を比較します。

Windows ベースのソリューションと Linux ベースのソリューションとして動作する Kaspersky Security Center の機能比較

機能またはプロパティ	Kaspersky Security Center 15.1	
	Windows ベースのソリューション	Linux ベースのソリューション
管理サーバーの位置	オンプレミス	オンプレミス
データベース管理システム（DBMS）の位置	オンプレミス	オンプレミス
管理サーバーをインストールするオペレーティングシステム	Windows	Linux
管理コンソールの種別	オンプレミスおよび Web ベース	Web ベース
Web ベースの管理コンソールをインストールするオペレーティングシステム	Windows または Linux	Linux
管理サーバーの階層構造	✓	✓
管理グループの階層	✓	✓
ネットワークポーリング	✓	✓ （IP 範囲、ドメインコントローラー、Samba 4 Active Directory、Microsoft Active Directory による）
管理対象デバイスの最大数	100000	20000
Windows、macOS、Linux 管理対象デバイスの保護	✓	✓ （Linux および Windows デバイスの保護のみ）
モバイルデバイスの保護	✓	—
仮想マシンの保護	✓	—
パブリッククラウドインフラストラクチャの保護	✓	—
デバイスベースのセキュリティ管理	✓	✓
ユーザーベースのセキュリティ管理	✓	✓

製品ポリシー	✓	✓
カスペルスキー製品のタスク	✓	✓
Kaspersky Security Network	✓	✓
KSN プロキシ	✓	✓
Kaspersky Private Security Network	✓	✓
カスペルスキー製品のライセンスの一元的な配信	✓	✓
定義データベースの自動アップデート	✓	✓
仮想管理サーバーのサポート	✓	✓
サードパーティ製ソフトウェアのアップデートのインストールと脆弱性の修正	✓	– （リモートインストールタスクの使用のみ）
管理対象デバイスのイベントに関する通知	✓	✓
ユーザーアカウントの作成と管理	✓	✓
ドメイン認証を使用してコンソールにサインインする	✓	✓ （シングルサインオンはサポートされていません）
SIEM システムとの統合	✓	✓ （Syslog の使用によってのみ）
ポリシーとタスクのステータスの監視	✓	✓
Kaspersky Security Center のフェールオーバークラスターの導入	✓	✓
Windows Server のフェールオーバークラスターへの管理サーバーのインストール	✓	–
SNMP を使用した管理サーバーの統計情報のサードパーティ製品への送信	✓	–
クライアントデバイスのリモート診断	✓	✓
クライアントデバイスのデスクトップへのリモート接続	✓	–
オブジェクトリビジョンの管理	✓	–
カスペルスキー製品の自動アップデート	✓	–
クライアントデバイスへのオペレーティングシステムの導入	✓	–
インストールパッケージおよびその他のファイルを公開するための Web サーバー	✓	–
Kaspersky Endpoint Detection and Response Optimum によって検知されたアラートの表示と操作	✓	–
管理サーバーの WSUS サーバーとしての使用	✓	–
Kaspersky Managed Detection and Response との統合	✓	–
アダプティブアノマリーコントロールのサポート	✓	–
管理グループのクラスターとサーバーアレイのサポート	✓	✓
サードパーティライセンスの管理	✓	–

Kaspersky Security Center Cloud コンソールの概要

Kaspersky Security Center をオンプレミスのアプリケーションとして使用することは、管理サーバーを含む Kaspersky Security Center をローカルデバイスにインストールし、ネットワークのセキュリティシステムをマイクロソフト管理コンソールベースの管理コンソール（Kaspersky Security Center Windows でのみ使用可能）、または Kaspersky Security Center Web コンソールで管理することを意味します。

その場合でも、Kaspersky Security Center をクラウドサービスとして使用することは可能です。この場合、Kaspersky Security Center がクラウド環境にインストール、維持されており、管理サーバーへのアクセスがサービスとして提供されます。ネットワークのセキュリティシステムをクラウドベースの管理コンソール（Kaspersky Security Center Cloud コンソール）で管理します。このコンソールのインターフェイスは、Kaspersky Security Center Web コンソールと同じです。

Kaspersky Security Center Cloud コンソールのインターフェイスとヘルプは、次の言語版で提供されています：

- 英語
- フランス語
- ドイツ語
- イタリア語
- 日本語
- ポルトガル語（ブラジル）
- ロシア語
- 簡体字中国語
- スペイン語
- スペイン語（中南米）
- 繁体字中国語

Kaspersky Security Center Cloud コンソールとその機能の詳細は、Kaspersky Security Center Cloud コンソールのヘルプ、Kaspersky Endpoint Security for Business のヘルプを参照してください。

Kaspersky Security Center 15.1

このセクションでは、Kaspersky Security Center 15.1 の使用方法について説明します。

オンラインヘルプに含まれる情報は、製品に付属するドキュメントに記載されている情報と異なっている場合があります。その場合は、最新の情報はオンラインヘルプの情報です。製品のインターフェイスのリンクをクリックするか、付属ドキュメント内のオンラインヘルプへのリンクをクリックして、オンラインヘルプに移動することができます。オンラインヘルプは、事前の通知なしに更新されることがあります。必要に応じて、オンラインヘルプとオフラインヘルプを切り替えることができます。

基本概念

このセクションでは、Kaspersky Security Center の基本概念について説明します。

管理サーバー

Kaspersky Security Center のコンポーネントを使用すると、クライアントデバイスにインストールされたカスペルスキー製品をリモート管理できます。

管理サーバーがインストールされたデバイスは、*管理サーバー*（「*サーバー*」とも表記）と呼ばれます。管理サーバーについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

管理サーバーは、次の属性を持つサービスとしてデバイスにインストールされます：

- 名称は「Kaspersky Security Center 管理サーバー」
- オペレーティングシステムの起動時に自動実行される
- **ローカルシステム**アカウントまたは管理サーバーのインストール時に選択したユーザーアカウントを使用する

管理サーバーは、次の機能を実行します：

- 管理グループ構造の保管
- クライアントデバイスの設定に関する情報の保管
- アプリケーション配布パッケージのリポジトリの管理
- クライアントデバイスへのアプリケーションのリモートインストールおよびアプリケーションの削除
- カスペルスキー製品の定義データベースおよびソフトウェアモジュールのアップデート
- クライアントデバイスのポリシーとタスクの管理
- クライアントデバイスで発生したイベントに関する情報の保管
- カスペルスキー製品の操作に関するレポートの生成

- クライアントデバイスへのライセンスの配信と、ライセンスに関する情報の保管
- （クライアントデバイスでのウイルスの検知など）タスクの進捗に関する通知の転送

製品のインターフェイスで管理サーバーに名前を付ける

MMC ベースの管理コンソールと Kaspersky Security Center Web コンソールの製品インターフェイスで、管理サーバーに次の名前をつけることが可能です：

- 「*device_name*」または「管理サーバー：*device_name*」などの管理サーバーデバイスの名前。
- 「*IP_address*」または「管理サーバー：*IP_address*」などの管理サーバーの IP アドレス。
- セカンダリ管理サーバーおよび仮想管理サーバーには、これらをプライマリ管理サーバーに接続する際に指定したカスタム名を使用できます。
- Linux デバイスにインストールした Kaspersky Security Center Web コンソールを使用している場合は、本製品は応答ファイルで信頼済みとして指定した管理サーバーの名前を表示します。

管理コンソールまたは Kaspersky Security Center Web コンソールを使用して管理サーバーに接続できます。

管理サーバーの階層構造

管理サーバーは、階層に配置できます。各管理サーバーは、階層の同一ネスト上に複数のセカンダリ管理サーバー（「*セカンダリサーバー*」とも表記）を保持することも、複数のネストレベル上に複数のサーバーを保持することもできます。セカンダリ管理サーバーのネストレベルに制限はありません。プライマリ管理サーバーの管理グループには、すべてのセカンダリ管理サーバーのクライアントデバイスが含められます。このようにして、ネットワークの独立したセクションを、様々な管理サーバーを使用して管理できます。管理サーバーの管理には、プライマリ管理サーバーが使用されます。

*仮想管理サーバー*はセカンダリ管理サーバーの特殊な例です。

管理サーバーの階層を使用して、次のことを実現できます：

- （ネットワーク全体で1台の管理サーバーがインストールされている場合と比較して）管理サーバーの負荷を軽減する。
- イントラネットのトラフィックを削減して、リモートオフィスとの通信を簡略化する。プライマリ管理サーバーとネットワーク上のすべてのデバイス（他の地域にあるデバイスも含む）との間で接続を確立する必要はありません。各ネットワークセグメントにセカンダリ管理サーバーをインストールし、セカンダリ管理サーバーの管理グループ内にデバイスを配置し、高速通信チャネルを使用してセカンダリ管理サーバーとプライマリ管理サーバー間の接続を確立すれば十分です。
- アンチウイルスセキュリティ管理者間で、責任区分を明確にする。企業ネットワーク内のアンチウイルスセキュリティステータスの一元管理機能と監視機能も利用できます。
- サービスプロバイダーが Kaspersky Security Center を使用する。サービスプロバイダーでインストールする必要があるのは、Kaspersky Security Center と Kaspersky Security Center Web コンソールのみです。サービスプロバイダーが様々な組織の多くのデバイスを管理するには、管理サーバーの階層に仮想管理サーバーを追加します。

管理グループの階層に含まれる各デバイスは、1台の管理サーバーにしか接続できません。デバイスから管理サーバーへの接続を個別に監視する必要があります。ネットワーク属性に基づいて様々な管理サーバーの管理グループ内でデバイスを検索する機能を使用してください。

仮想管理サーバー

仮想管理サーバー（「*仮想サーバー*」とも表記）は、クライアント組織のネットワークの保護を管理する、Kaspersky Security Center のコンポーネントです。

仮想管理サーバーは特殊なセカンダリ管理サーバーであり、物理管理サーバーと比較すると、次の制限があります：

- 仮想管理サーバーは、プライマリ管理サーバー上にのみ作成できます。
- 仮想管理サーバーは、プライマリ管理サーバーのデータベースを使用します。仮想管理サーバーではデータのバックアップと復元タスク、およびアップデートのスキャンとダウンロードタスクはサポートされていません。
- 仮想サーバーでは、セカンダリ管理サーバー（仮想サーバーを含む）の作成がサポートされていません。

さらに、仮想管理サーバーには次の制限があります：

- 仮想管理サーバーのプロパティウィンドウでは、セクション数が限られています。
- 仮想管理サーバーが管理するクライアントデバイスにカスペルスキー製品をリモートからインストールするには、仮想管理サーバーと通信するためにネットワークエージェントがインストールされたクライアントデバイスが必要です。そのデバイスは、最初に仮想管理サーバーと接続する際、自動的にディストリビューションポイントとして設定され、その他のクライアントデバイスと仮想管理サーバーを接続するゲートウェイとして機能します。
- 仮想サーバーでネットワークをポーリングするためには、ディストリビューションポイントを使用する必要があります。
- 正常に動作しない仮想サーバーが Kaspersky Security Center によって再起動される場合、プライマリ管理サーバーとすべての仮想サーバーが再起動されます。
- 仮想サーバー上で作成されたユーザーには、管理サーバー上のロールを割り当てることはできません。

仮想管理サーバーの管理者は、その仮想管理サーバーにおけるすべての権限を持ちます。

モバイルデバイスサーバー

*モバイルデバイスサーバー*は、Kaspersky Security Center のコンポーネントの1つです。このコンポーネントにより、管理コンソールからモバイルデバイスにアクセスし、モバイルデバイスを管理できます。モバイルデバイスサーバーは、モバイルデバイスについての情報を受け取り、そのプロファイルを保存します。

Kaspersky Security Center には、モバイルデバイスサーバーとして iOS MDM サーバーが含まれています。このモバイルデバイスサーバーは、APNs（Apple® Push Notification Service）をサポートするモバイルデバイスの管理に使用します。

Kaspersky Security Center のモバイルデバイスサーバーでは、次のデバイスを管理します：

- 個々のモバイルデバイス。
- 複数のモバイルデバイス。
- サーバーのクラスターに同時接続されている複数のモバイルデバイス。サーバーのクラスターに接続すると、このクラスターにインストールされているモバイルデバイスサーバーが管理コンソールに1台のサーバーとして表示されます。

Web サーバー

Kaspersky Security Center *Web* サーバー（略称として単に「*Web* サーバー」とも表記）は、管理サーバーとともにインストールされる Kaspersky Security Center のコンポーネントです。Web サーバーは、スタンドアロンインストールパッケージ、iOS MDM プロファイル、および共有フォルダーのファイルをネットワーク上で伝送できるように設計されています。

スタンドアロンインストールパッケージは作成時に、Web サーバー上に自動的に公開されます。スタンドアロンパッケージをダウンロードするリンクは、作成済みスタンドアロンインストールパッケージのリストに表示されます。必要に応じて、スタンドアロンパッケージの公開を取り消したり、Web サーバー上にスタンドアロンパッケージを再度公開したりできます。

ユーザーのモバイルデバイス用の iOS MDM プロファイルも、作成時に Web サーバー上に自動的に公開されます。公開中のプロファイルは、ユーザーのモバイルデバイスに正常にインストールされるとすぐに、自動的に Web サーバーから削除されます。

共有フォルダーは、管理サーバーで管理されるデバイスを使用するすべてのユーザーが利用できる情報の保管領域として使用されます。共有フォルダーに直接アクセスできないユーザーには、Web サーバーを使用して、そのフォルダーから情報を提供することができます。

Web サーバーを使用して共有フォルダーからユーザーに情報を提供するには、管理者が共有フォルダー内に public という名前のサブフォルダーを作成し、情報をそのサブフォルダーに貼り付ける必要があります。

情報転送リンクの構文は次の通りです：

`https://<Web サーバー名>:<HTTPS ポート>/public/<オブジェクト>`

説明：

- `<Web サーバー名>` は、Kaspersky Security Center Web サーバーの名前です。
- `<HTTPS ポート>` は、管理者が定義した Web サーバーの HTTPS ポートです。HTTPS ポートは、管理サーバーのプロパティウィンドウの［**Web サーバー**］セクションで設定できます。既定のポート番号は 8061 です。
- `<オブジェクト>` は、ユーザーがアクセス権を持っているサブフォルダーまたはファイルです。

管理者は、メールなど便利な方法を利用して、ユーザーに新しいリンクを送信します。

ユーザーは、そのリンクを使用して、必要な情報をローカルデバイスにダウンロードできます。

ネットワークエージェント

管理サーバーとデバイスとの対話は、Kaspersky Security Center のコンポーネントの*ネットワークエージェント*によって実行されます。ネットワークエージェントは、Kaspersky Security Center を使用してカスペルスキー製品を管理するすべてのデバイスにインストールします。

ネットワークエージェントは、次の属性を持つサービスとしてデバイスにインストールされます：

- 名称は「Kaspersky Security Center ネットワークエージェント」
- オペレーティングシステムの起動時に自動実行される
- ローカルシステムアカウントを使用する

ネットワークエージェントがインストールされたデバイスは「*管理対象デバイス*」または単に「*デバイス*」と呼ばれます。

ネットワークエージェントは Windows デバイス、Linux デバイス、Mac デバイスにインストールできます。このコンポーネントは、次のいずれかのソースから取得できます：

- 管理サーバーの保管領域のインストールパッケージ（管理サーバーをインストールしている必要があります）
- カスペルスキーの Web サーバーにあるインストールパッケージ

管理サーバーをインストールしているデバイスでは、サーバーバージョンのネットワークエージェントが管理サーバーとともに自動的にインストールされるので、手動でネットワークエージェントをインストールする必要はありません。

ネットワークエージェントを起動するプロセスの名前は「*klnagent.exe*」です。

ネットワークエージェントによって管理対象デバイスと管理サーバーが同期します。*同期*間隔（「ハートビート」とも表記）を管理対象 10,000 台につき 15 分に設定することを推奨します。

管理グループ

管理グループ（以後、*グループ*と表記）は、基準に従ってまとめられた管理対象デバイスの仮想グループで、グループ内のデバイスを Kaspersky Security Center 内で 1 つの単位として管理することを目的としています。

管理グループ内の管理対象デバイスはすべて、次の操作を実行できるように設定されます：

- 同一のアプリケーション設定を使用する（設定はグループポリシーで定義できます）。
- 特定の設定でグループタスクを作成することにより、すべてのアプリケーションで共通の動作モードを使用する。グループタスクの例としては、共通のインストールパッケージの作成とインストール、定義データベースおよびモジュールのアップデート、デバイスのオンデマンドスキャン、リアルタイム保護の有効化などがあります。

1 台の管理対象デバイスが所属できる管理グループは 1 つだけです。

管理サーバーとグループに対して、任意の階層レベル数で階層構造を作成できます。1 つの階層レベルに、セカンダリ管理サーバーや仮想管理サーバー、グループ、および管理対象デバイスを含めることができます。デバイスの物理的な位置を動かすことなく、あるグループから別のグループへデバイスを移動できます。たとえば、従業員の配属が経理から開発に異動になった場合、この従業員のコンピューターを経理部門用の管理グループから開発部門用の管理グループに移動できます。これにより、コンピューターでは開発部門向けのセキュリティ製品設定が自動的に取得されます。

管理対象デバイス

管理対象デバイスとは、ネットワークエージェントがインストールされたコンピューターデバイス（Windows、Linux、macOS）およびカスペルスキー製品がインストールされたモバイルデバイスです。これらのデバイスにインストールされたセキュリティ製品のタスクとポリシーを作成することで、これらのデバイスを管理できます。管理対象デバイスからのレポートも受信できます。

モバイルデバイス以外の管理対象デバイスを、ディストリビューションポイントや接続ゲートウェイとして動作させることができます。

1台のデバイスを管理対象にできる管理サーバーは1台のみです。1台の管理サーバーで、モバイルデバイスを含めて最大100,000台のデバイスを管理できます。

未割り当てデバイス

*未割り当てデバイス*とは、ネットワークに接続されているがどの管理グループにも含まれていないデバイスです。未割り当てデバイスに対して、管理グループへ移動したり、アプリケーションをインストールしたりなどの操作を実行できます。

ネットワーク内で検出された新しいデバイスは、「**未割り当てデバイス**」管理グループに割り当てられます。検出されたデバイスが自動的に他のグループに移動されるようにルールを設定できます。

管理コンピューター

*管理者用ワークステーション*は、管理コンソールがインストールされたデバイス、またはKaspersky Security Center Webコンソールを管理者が開くために使用するデバイスです。管理者は、これらのデバイスを使用して、クライアントデバイスにインストールされているすべてのカスペルスキー製品を一元的にリモート管理できます。

管理コンソールがデバイスにインストールされると、アイコンが表示され、ここから管理コンソールを起動できるようになります。アイコンは［**スタート**］→［**プログラム**］→［**Kaspersky Security Center**］メニューにあります。

管理コンピューターの数に制限はありません。任意の管理コンピューターから、ネットワーク上にある複数の管理サーバーで構成される管理グループを一度に管理できます。管理コンピューターは、任意の階層レベルにある管理サーバー（物理または仮想）に接続できます。

管理コンピューターは、管理グループにクライアントデバイスとして含めることができます。

任意の管理サーバーの管理グループ内で、1台のデバイスが管理サーバーのクライアント、管理サーバー、または管理コンピューターとして機能できます。

管理プラグイン

カスペルスキー製品は、*管理プラグイン*と呼ばれる専用コンポーネントを使用して、管理コンソールから管理できます。Kaspersky Security Centerで管理できるカスペルスキー製品には、管理プラグインが含まれています。

アプリケーション管理プラグインを使用すると、管理コンソールで次の処理を行うことができます：

- アプリケーションポリシーおよび設定の作成と編集、およびアプリケーションタスクの設定
- アプリケーションタスク、動作中に発生するイベント、およびクライアントデバイスから受信するアプリケーション動作の統計データに関する情報の取得

管理プラグインは、カスペルスキーのテクニカルサポートサイトからダウンロードできます。

Web 管理プラグイン

Kaspersky Security Center Web コンソールによるカスペルスキー製品のリモート管理では、*Web 管理プラグイン*という特別なコンポーネントが使用されます。以降、Web 管理プラグインは*管理プラグイン*とも表記されます。管理プラグインは、Kaspersky Security Center Web コンソールと特定のカスペルスキー製品との間のインターフェイスです。管理プラグインを使用して、該当製品のタスクとポリシーを設定できます。

管理 Web プラグインは、カスペルスキーのテクニカルサポートサイトからダウンロードできます。

管理プラグインには次の機能があります：

- カスペルスキーのタスクを作成および編集し、各種設定を編集するインターフェイス
- カスペルスキー製品と管理対象デバイスのリモートからの一元管理に使用できるポリシーおよびポリシーのプロファイルを作成および編集するインターフェイス
- カスペルスキー製品で生成されたイベントの転送
- Kaspersky Security Center Web コンソールでは、転送されたカスペルスキー製品の動作データ、イベント、および統計情報を表示できます

ポリシー

*ポリシー*とは、管理グループとそのサブグループに適用される一連のカスペルスキー製品の設定です。管理グループのデバイスに複数のカスペルスキー製品をインストールできます。Kaspersky Security Center は、管理グループ内のカスペルスキー製品ごとに1つのポリシーを提供します。ポリシーには、次のいずれかのステータスがあります（以下の表を参照）。

ポリシーのステータス

ステータス	説明
アクティブ	現在デバイスに適用されているポリシー。各管理グループ内のカスペルスキー製品に対してアクティブにできるポリシーは1つだけです。デバイスは、カスペルスキー製品のアクティブポリシーの設定値を適用します。
非アクティブ	現在デバイスに適用されていないポリシー。
モバイルユーザー	このオプションをオンにすると、デバイスが企業ネットワークから離れるとポリシーがアクティブになります。

ポリシーは、次のルールに従って機能します：

- 1つのアプリケーションに対して、異なる値を持つ複数のポリシーを定義することができます。
- 現在のアプリケーションに対してアクティブにできるポリシーは1つだけです。

- 特定のイベントが発生した時に、非アクティブポリシーを有効化できます。たとえば、ウイルスアウトブレイク中に、より厳格なアンチウイルスによる保護設定を適用することができます。

- ポリシーには子ポリシーを設定できます。

一般には、ウイルス攻撃などの緊急事態への備えとしてポリシーを使用できます。たとえば、フラッシュドライブを介した攻撃が発生した場合は、フラッシュドライブへのアクセスをブロックするポリシーを有効化できます。この場合、現在アクティブなポリシーは自動的に非アクティブになります。

異なる状況で複数の設定の変更のみが想定される場合などで、複数のポリシーを管理することを防ぐために、ポリシープロファイルを使用できます。

*ポリシープロファイル*とは、ポリシーの設定値の代わりに使用される、指定されたポリシー設定値のサブセットです。ポリシープロファイルは、管理対象デバイスでの有効な設定の形成に影響を与えます。*有効な設定*とは、デバイスに現在適用されている一連のポリシー設定、ポリシープロファイル設定、およびローカルアプリケーション設定です。

ポリシープロファイルは、次のルールに従って機能します：

- ポリシープロファイルは、特定の有効化条件下で有効になります。

- ポリシープロファイルには、ポリシー設定とは異なる設定値が含まれます。

- ポリシープロファイルを有効化すると、管理対象デバイスの有効な設定が変更されます。

- 1つのポリシーに最大100個のポリシープロファイルを含めることができます。

ポリシーのプロファイル

別々の管理グループに対応して単一のポリシーから枝分かれした複数のポリシーの作成が必要になる場合があります。また、これらの枝分かれ後のポリシーについても、一元的に設定の変更を行えると便利です。枝分かれ後のポリシー同士では、1つか2つの設定値が異なるだけという場合もあります。たとえば、経理部門の従業員には単一のポリシーが適用されるが、部門内の管理職にはフラッシュドライブの使用が許可され、その他のメンバーには許可されないという点が異なる場合などです。こうした状況では、管理グループの階層のみを使用して適切なポリシーを適用することはそれほど簡単ではありません。

単一のポリシーから枝分かれした複数のポリシーを個別に作成しなくても、Kaspersky Security Centerでは*ポリシーのプロファイル*を作成して対応できます。ポリシーのプロファイルは、同じ管理グループ内にあるデバイスを異なるポリシー設定に従って動作させる場合に必要です。

ポリシーのプロファイルには、ポリシー設定のサブセットが指定されています。このサブセットはポリシーとともに対象デバイスに配信され、*プロファイルの有効化条件*と呼ばれる特定の条件下でポリシーを補完する機能を果たします。プロファイルに含まれるのは、管理対象デバイスでアクティブな「基本」ポリシーとは異なる設定（差分）のみです。プロファイルを有効にすると、元々デバイスで有効になっていた「基本」ポリシーの設定が修正されます。修正後の設定では、プロファイルで指定された値が適用されます。

タスク

Kaspersky Security Centerは、様々な*タスク*を作成して実行することにより、デバイス上にインストールされたカスペルスキー製品を管理します。アプリケーションのインストール、起動、停止、ファイルのスキャン、定義データベースやソフトウェアモジュールのアップデート、アプリケーションでのその他のタスクを実行するには、タスクが必要です。

アプリケーションのタスクを作成できるのは、そのアプリケーション用の管理プラグインがインストールされている場合に限られます。

タスクは管理サーバー上とデバイス上で実行できます。

次のタスクは管理サーバーで実行されます：

- レポートの自動配信
- 管理サーバーのリポジトリへのアップデートのダウンロード
- 管理サーバーデータのバックアップ
- データベースのメンテナンス
- Windows Update の同期の実行
- 基準となるデバイスの OS イメージに基づいたインストールパッケージの作成

次の種別のタスクはデバイスで実行されます：

- *ローカルタスク* - 特定の 1 台のデバイスで実行されるタスク

  ローカルタスクを変更するには、管理者が管理コンソールツールを使用するか、またはリモートデバイスのユーザーが実行します（たとえば、セキュリティ製品のインターフェイスを使用）。管理対象デバイスの管理者とユーザーが同時にローカルタスクを変更する場合、管理者が行う変更内容の方が優先度が高いため有効になります。

- *グループタスク* - 特定のグループに属するすべてのデバイスで実行されるタスク

  タスクのプロパティで特別な設定を行わない限り、グループタスクは選択したグループのすべてのサブグループに影響します。さらに、グループタスクは該当するグループまたはそのサブグループのいずれかに導入されている、セカンダリおよび仮想管理サーバーに接続されているデバイスにも適用されます（オプション設定による）。

- *グローバルタスク* - 管理グループに含まれるかどうかに関係なく、特定のデバイスで実行されるタスク

アプリケーションごとに、任意の数のグループタスク、グローバルタスク、ローカルタスクを作成できます。

タスクの設定に変更を加え、タスクの進行状況を表示し、タスクをコピー、エクスポート、インポート、および削除できます。

タスクは、そのタスクを作成した対象のアプリケーションが実行中である場合のみ、デバイス上で開始されます。

タスクの実行結果は、管理サーバー上の Microsoft Windows のイベントログと Kaspersky Security Center のイベントログに一元的に保存されます。また、各デバイスのローカルにも保存されます。

タスクの設定には個人データを使用しないでください。たとえば、ドメイン管理者パスワードを指定することは避けてください。

タスク範囲

*タスク*の*範囲*とは、タスクが実行されるデバイスの範囲です対象範囲には次の種別があります：

- *ローカルタスク*の対象範囲は、そのデバイス自体です。
- *管理サーバータスク*の対象範囲は、管理サーバーです。
- *グループタスク*の対象範囲は、グループに含まれているデバイスのリストです。

*グローバルタスク*の作成時に、次の方法を使用して対象範囲を指定できます：

- 特定のデバイスを手動で指定する

  デバイスのアドレスとして、IP アドレス（または IP アドレス範囲）、NetBIOS 名または DNS 名を使用できます。

- 追加するデバイスのアドレスが記載されている TXT ファイルからデバイスのリストをインポートする（各アドレスを独立した行に記載する必要があります）。

  デバイスのリストをファイルからインポートするかまたはリストを手動で作成し、デバイスが名前によって識別される場合、リストに含めることができるのはその情報が管理サーバーのデータベースに登録済みであるデバイスのみです。データベースへの情報の入力は、デバイスの接続時、またはデバイスの検索中に実行されます。

- デバイスの抽出を指定する。

  時間の経過とともに、抽出に含まれるデバイスセットの変更に応じてタスクの範囲が変化します。デバイスの抽出は、デバイスにインストールされているソフトウェアを含むデバイス属性、およびデバイスに割り当てられているタグに基づいて作成できます。デバイスの抽出は、タスクの範囲を定義するための最も柔軟性の高い方法です。

  デバイスの抽出を対象とするタスクは常に、管理サーバーのスケジュールに基づいて実行されます。このタスクは、管理サーバーと接続されていないデバイスでは実行できません。他の方法でタスク範囲が指定されたタスクはデバイス上で直接実行されるため、デバイスと管理サーバーとの接続の有無には左右されません。

  デバイスの抽出を対象とするタスクは、デバイスのローカル時間ではなく管理サーバーのローカル時間に基づいて実行されます。他の方法でタスク範囲が指定されたタスクはデバイスのローカル時間に基づいて実行されます。

ローカルアプリケーション設定とポリシーの関連付け

ポリシーを使用して、グループ内のすべてのデバイスに同じ値のアプリケーション設定を指定できます。

ローカルアプリケーション設定を使用して、ポリシーで指定されている設定値をグループ内の個別のデバイスに再定義できます。設定値を指定できるのは、ポリシーで変更が許可されている設定（ロック解除された設定）だけです。

クライアントデバイスのアプリケーションで使用される値は、その設定がポリシー内でロックされているかどうか（🔒）に基づいて決定されます：

- 設定の変更がロックされている場合、ポリシー内で定義されている値が、すべてのクライアントデバイスで使用される。

- 設定の変更がロック解除されている場合、各クライアントデバイスのアプリケーションは、ポリシーで指定されている値ではなくローカル設定の値を使用する。設定は、ローカルアプリケーション設定で変更できます。

このため、クライアントデバイスでタスクを実行する場合、次の 2 つの方法で定義した設定が使用されます：

- タスク設定とローカルアプリケーション設定（ポリシー内の設定の変更がロックされていない場合）。
- グループポリシー（設定の変更がロックされている場合）。

ローカルアプリケーション設定は、最初にポリシー設定に基づいてポリシーが適用された後で適用されます。

ディストリビューションポイント

ディストリビューションポイント（旧称：アップデートエージェント）とは、ネットワークエージェントがインストールされ、アップデートの配信やアプリケーションのリモートインストール、ネットワーク内のデバイスの情報の収集に使用されるデバイスです。ディストリビューションポイントは、次の機能を実行できます：

- 管理サーバーから受信したアップデートおよびインストールパッケージをグループ内のクライアントデバイスに配布します（UDP を使用したマルチキャストを含む）。アップデートは、管理サーバーまたはカスペルスキーのアップデートサーバーから受信可能です。後者の場合は、ディストリビューションポイントの[アップデートタスクを作成する必要があります](#)。

  macOS を実行しているディストリビューションポイントデバイスでは、カスペルスキーのアップデートサーバーからアップデートをダウンロードできません。

  > *ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクの対象範囲に macOS を実行しているデバイスが 1 台以上含まれている場合、すべての Windows デバイスでタスクが正常に完了した場合でも、タスクには「*失敗*」ステータスが付与されます。

  ディストリビューションポイントにより、アップデートの配信が加速され、管理サーバーのリソースが解放されます。

- UDP を使用して、マルチキャストによってポリシーとグループタスクを配信します。
- [管理グループのデバイス](#)に対して、管理サーバーとの接続のゲートウェイとして動作します。

  グループ内の管理対象デバイスと管理サーバーとの間で直接接続を確立できない場合は、このグループの管理サーバーへの接続ゲートウェイとしてディストリビューションポイントを使用できます。この場合、管理対象デバイスは接続ゲートウェイに接続され、接続ゲートウェイが管理サーバーに接続されます。

  接続ゲートウェイとして動作するディストリビューションポイントを使用することで、管理対象デバイスと管理サーバーとの間の直接接続がブロックされることはありません。接続ゲートウェイは使用できないが、管理サーバーとの直接接続が技術的に可能な場合は、管理対象デバイスは管理サーバーに直接接続されます。

- 新しいデバイスを検出したり既存のデバイスの情報を更新するために、ネットワークを検索します。ディストリビューションポイントは管理サーバーと同じ方法でデバイスを検出できます。
- ディストリビューションポイントのオペレーティングシステムのツールを使用して、サードパーティ製ソフトウェアとカスペルスキー製品のリモートインストールを実行します。ディストリビューションポイントは、ネットワークエージェントなしにクライアントデバイスへのインストールを実行できます。

  この機能により、管理サーバーが直接アクセスできないネットワークに配置されているクライアントデバイスに、ネットワークエージェントのインストールパッケージをリモートで転送できます。

- Kaspersky Security Network（KSN）に参加したプロキシサーバーとして動作します。

  ディストリビューションポイントで KSN プロキシサーバーを有効にして、デバイスを KSN プロキシサーバーとして動作させることができます。この場合、KSN プロキシサービス（ksnproxy）はデバイス上で実行されます。

管理サーバーからディストリビューションポイントへのファイル転送は、HTTP で、または SSL 接続が有効な場合は HTTPS で実行されます。HTTP または HTTPS を使用すると、トラフィック量が削減され、SOAP と比較して速度が速くなります。

ネットワークエージェントをインストールしたデバイスは、管理者が手動で、または管理サーバーから自動で、ディストリビューションポイントに割り当てることができます。指定された管理グループのディストリビューションポイントの完全なリストは、ディストリビューションポイントのリストのレポートに表示されます。

ディストリビューションポイントの範囲は、管理者により割り当てられている管理グループ、および、埋め込みのすべてのレベルのサブグループです。複数のディストリビューションポイントが管理グループの階層に割り当てられている場合、管理対象デバイスのネットワークエージェントが、階層内の最も近いディストリビューションポイントに接続します。

ネットワークの場所は、ディストリビューションポイントの範囲にすることもできます。ネットワークの場所は、ディストリビューションポイントがアップデートを配信するデバイスのセットを手動で作成する場合に使用されます。ネットワークの場所は、Windows オペレーティングシステムが実行されているデバイスの場合にのみ判別できます。

管理サーバーによってディストリビューションポイントが自動的に割り当てられた場合、管理グループではなくブロードキャストドメインによって割り当てられます。これは、すべてのブロードキャストドメインが管理サーバーで認識済みである場合に発生します。ネットワークエージェントは同じサブネットに存在する他のネットワークエージェントとメッセージを交換し、得た情報を管理サーバーに送信します。管理サーバーはその情報をネットワークエージェントのブロードキャストドメインでのグループ化に利用します。管理グループ内のネットワークエージェントの 70% 以上を検索した後にブロードキャストドメインが管理サーバーに認識されます。管理サーバーはブロードキャストドメインを 2 時間ごとに検索します。ディストリビューションポイントは、ブロードキャストドメイン別に割り当てられた後、管理グループ別に再度割り当てることはできません。

管理者がディストリビューションポイントを手動で割り当てる場合、管理グループまたはネットワークロケーションに割り当てることができます。

アクティブな接続プロファイルを持つネットワークエージェントは、ブロードキャストドメインの検知の対象外となります。

Kaspersky Security Center では、各ネットワークエージェントに対して、他のどのアドレスとも異なる一意の IP マルチキャストアドレスを割り当てます。これにより、IP の重複によって発生するネットワークの過負荷を回避できます。

2 つ以上のディストリビューションポイントを単一のネットワークエリアまたは単一の管理グループに割り当てると、それらの 1 つがアクティブなディストリビューションポイントとなり、残りがスタンバイディストリビューションポイントとなります。アクティブなディストリビューションポイントはアップデートとインストールパッケージを直接管理サーバーからダウンロードします。一方、スタンバイのディストリビューションポイントはアクティブなディストリビューションポイントからのみアップデートを受信します。この場合、ファイルは管理サーバーから一度ダウンロードされてからディストリビューションポイント間で配信されます。アクティブなディストリビューションポイントが何かの理由で利用不可能になった場合、スタンバイのディストリビューションポイントがアクティブになります。管理サーバーは自動的にディストリビューションポイントをスタンバイとして割り当てます。

ディストリビューションポイントのステータス（「*アクティブ*」または「*スタンバイ*」）とチェックボックスが、klnagchk のレポートに表示されます。

ディストリビューションポイントには、少なくとも 4 GB の空きディスク容量が必要です。ディストリビューションポイントのディスクの空き容量が 2 GB 未満の場合、Kaspersky Security Center は*警告*の重要度でセキュリティ上の問題を作成します。セキュリティの問題は、デバイスのプロパティの**セキュリティ問題**セションで公開されます。

ディストリビューションポイントとして割り当てられているデバイスでリモートインストールタスクを実行するには、追加の空きディスク容量が必要です。空きディスク容量はインストールするすべてのインストールパッケージの合計サイズを上回っていなければなりません。

ディストリビューションポイントとして割り当てられているデバイスでアップデート（パッチ適用）タスクと脆弱性の修正タスクを実行するには、追加の空きディスク容量が必要です。空きディスク容量は、インストールするすべてのパッチの合計サイズの少なくとも 2 倍でなければなりません。

ディストリビューションポイントとして動作するデバイスについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

接続ゲートウェイ

*接続ゲートウェイ*は、特別なモードで動作するネットワークエージェントです。接続ゲートウェイは、他のネットワークエージェントからの接続を受け入れ、サーバーとの独自の接続を介してそれらを管理サーバーにトンネリングします。通常のネットワークエージェントとは異なり、接続ゲートウェイは、管理サーバーへの接続を確立するのではなく、管理サーバーからの接続を待機します。

接続ゲートウェイが通信可能なデバイスは 10,000 台までです。

接続ゲートウェイの使用方法は次の 2 つです：

- 非武装地帯（DMZ）への接続ゲートウェイのインストールを推奨します。モバイルユーザーデバイスにインストールされた別のネットワークエージェントのために、接続ゲートウェイを介した管理サーバーへの接続を専用に設定する必要があります。

  いかなる場合でも、ネットワークエージェントから管理サーバーへ転送されるデータを接続ゲートウェイが変更または処理することはありません。また、このデータをバッファに書き込むこともありません。したがって、ネットワークエージェントからデータを受信し、それを管理サーバーへ後で転送することもありません。ネットワークエージェントが接続ゲートウェイを介して管理サーバーへの接続を試行したが接続ゲートウェイが管理サーバーへ接続できない場合、ネットワークエージェントは管理サーバーがアクセス不能であると判断します。データはすべてネットワークエージェントに残ります（接続ゲートウェイには残りません）。

  接続ゲートウェイが別の接続ゲートウェイを介して管理サーバーへ接続することはできません。これは、ネットワークエージェントが同時に接続ゲートウェイとして動作したり、接続ゲートウェイを使用して管理サーバーへ接続したりすることができないことを意味します。

  接続ゲートウェイはすべて、管理サーバーのプロパティにあるディストリビューションポイントのリストに含まれています。

- 接続ゲートウェイは、ネットワーク内で使用することも可能です。たとえば、自動的に割り当てられたディストリビューションポイントは、自身の範囲内の接続ゲートウェイにもなります。ただし、接続ゲートウェイを内部ネットワークで使用しても、大きな利点はありません。管理サーバーが受信するネットワーク接続の数は減少しますが、受信データ量は減少しません。接続ゲートウェイがない場合でも、すべてのデバイスは管理サーバーへ接続可能です。

主要なインストールシナリオ

このシナリオの手順に従って、管理サーバーを導入し、ネットワークに接続されたデバイスにネットワークエージェントとセキュリティ製品をインストールできます。このシナリオによって、本製品の詳細を確認したり、今後の作業のためにアプリケーションをインストールしたりできます。

Kaspersky Security Center のインストールは次の手順で実行します：

1. 準備作業
2. 管理サーバーのデバイスに Kaspersky Security Center とカスペルスキー製品をインストールする
3. クライアントデバイスでのカスペルスキー製品の一元的な導入

Kaspersky Security Center のクラウド環境への導入とサービスプロバイダーによる Kaspersky Security Center の導入は、別のヘルプセクションで説明されています。

管理サーバーのインストールに少なくとも 1 時間、シナリオの完了に少なくとも 1 営業日を割り当てることを推奨します。Kaspersky Security Center 管理サーバーとして機能するコンピューターにも、Kaspersky Security for Windows Server や Kaspersky Endpoint Security などのセキュリティ製品をインストールしてください。

シナリオが完了すると、組織のネットワークに以下の方法で保護が導入されます：

- 管理サーバー用の DBMS がインストールされます。
- Kaspersky Security Center 管理サーバーがインストールされます。
- 必要なすべてのポリシーとタスクが作成されます。ポリシーとタスクの既定の設定が指定されます。
- セキュリティ製品（Kaspersky Endpoint Security for Windows など）とネットワークエージェントが管理対象デバイスにインストールされます。
- 管理グループが作成されます（1 つの階層に統合される場合があります）。
- 必要な場合、モバイルデバイス保護が導入されます。
- 必要に応じて、ディストリビューションポイントが割り当てられます。

Kaspersky Security Center のインストールシナリオは、次の手順で進みます：

準備作業

1 必要なファイルの取得

Kaspersky Security Center のライセンス（アクティベーションコード）またはカスペルスキーセキュリティ製品のライセンス（アクティベーションコード）があることを確認します。

販売代理店から受け取ったアーカイブを解凍します。このアーカイブには、ライセンス情報ファイル（key ファイル）、アクティベーションコード、各ライセンスでアクティベート可能なカスペルスキー製品のリストが含まれています。

Kaspersky Security Center を試用版で使用する場合は、カスペルスキーの Web サイトで 30 日間有効な試用版を取得できます。

Kaspersky Security Center に含まれないカスペルスキーセキュリティ製品のライセンスに関する詳細情報は、各製品のドキュメントを参照してください。

2 組織を保護する仕組みの選択

Kaspersky Security Center コンポーネントの詳細をご確認ください。組織に応じて最適な保護の仕組みとネットワークの設定を選択します。分散ネットワークを運用している場合、ネットワークの設定と通信チャネルのスループットに基づき、使用する管理サーバーの数と、使用する管理サーバーを組織内で分配すべき方法を定義します。

様々な運用状況で最適なパフォーマンスを実現し維持するには、ネットワークに接続されたデバイスの数、ネットワークのトポロジー、必要な Kaspersky Security Center の機能を考慮する必要があります（詳しくは Kaspersky Security Center サイジングガイドを参照してください）。

管理サーバーの階層を使用するかどうかを定義します。これを定義するには、すべてのクライアントデバイスを 1 台の管理サーバーでカバーすることが可能かつ有益か、または管理サーバーの階層を構築することが必要か、いずれかを評価する必要があります。また、保護対象のネットワークが属する組織の組織構造と同一の管理サーバーの階層を構築する必要がある場合があります。

モバイルデバイスの保護を確実にしなければならない場合は、iOS MDM サーバーの構成に必要なすべての必須処理を実行します。

管理サーバーとして選択したデバイスと、管理コンソールのインストール用のデバイスが、すべてのハードウェアおよびソフトウェア要件を満たしていることを確認します。

3 カスタム証明書を使用するための準備

組織の公開鍵インフラストラクチャ（PKI）で、特定の認証局（CA）によって発行されたカスタム証明書を使用する必要がある場合は、それらの証明書を準備し、すべての要件を満たしていることを確認してください。

4 Kaspersky Security Center のライセンスの準備

Kaspersky Security Center をモバイルデバイス管理や SIEM システムとの連携、脆弱性とパッチ管理サポートとともに使用することを計画している場合、製品のライセンス管理に使用するライセンス情報ファイルまたはアクティベーションコードを持っていることを確認します。

5 管理対象セキュリティ製品のライセンスの準備

保護導入の際、Kaspersky Security Center で管理する製品の有効なライセンスをカスペルスキーに提供する必要があります（管理可能なセキュリティ製品のリストを参照）。セキュリティ製品のライセンスの詳細は、該当する製品のドキュメントを参照してください。

6 管理サーバーと DBMS のハードウェア構成の選択

ネットワーク上のデバイスの数を考慮して、DBMS と管理サーバーのハードウェア構成を計画します。

7 DBMS の選択

DBMS の選択時は、この管理サーバーによってカバーされる管理対象デバイスの数を考慮します。ネットワーク上のデバイスの数が 10,000 台より少なく、増加する見込みがない場合、SQL Express や MySQL などの無料の DBMS を選択し、管理サーバーと同じデバイスにインストールできます。または、最大 20,000 台のデバイスを管理できる MariaDB の DBMS を使用することも可能です。ネットワーク上のデバイスの数が 10,000 台より多い場合（または 10,000 台より多くなる見込みがある場合）、有料の SQL DBMS を選択し、専用のデバイスにインストールしてください。有料の DBMS では複数の管理サーバーを使用できますが、無料の DBMS では 1 つの管理サーバーしか使用できません。

SQL Server DBMS を選択する場合、MySQL、MariaDB、Azure SQL DBMS に保管されたデータを移行することができます。移行を実行するには、データをバックアップし、新しい DBMS へ復元します。

8 DBMS のインストールとデータベースの作成

DBMS を使用するためのアカウントの詳細を確認し、DBMS をインストールします。

インストールの前に、サポート対象の DBMS を選択してください。たとえば、PostgreSQL、Postgres Pro、Microsoft SQL Server、MySQL、または MariaDB を選択できます。

選択した DBMS のインストール方法については、該当製品のマニュアルを参照してください。

MariaDB、MySQL、PostgreSQL、または Postgres Pro をインストールする場合は、DBMS が適切に機能するように推奨設定を使用してください。

管理サーバーのインストール時に DBMS の設定が必要になるので、書き留めて保存してください。この設定には SQL Server の名前、SQL Server 接続に使用するポートの番号、SQL Server へのアクセス用アカウント名とパスワードが含まれます。

PostgreSQL または Postgres Pro DBMS をインストールする場合は、スーパーユーザーのパスワードを指定したことを確認してください。パスワードが指定されていない場合、管理サーバーがデータベースに接続できない可能性があります。

既定では、Kaspersky Security Center は管理サーバー情報のデータベースを作成しますが、このデータベースを作成せずに、別のデータベースを使用することもできます。その場合、使用するデータベースが既に作成されていることと、データベースの名前を確認できること、管理サーバーがこのデータベースへのアクセスに使用するアカウントに db_owner ロールが付与されていることを確認してください。

詳細な情報が必要な場合は、DBMS の管理者へお問い合わせください。

9 ポートの設定

選択したセキュリティ構成に従ったコンポーネント間の対話に必要なすべてのポートが開いていることを確認します。

インターネットアクセスを管理サーバーに提供する必要がある場合、ネットワーク設定に応じてポートを設定し、接続設定を指定します。

10 アカウントの確認

Kaspersky Security Center 管理サーバーの正常なインストールとその後のデバイスでの保護導入に必要なローカル管理者権限をすべて備えていることを確認します。クライアントデバイスのローカル管理者権限は、それらのデバイスへのネットワークエージェントのインストールのみに必要です。ネットワークエージェントのインストール後、デバイス管理者権限のあるアカウントを使用せずにネットワークエージェントを使用して、アプリケーションをデバイスにリモートでインストールすることができます。

既定では、Kaspersky Security Center インストーラーは、管理サーバーのインストールに選択されたデバイス上に次の 3 個のアカウントを作成します。そして、これらのアカウントで管理サーバーと Kaspersky Security Center が実行されます：

- KL-AK-*：管理サーバーのサービスアカウント
- NT Service/KSC*：管理サーバープールにある他のサービス用のアカウント
- KlPxeUser：オペレーティングシステムの導入用アカウント

管理サーバーのサービスおよびその他のサービス用のアカウントを作成しない方法もあります。管理サーバーをフェールオーバークラスターにインストールする場合や、ローカルアカウントの代わりにドメインアカウントを使用する場合には、既存のアカウント（ドメインアカウントなど）を使用することも可能です。この場合、管理サーバーと Kaspersky Security Center の実行に使用するアカウントが間違いなく作成されていることを確認してください。さらに、このアカウントは特権アカウントではなく、DBMS へアクセスするために必要な権限をすべて所有している必要があります。（Kaspersky Security Center によるデバイスへのオペレーティングシステムの導入を計画している場合、アカウントの作成を省略しないでください。）

管理サーバーのデバイスに Kaspersky Security Center とカスペルスキー製品をインストールする

1 管理サーバー、管理コンソール、Kaspersky Security Center Web コンソール、セキュリティ製品の管理プラグインのインストール

カスペルスキーの Web サイトから、Kaspersky Security Center をダウンロードします。完全なパッケージ、Web コンソールのみ、または管理コンソールのみをダウンロードできます。

選択したデバイス（複数の管理サーバーを使用する場合は複数のデバイス）に管理サーバーをインストールします。管理サーバーの標準インストールまたはカスタムインストールを選択できます。管理コンソールは管理サーバーと一緒にインストールされます。管理サーバーは、ドメインコントローラーではなく専用サーバーにインストールすることを推奨します。

ネットワーク内の小規模エリアで動作をテストするなど、Kaspersky Security Center の試用評価が目的の場合は、標準インストールを推奨します。標準インストール中は、データベースのみを設定します。また、カスペルスキー製品の既定の管理プラグインセットのみをさらにインストールできます。Kaspersky Security Center の使用経験があり、標準インストール後にすべての設定を適切に指定する方法を把握している場合は、標準インストールを使用することもできます。

共有フォルダーのパス、管理サーバーへの接続用アカウントおよびポート、データベース設定などの Kaspersky Security Center の設定を編集する場合は、カスタムインストールを推奨します。カスタムインストールでは、インストールするカスペルスキー製品の管理プラグインの指定ができます。必要に応じて、サイレントモードでカスタムインストールを開始できます。

管理コンソールとサーバー版のネットワークエージェントが管理サーバーとともにインストールされます。インストール中に Kaspersky Security Center Web コンソールのインストールも選択できます。

ネットワーク経由で管理サーバーを管理するために、必要に応じて、管理者用ワークステーションに別途管理コンソールまたは Kaspersky Security Center Web コンソール（またはその両方）をインストールます。

2 初期セットアップとライセンス設定

管理サーバーのインストールが完了すると、管理サーバーへの最初の接続時にクイックスタートウィザードが自動的に開始します。既存要件に従って、管理サーバーの初期設定を行います。初期設定段階中に、ウィザードが既定値設定を使用して、保護の導入に必要なポリシーとタスクを作成します。しかしながら、既定の設定は組織のニーズに対して十分ではない場合があります。必要に応じて、ポリシーとタスクの設定を編集できます（クライアント組織のネットワーク保護の設定、シナリオ：ネットワーク保護の設定）。

基本機能に含まれない機能を使用する場合は、該当製品のライセンスを設定します。クイックスタートウィザードで実行する手順で、この設定を行えます。

3 管理サーバーのインストールの確認

これまでの手順が完了したら、管理サーバーがインストールされ使用の準備ができています。

管理コンソールが実行中であり、管理コンソールを使用して管理サーバーに接続できることを確認します。また、管理サーバーのリポジトリへのアップデートのダウンロードタスク（コンソールツリーの［**タスク**］フォルダー）と Kaspersky Endpoint Security のポリシー（コンソールツリーの［**ポリシー**］フォルダー）が使用できることを確認します。

確認が完了したら、次の手順に進みます。

クライアントデバイスでのカスペルスキー製品の一元的な導入

1 ネットワーク接続されたデバイスの検出

このステップはクイックスタートウィザードの一部です。デバイスの検索は手動で開始することもできます。Kaspersky Security Center は、ネットワークで検出されたすべてのデバイスのアドレスと名前を受信します。その後、Kaspersky Security Center を使用してカスペルスキー製品と他社製ソフトウェアを、検出されたデバイスにインストールできます。Kaspersky Security Center はデバイスの検索を定期的に開始するため、新しいインスタンスがネットワークに現れると、そのインスタンスは自動的に検出されます。

2 ネットワーク接続されたデバイスへのネットワークエージェントとセキュリティ製品のインストール

組織のネットワークに対する保護の導入時（クライアント組織のネットワーク保護の設定、シナリオ：ネットワーク保護の設定）には、デバイスの検索中に管理サーバーによって検出されたデバイスにネットワークエージェントとセキュリティ製品（Kaspersky Endpoint Security など）をインストールする必要があります。

セキュリティ製品は、ウイルスや、脅威をもたらす他のプログラムからデバイスを保護します。ネットワークエージェントは、デバイスと管理サーバー間の通信が確実に行われるようにします。ネットワークエージェントは自動的に設定されるようになっています。

必要に応じて、ネットワークエージェントをサイレントモードでインストールできます（応答ファイルの使用 / 不使用は問いません）。

ネットワーク接続されたデバイスへのネットワークエージェントとセキュリティ製品のインストールを開始する前に、それらのデバイスがアクセス可能である（電源が入っている）ことを確認してください。ネットワークエージェントを仮想マシンと物理デバイスにインストールできます。

セキュリティ製品とネットワークエージェントのインストールは、リモートでもローカルでも実行可能です。

リモートインストール – 製品導入ウィザードを使用して、管理サーバーによって検出された組織ネットワーク内のデバイスにセキュリティ製品（Kaspersky Endpoint Security for Windows など）とネットワークエージェントをリモートでインストールできます。通常は、ネットワーク接続されたデバイスのほとんどに、リモートインストールで保護を導入できます。ただし、デバイスの電源が入っていない場合や何らかの理由でデバイスにアクセスできない場合などにエラーが発生することがあります。この場合、手動でデバイスに接続してローカルインストールを使用してください。

ローカルインストール – リモートインストールで保護を導入できなかったネットワークデバイスに使用します。このようなデバイスに保護をインストールするには、デバイスのローカルで実行できるスタンドアロンインストールパッケージを作成します。

Linux オペレーティングシステムと macOS オペレーティングシステムを実行しているデバイスへのネットワークエージェントのインストールについてはそれぞれ、Kaspersky Endpoint Security for Linux と Kaspersky Endpoint Security for Mac のヘルプを参照してください。Linux オペレーティングシステムや macOS オペレーティングシステムを実行しているデバイスは、Windows を実行しているデバイスよりも脆弱性が少ないと考えられていますが、それらのデバイスにもセキュリティ製品をインストールすることを推奨します。

インストール後、セキュリティ製品が管理対象デバイスにインストールされていることを確認してください。カスペルスキー製品バージョンレポートを実行し、結果を表示します。

3 ライセンスのクライアントデバイスへの導入

クライアントデバイスにライセンスを導入し、デバイス上の管理対象セキュリティ製品をアクティベートします。

4 モバイルデバイス保護を設定する

このステップはクイックスタートウィザードの一部です。

企業用モバイルデバイスを管理する場合は、モバイルデバイス管理の準備と導入に必要な手順を実行します。

5 管理グループ構造の作成

ネットワーク接続デバイスへ最も便利な方法で保護を導入する目的で、組織の構造を考慮してデバイスのプール全体を管理グループに分割しなければならない場合があります。グループにデバイスを配置する移動ルールを作成するか、デバイスを手動で配置することができます。管理グループへのグループタスクの割り当て、ポリシーの範囲の定義、およびディストリビューションポイントの割り当てが可能です。

すべての管理対象デバイスが適切な管理グループに正しく割り当てられ、ネットワーク上に未割り当てデバイスが存在しないことを確認します。

6 ディストリビューションポイントの割り当て

Kaspersky Security Center は管理グループにディストリビューションポイントを自動的に割り当てますが、必要に応じて手動で割り当てることも可能です。大規模なネットワークにはディストリビューションポイントを使用することを推奨します。その理由は、低いスループットレートのチャネルを介して通信するデバイス（またはデバイスグループ）へのアクセスを管理サーバーに提供するために使用する分散構造ネットワーク上、および管理サーバーで、負荷を減らすためです。Linux を実行しているデバイスをディストリビューションポイントとして使用することも、Windows を実行しているデバイスを使用することもできます。

Kaspersky Security Center で使用するポート

下記の表に、管理サーバーとクライアントデバイスで開く必要のある既定のポートを示します。必要に応じて、既定のポート番号を変更できます。

下記の表に、管理サーバーで開く必要のある既定のポートを示します。管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MySQL Server 用のポート 3306、Microsoft SQL Server 用のポート 1433、PostgreSQL および Postgres Pro 用のポート 5432 など）。関連する情報については、DBMS のドキュメントを参照してください。

管理サーバーで開く必要のあるポート

ポート番号	ポートを開くプロセスの名前	プロトコル	ポートの目的	範囲
8060	klcsweb	TCP	公開済みインストールパッケージをクライアントデバイスに送信する	インストールパッケージの公開 管理コンソールまたは Kaspersky Security Center Web コンソールにある管理サーバーのプロパティウィンドウの［**Web サーバー**］セクションで、既定のポート番号を変更できます。
8061	klcsweb	TCP (TLS)	公開済みインストールパッケージをクライアントデバイスに送信する	インストールパッケージの公開 管理コンソールまたは Kaspersky Security Center Web コンソールにある管理サーバーのプロパティウィンドウの［**Web サーバー**］セクションで、既定のポート番号を変更できます。
13000	klserver	TCP (TLS)	ネットワークエージェントおよびセカンダリ管理サーバーからの接続の受信、セカンダリ管理サーバーでのプライマリ管理サーバーからの接続の受信（セカンダリ管理サーバーが DMZ にある場合など）	クライアントデバイスとセカンダリ管理サーバーの管理 接続ポートの設定中にネットワークエージェントから接続を受信する既定のポートの番号を変更できます。管理コンソールまたは Kaspersky Security Center Web コンソールで管理サーバーの階層の作成中にセカンダリ管理サーバーから接続を受信する既定のポートの番号を変更できます。
13000	klserver	UDP	ネットワークエージェントからオフにされたデバイスに関する情報を受信する	クライアントデバイスの管理。 管理コンソールまたは Kaspersky Security Center Web コンソールにあるネットワークエージェントのポリシーの設定で、既定のポート番号を変更できます。
13291	klserver	TCP (TLS)	管理コンソールから管理サーバーへの接続を受信する	管理サーバーの管理 管理コンソールの管理サーバーのプロパティウィンドウで、既定のポート番号を変更できます。
13299	klserver	TCP (TLS)	Kaspersky Security Center Web コンソールから管理サーバーへの接続を受信する、OpenAPI 経由での管理サーバーへの接続を受信する	Kaspersky Security Center Web コンソール、OpenAPI 既定のポート番号は、管理コンソールの管理サーバーのプロパティウィンドウ（［**全般**］の［**接続ポート**］サブセクション）、管理コンソールまたは Kaspersky Security Center Web コンソールでの管理サーバー階層の作成時に変更できます。
14000	klserver	TCP	ネットワークエージェントから接続を受信する	クライアントデバイスの管理。 既定のポート番号は、Kaspersky Security Center のインストール中の接続ポートの設定時または管理サーバーにクライアントデバイスを手動で接続している際に変更できます。
13111（KSN プロキシサービスがデバイスで実行されている場合のみ）	ksnproxy	TCP	管理対象デバイスから KSN プロキシサーバーへの要求を受信する	KSN プロキシサーバー。 対象となる既定のポート番号は管理サーバーのプロパティで変更できます。
15111（KSN	ksnproxy	UDP	管理対象デバイスから KSN プロキシサー	KSN プロキシサーバー。

プロキシサービスがデバイスで実行されている場合のみ）			バーへの要求を受信する	対象となる既定のポート番号は管理サーバーのプロパティで変更できます。
17000	klactprx	TCP (TLS)	管理対象デバイスから製品のアクティベーション用の接続を受信する（モバイルデバイスを除く）	カスペルスキー製品をアクティベーションコードでアクティベートするために、モバイルではないデバイスで使用しているアクティベーションプロキシサーバー。 対象となる既定のポート番号は管理サーバーのプロパティで変更できます。
17100（モバイルデバイスを管理している場合のみ）	klactprx	TCP (TLS)	モバイルデバイスから製品のアクティベーション用の接続を受信する	モバイルデバイス用のアクティベーションプロキシサーバー。 対象となる既定のポート番号は管理サーバーのプロパティで変更できます。
19170	klserver	HTTPS (TLS)	klsctunnel ユーティリティを使用した管理対象デバイスへの接続のトンネリング	Kaspersky Security Center Web コンソールを使用した管理対象デバイスへのリモート接続。 既定のポート番号は、管理コンソールの管理サーバーのプロパティウィンドウ（［**全般**］セクションの［**追加のポート**］サブセクション）でのみ変更できます。
13292（モバイルデバイスを管理している場合のみ）	klserver	TCP (TLS)	モバイルデバイスから接続を受信する	モバイルデバイス管理。 管理コンソールまたは Kaspersky Security Center Web コンソールにある管理サーバーのプロパティウィンドウで、既定のポート番号を変更できます。
13294（モバイルデバイスを管理している場合のみ）	klserver	TCP (TLS)	UEFI 保護デバイスから接続を受信する	UEFI 保護クライアントデバイスの管理 モバイルデバイスの接続時または後から、管理コンソールまたは Kaspersky Security Center Web コンソールにある管理サーバーのプロパティウィンドウ（［**全般**］セクションの［追加のポート］サブセクション）で、既定のポート番号を変更できます。
13296	klserver	TCP (TLS)	Prometheus 用 Kaspersky Security Center メトリクスの公開	Prometheus によってさらに取得される Kaspersky Security Center メトリクスを公開します。 次のリンクからメトリクスを表示できます：https://<サーバーアドレス>:13296/metrics。<サーバーアドレス> には、管理サーバーの IP アドレスまたはドメイン名を指定します。 管理コンソールの管理サーバーのプロパティウィンドウで、既定のポート番号を変更できます。
30522、 30523（ローカルホストインターフェイス上のポート）	klnagent	TCP	FileTransferBridge コンポーネントを使用して管理サーバーからカスペルスキー製品のアップデートを受信します	カスペルスキー製品のアップデートを受信する管理サーバーデバイス。

次の表は、iOS MDM サーバーで開く必要のある既定のポートを示しています（モバイルデバイスを管理している場合のみ）。

Kaspersky Security Center の iOS MDM サーバーで使用するポート

ポート番号	ポートを開くプロセスの名前	プロトコル	ポートの目的	範囲
443	kliosmdmservicesrv	TCP (TLS)	iOS モバイルデバイスから接続を受信する	モバイルデバイス管理。 既定のポート番号は、iOS MDM サーバーのインストール時に変更できます。

下記の表に、Kaspersky Security Center Web コンソールサーバーで開く必要のある既定のポートを示します。管理サーバーがインストールされている同じデバイスでも、別のデバイスでも問題ありません。

Kaspersky Security Center の Web コンソールサーバーで使用するポート

ポート番号	ポートを開くプロセスの名前	プロトコル	ポートの目的	範囲

8080	Node.js: Server-side JavaScript	TCP (TLS)	ブラウザーから Kaspersky Security Center Web コンソールへの接続を受信する	Kaspersky Security Center Web コンソール。 既定のポート番号は、Windows または Linux プラットフォームで実行中のデバイスに Kaspersky Security Center Web コンソールをインストールする際に変更できます。Linux ALT オペレーティングシステム上に Kaspersky Security Center Web コンソールをインストールする場合、ポート番号 8080 はオペレーティングシステムによって使用されているため、ポート番号には 8080 以外の数字を指定する必要があります。

下記の表に、ネットワークエージェントがインストールされている管理対象デバイスの管理で開く必要のある既定のポートを示します。

ネットワークエージェントが使用するポート

ポート番号	ポートを開くプロセスの名前	プロトコル	ポートの目的	範囲
15000	klnagent	UDP	管理サーバーまたはディストリビューションポイントからネットワークエージェントへの管理信号	クライアントデバイスの管理。 管理コンソールまたは Kaspersky Security Center Web コンソールにあるネットワークエージェントのポリシーの設定で、既定のポート番号を変更できます。
15000	klnagent	UDP ブロードキャスト	同じブロードキャストドメイン内の他のネットワークエージェントに関するデータの取得（データは管理サーバーに送信されます）	アップデートおよびインストールパッケージの提供。
15001	klnagent	UDP	ディストリビューションポイント（使用している場合）からマルチキャスト要求を受信する	ディストリビューションポイントからアップデートとインストールパッケージを受信する。 既定のポート番号は、管理コンソールまたは Kaspersky Security Center Web コンソールのディストリビューションポイントのプロパティウィンドウで変更できます。
30522、 30523（ローカルホストインターフェイス上のポート）	klnagent	TCP	FileTransferBridge コンポーネントを使用して管理サーバーからカスペルスキー製品のアップデートを受信します	定義データベースのアップデート元として指定された管理サーバーからカスペルスキー製品のアップデートを受信する管理対象デバイス。
161	klnagent	SNMP	ネットワークに接続されたデバイスの監視と検出。	デバイスの検出可能性。

klnagent プロセスは、エンドポイントオペレーティングシステムの動的ポート範囲から空きポートを要求することもできます。これらのポートは、オペレーティングシステムによって自動的に klnagent プロセスに割り当てられるため、klnagent プロセスは別のソフトウェアで使用されている一部のポートを使用できます。klnagent プロセスがそのソフトウェアの動作に影響を与える場合は、このソフトウェアのポート設定を変更するか、オペレーティングシステムの既定の動的ポート範囲を変更して、影響を受けるソフトウェアに使用されるポートを除外します。

また、Kaspersky Security Center とサードパーティ製ソフトウェアとの互換性に関する推奨事項は参照のみを目的として説明されており、サードパーティ製ソフトウェアの新しいバージョンには適用できない場合があることにも注意してください。説明されているポート設定の推奨事項は、テクニカルサポートの経験とベストプラクティスに基づいています。

下記の表に、ディストリビューションポイントとして動作するネットワークエージェントがインストールされたデバイスで開く必要がある既定のポートを示します。ネットワークエージェントで使用されるポートに加えて、リストにあるポートをディストリビューションポイントデバイスで開いておく必要があります（上記の表を参照）。

ディストリビューションポイントとして動作するネットワークエージェントが使用するポート

ポート番号	ポートを開くプロセスの名前	プロトコル	ポートの目的	範囲
13000	klnagent	TCP (TLS)	ディストリビューションポイントが DMZ 内の接続ゲートウェイとして機能する場合、ネットワークエージェントおよび Kaspersky	クライアントデバイスの管理、アップデートおよびイ

			Security Center からの接続を受信します。管理サーバーがインストールされているデバイスがディストリビューションポイントとして指定されている場合、SSL 接続には既定でポート 13000 ではなくポート 13001 が使用されます。	ンストールパッケージの提供。 詳細については、以下のトピックを参照してください：管理サーバー、ネットワークセグメント内の接続ゲートウェイ、およびクライアントデバイス。 既定のポート番号は、管理コンソールまたは Kaspersky Security Center Web コンソールのディストリビューションポイントのプロパティウィンドウで変更できます。
13111（KSN プロキシサービスがデバイスで実行されている場合のみ）	ksnproxy	TCP	管理対象デバイスから KSN プロキシサーバーへの要求を受信する	KSN プロキシサーバー。 既定のポート番号は、管理コンソールまたは Kaspersky Security Center Web コンソールのディストリビューションポイントのプロパティウィンドウで変更できます。
15111（KSN プロキシサービスがデバイスで実行されている場合のみ）	ksnproxy	UDP	管理対象デバイスから KSN プロキシサーバーへの要求を受信する	KSN プロキシサーバー。 既定のポート番号は、管理コンソールまたは Kaspersky Security Center Web コンソールのディストリビューションポイントのプロパティウィンドウで変更できます。
17111（KSN プロキシサービスがデバイスで実行されている場合のみ）	ksnproxy	HTTPS	管理対象デバイスから KSN プロキシサーバーへの要求を受信する	KSN プロキシサーバー。 既定のポート番号は、管理コンソールまたは Kaspersky Security Center Web コンソールのディストリビューションポイントのプロパティウィンドウで変更できます。
13295（ディストリビューションポイントをプッシュサーバーとして使用する場合のみ）	klnagent	TCP (TLS)	クライアントデバイスからの接続の受信	プッシュサーバー： 既定のポート番号は、管理コンソールまたは Kaspersky Security Center Web コンソールのディストリビューションポイントのプロパティウィンドウで変更できます。

Kaspersky Security Center を使用するための証明書

このセクションでは、Kaspersky Security Center の証明書に関する情報と、管理サーバー向けのカスタム証明書を発行する方法について説明します。

Kaspersky Security Center の証明書について

Kaspersky Security Center では、次の種類の証明書を使用することで、製品コンポーネント間の安全な対話を可能にしています。

- 管理サーバー証明書

- モバイル証明書
- iOS MDM サーバー証明書
- Kaspersky Security Center Web サーバーの証明書
- Kaspersky Security Center Web コンソールの証明書

既定では、Kaspersky Security Center は自己署名証明書（つまり、Kaspersky Security Center 自体によって発行された証明書）を使用しますが、組織のネットワークの要件をより適切に満たし、セキュリティ標準に準拠するために、それらをカスタム証明書に置換することができます。カスタム証明書が該当するすべての要件を満たしているかどうかを管理サーバーが検証し、その後、この証明書は自己署名証明書と同じ機能範囲があると判断されます。唯一の違いは、カスタム証明書は期限切れ時に自動的に再発行されないことです。証明書のタイプに応じて、klsetsrvcert ユーティリティを使用するか、管理コンソールの［管理サーバーのプロパティ］セクションを介して、証明書をカスタム証明書に置換します。Klsetsrvcert ユーティリティを使用している際には、次の値のいずれかを使用して証明書を指定する必要があります：

- C：（ポート 13000 と 13291 に共通の証明書）
- CR：（ポート 13000 と 13291 に共通の予備の証明書）
- M：（ポート 13292 のモバイル証明書）
- MR：（ポート 13292 のモバイル予備証明書）
- MCA：（自動生成されたユーザー証明書のモバイル認証局）

klsetsrvcert ユーティリティをダウンロードする必要はありません。Kaspersky Security Center の配布キットに含まれています。このユーティリティには、Kaspersky Security Center の以前のバージョンとの互換性はありません。

管理サーバー証明書の最大有効期間は 397 日以下である必要があります。

管理サーバー証明書

管理サーバー証明書は、管理サーバーの認証、および管理サーバーと管理対象デバイス上のネットワークエージェント間、またはプライマリ管理サーバーとセカンダリ管理サーバー間のセキュアな対話に必要です。管理コンソールと管理サーバーの初回接続時に、現在の管理サーバー証明書の使用の確認が要求されます。このような確認は、管理サーバー証明書を交換するたび、管理サーバーを再インストールするたび、およびセカンダリ管理サーバーをプライマリ管理サーバーに接続する時にも必要です。この証明書は共通（「C」）と呼ばれます。

共通 （「C」）証明書は、管理サーバーコンポーネントのインストール時に自動的に作成されます。証明書には次の 2 つの要素があります：

- klserver.cer ファイルは、既定では管理サーバーコンポーネントがインストールされたデバイスの［C:\ProgramData\KasperskyLab\adminkit\1093\cert］フォルダーにあります。
- Windows 保護ストレージにある秘密鍵。

また、共通予備（「CR」）証明書も存在します。Kaspersky Security Center は、共通証明書の有効期限が切れる 90 日前にこの証明書を自動的に生成します。その後、共通予備証明書を使用して、管理サーバー証明書はシームレスに置換されます。共通証明書の有効期限が近づくと、共通予備証明書を使用して、管理対象デバイスにインストールされているネットワークエージェントインスタンスとの接続が維持されます。この目的で、共通予備証明書は、古い共通証明書の有効期限が切れる 24 時間前に自動的に新しい共通証明書になります。

データを失うことなく管理サーバーをあるデバイスから別のデバイスに移動するために、他の管理サーバー設定とは別に管理サーバー証明書をバックアップすることもできます。

モバイル証明書

モバイルデバイスでの管理サーバーの認証には、モバイル証明書（「M」）が必要です。モバイル証明書の使用は、クイックスタートウィザードの専用の手順で設定します。

また、モバイル予備（「MR」）証明書も存在します。これは、モバイル証明書のシームレスな置換に使用されます。Kaspersky Security Center は、共通証明書の有効期限が切れる 60 日前にこの証明書を自動的に生成します。モバイル証明書の有効期限が近づくと、モバイル予備証明書を使用して、管理対象のモバイルデバイスにインストールされているネットワークエージェントインスタンスとの接続が維持されます。この目的で、モバイル予備証明書は、古い証明書の有効期限が切れる 24 時間前に自動的に新しい証明書になります。

接続シナリオで、モバイルデバイスでクライアント証明書を使用する必要がある場合（双方向 SSL 認証を含む接続）、自動生成されたクライアント証明書（「MCA」）の認証局を使用してそれらの証明書を生成できます。また、クイックスタートウィザードを使用すると、別の認証局によって発行されたカスタムクライアント証明書の使用を開始できます。一方、組織のドメイン公開鍵インフラストラクチャ（PKI）と統合すると、ドメイン認証局を使用してクライアント証明書を発行できます。

iOS MDM サーバー証明書

iOS オペレーティングシステムで動作しているモバイルデバイスでの管理サーバーの認証には、iOS MDM サーバー証明書が必要です。これらのデバイスとのインタラクションは、ネットワークエージェントを含まない Apple モバイルデバイス管理（MDM）プロトコルを介して実行されます。代わりに、クライアント証明書を含む特別な iOS MDM プロファイルを各デバイスにインストールして、双方向 SSL 認証を保証します。

また、クイックスタートウィザードを使用すると、別の認証局によって発行されたカスタムクライアント証明書の使用を開始できます。一方、組織のドメイン公開鍵インフラストラクチャ（PKI）と統合すると、ドメイン認証局を使用してクライアント証明書を発行できます。

これらの iOS MDM プロファイルをダウンロードすると、クライアント証明書が iOS デバイスに送信されます。iOS MDM Server クライアント証明書は、管理対象の iOS デバイスごとに一意です。自動生成されたユーザー証明書（「MCA」）の認証局を使用して、すべての iOS MDM Server クライアント証明書を生成します。

Kaspersky Security Center Web サーバーの証明書

Kaspersky Security Center 管理サーバーのコンポーネントである Kaspersky Security Center Web サーバー（以降、「Web サーバー」と表記) は、特殊な種別の証明書を使用します。この証明書は、後で管理対象デバイスにダウンロードするネットワークエージェントインストールパッケージの公開、および iOS MDM プロファイル、iOS アプリ、Kaspersky Security for Mobile インストールパッケージの公開に必要です。この目的のために、Web サーバーは様々な証明書を使用できます。

モバイルデバイスのサポートが無効になっている場合、Web サーバーは優先度の高い順に次の証明書のいずれかを使用します：

1. 管理コンソールを使用して手動で指定したカスタム Web サーバー証明書

2. 共通管理サーバー証明書（「C」）

モバイルデバイスのサポートが有効になっている場合、Web サーバーは優先度の高い順に次の証明書のいずれかを使用します：

1. 管理コンソールを使用して手動で指定したカスタム Web サーバー証明書
2. カスタムモバイル証明書
3. 自己署名モバイル証明書（「M」）
4. 共通管理サーバー証明書（「C」）

Kaspersky Security Center Web コンソールの証明書

Kaspersky Security Center Web コンソールサーバー（以降「Web コンソール」と表記）には、独自の証明書があります。Web サイトを開く際に、ブラウザは接続が信頼できるかどうかを確認します。Web コンソール証明書を使用して、Web コンソールを認証できます。この証明書は、ブラウザーと Web コンソールの間のトラフィックの暗号化にも使用されます。

Web コンソールを開くと、ブラウザーから Web コンソールとの接続がプライベートでなく Web コンソールの証明書が無効であると通知される場合があります。この警告は、Web コンソールの証明書が自己署名で、Kaspersky Security Center によって自動で生成されているために表示されます。この警告が表示されないようにするには、次の操作のうち 1 つを実行します：

- カスタム証明書と Web コンソールの証明書を置き換える（推奨）。企業のインフラストラクチャで信頼済みで、かつ、カスタム証明書の要件を満たす証明書を作成する。
- ブラウザーの信頼済み証明書のリストに Web コンソールの証明書を追加する。カスタム証明書を作成できない場合には、この方法を推奨します。

管理サーバー証明書の概要

管理サーバー証明書（管理コンソールによる接続およびデバイスとのデータ交換中の管理サーバー認証）に基づいて 2 つの操作が実行されます。証明書は、プライマリ管理サーバーがセカンダリ管理サーバーに接続する際の認証にも使用されます。

カスペルスキーが発行する証明書

管理サーバー証明書は、管理サーバーのインストール中に自動的に作成され、フォルダー「%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert」に格納されます。

管理サーバーの証明書が管理サーバーのバージョン 12.2 以前で生成された場合、管理サーバーの証明書は 5 年間有効です。それ以外の場合、証明書の有効期間は 397 日に制限されます。現在の証明書が期限切れになる 90 日前に、新しい証明書が管理サーバーにより予備の証明書として作成されます。その後、有効期限の 1 日前に、現在の証明書が自動的に新しい証明書で置換されます。新しい証明書を使用して管理サーバーを認証するように、すべてのクライアントデバイスのネットワークエージェントが自動的に再設定されます。

カスタム証明書

必要に応じて、カスタム証明書を管理サーバーに割り当てることができます。たとえば、企業の既存の PKI とのより容易な統合や、証明書フィールドの設定のカスタマイズなどの理由で、こうした操作が必要になる場合があります。

管理サーバー証明書の最大有効期間は 397 日以下である必要があります。

証明書を置換すると、以前 SSL を介して管理サーバーに接続したすべてのネットワークエージェントの接続が切断され、「管理サーバー証明書エラー」が返されます。このエラーを解消するには、証明書の置換後に接続を復元する必要があります。

管理サーバー証明書を紛失した場合、その証明書を復元するには、管理サーバーを再インストールしてデータを復元する必要があります。

別のブラウザーで Kaspersky Security Center Web コンソールを開いて、管理サーバーの証明書ファイルを管理サーバーのプロパティウィンドウでダウンロードすると、ダウンロードされたファイルに異なる名前が付与されます。

Kaspersky Security Center で使用されるカスタム証明書の要件

次の表は、Kaspersky Security Center の様々なコンポーネントに指定されているカスタム証明書の要件を示しています。

Kaspersky Security Center 証明書の要件

証明書の種別	要件	コメント
共通証明書、予備の共通証明書（「C」「CR」）	最短鍵長：2048 Basic Constraints（基本制約）： • Path Length Constraint（パス長制約）：None Key Usage（鍵用途）： • デジタル署名 • 証明書の署名の検証 • 鍵の暗号化 • 証明書失効リスト（CRL）の署名の検証 Extended Key Usage（拡張鍵用途）（任意）：サーバー認証、クライアント認証。	Extended Key Usage パラメータは任意です。 Path Length Constraint の値は「None」ではなく、「1」以上の整数である場合があります。
モバイルデバイス用証明書、モバイルデバイス用の予備の証明書（「M」「MR」）	最短鍵長：2048 Basic Constraints（基本制約）： • CA：true • Path Length Constraint（パス長制約）：None Key Usage（鍵用途）： • デジタル署名 • 証明書の署名の検証 • 鍵の暗号化 • 証明書失効リスト（CRL）の署名の検証	Extended Key Usage パラメータは任意です。 Path Length Constraint の値は「None」ではない場合があります（共通証明書の Path Length Constraint の値が「1」以上である場合）。

	Extended Key Usage（拡張鍵用途）（任意）：サーバー認証。	
自動生成されたユーザー証明書用の CA 証明書（「MCA」）	最短鍵長：2048 Basic Constraints（基本制約）： • CA：true • Path Length Constraint（パス長制約）：None Key Usage（鍵用途）： • デジタル署名 • 証明書の署名の検証 • 鍵の暗号化 • 証明書失効リスト（CRL）の署名の検証 Extended Key Usage（拡張鍵用途）（任意）：サーバー認証、クライアント認証。	Extended Key Usage パラメータは任意です。 Path Length Constraint の値は「None」ではない整数の場合があります（共通証明書の Path Length Constraint の値が「1」以上である場合）。
Web サーバーの証明書	Extended Key Usage（拡張鍵用途）：サーバー認証。 証明書が指定されている PKCS #12 コンテナーや PEM コンテナーには、公開鍵のチェーン全体が含まれています。 証明書のサブジェクト代替名（SAN）が存在します。つまり、`subjectAltName` フィールドの値は有効です。 証明書は、サーバー証明書に適用されたブラウザーの有効な要件、および CA/Browser Forum の現在のベースライン要件を満たしています。	—
Kaspersky Security Center Web コンソールの証明書	証明書が指定される PEM コンテナーには、公開鍵のチェーン全体が含まれます。 証明書のサブジェクト代替名（SAN）が存在します。つまり、`subjectAltName` フィールドの値は有効です。 証明書は、サーバー証明書に対するブラウザーの有効な要件、および CA /Browser Forum の現在のベースライン要件を満たしています。	暗号化された証明書は、Kaspersky Security Center Web コンソールではサポートされていません。

シナリオ：管理サーバーのカスタム証明書の指定

管理サーバーのカスタム証明書を割り当てることができます。目的の例として、企業で使用する既存の公開鍵インフラストラクチャ（PKI）との連携の改善、証明書フィールドのカスタム設定などがあります。管理サーバーのインストール直後、かつクイックウィザードの終了前に、証明書を置換することを推奨します。

管理サーバー証明書の最大有効期間は 397 日以下である必要があります。

必須条件

以下の条件を満たす必要があります：

- 新しい証明書は、PKCS#12 形式（たとえば、組織の PKI を使用）で作成する必要があります。
- その新規の証明書は、次の表にリストされた要件を満たす必要があります。

- 以下の表では、新しい証明書が信頼できる認証局（CA）によって発行される必要があることを意味する要件「CA：true」に注意してください。「CA：true」という要件の新しい証明書には、信頼の連鎖全体と秘密鍵が含まれている必要があり、その秘密鍵は拡張子が pfx または p12 のファイルに格納されている必要があります。

管理サーバー証明書の要件

証明書の種別	要件
共通証明書、予備の共通証明書（「C」「CR」）	最短鍵長：2048 Basic Constraints（基本制約）： • Path Length Constraint（パス長制約）：None Path Length Constraint の値は「None」ではなく、「1」以上の整数である場合があります。 Key Usage（鍵用途）： • デジタル署名 • 証明書の署名の検証 • 鍵の暗号化 • 証明書失効リスト（CRL）の署名の検証 Extended Key Usage（EKU：拡張鍵用途）：サーバー認証、クライアント認証。EKU は任意ですが、証明書に含まれる場合、サーバーとクライアントの認証データは EKU で指定されている必要があります。
モバイルデバイス用証明書、モバイルデバイス用の予備の証明書（「M」「MR」）	最短鍵長：2048 Basic Constraints（基本制約）： • CA：true • Path Length Constraint（パス長制約）：None Path Length Constraint の値は「None」ではない場合があります（共通証明書の Path Length Constraint の値が「1」以上である場合）。 Key Usage（鍵用途）： • デジタル署名 • 証明書の署名の検証 • 鍵の暗号化 • 証明書失効リスト（CRL）の署名の検証 Extended Key Usage（EKU：拡張鍵用途）：サーバー認証。EKU は任意ですが、証明書に含まれる場合、サーバーの認証データは EKU で指定されている必要があります。
自動生成されたユーザー証明書用の CA 証明書（「MCA」）	最短鍵長：2048 Basic Constraints（基本制約）： • CA：true • Path Length Constraint（パス長制約）：None Path Length Constraint の値は「None」ではない場合があります（共通証明書の Path Length Constraint の値が「1」以上である場合）。 Key Usage（鍵用途）： • デジタル署名 • 証明書の署名の検証 • 鍵の暗号化 • 証明書失効リスト（CRL）の署名の検証 Extended Key Usage（EKU：拡張鍵用途）：クライアント認証。EKU は任意ですが、証明書に含まれる場合、クライアントの認証データは EKU で指定されている必要があります。

パブリック CA によって発行された証明書には、証明書署名の許可がありません。このような証明書を使用するには、ネットワークのディストリビューションポイントまたは接続ゲートウェイに、ネットワークエージェントのバージョン 13 以降がインストールされていることを確認してください。そうしないと、署名の許可なしに証明書を使用できなくなります。

実行するステップ

管理サーバー証明書の指定は段階的に進行します。

1. **管理サーバー証明書の置換**

   この目的のために、コマンドラインで klsetsrvcert ユーティリティを使用します。

2. **新しい証明書を指定し、ネットワークエージェントの管理サーバーへの接続を復元**

   証明書を置換すると、以前 SSL を介して管理サーバーに接続したすべてのネットワークエージェントの接続が切断され、「管理サーバー証明書エラー」が返されます。新しい証明書を指定して接続を復元するには、コマンドラインで klmover ユーティリティを使用します。

3. **Kaspersky Security Center Web コンソールの設定で新しい証明書を指定する**

   証明書を置き換えた後、Kaspersky Security Center Web コンソールの設定でこれを指定します。この操作を実行しない場合、Kaspersky Security Center Web コンソールは管理サーバーに接続できなくなります。

結果

このシナリオを終了すると、管理サーバー証明書が置換され、管理対象デバイスのネットワークエージェントでサーバーが認証されます。

klsetsrvcert ユーティリティを使用した管理サーバー証明書の置換

管理サーバーの証明書を手動で置換するには：

コマンドラインから、次のユーティリティを実行します：

```
klsetsrvcert[-t <種別> {-i <入力ファイル> [-p <パスワード>] [-o <証明書の検証パラメータ>] |
-g <DNS 名>}][-f <時刻>][-r <CA のリストファイル>][-l <ログファイル>]
```

klsetsrvcert ユーティリティをダウンロードする必要はありません。Kaspersky Security Center の配布キットに含まれています。Kaspersky Security Center の以前のバージョンとは互換性がありません。

klsetsrvcert ユーティリティのパラメータの説明を次の表に示します。

klsetsrvcert ユーティリティのパラメータ値

パラメータ	値
`-t <種別>`	置換する証明書の種別。<種別>パラメータに指定可能な値： • `C`：ポート 13000 と 13291 の共通証明書を置換 • `CR`：ポート 13000 と 13291 の予備の証明書を置換

	• M：ポート 13292 のモバイルデバイス用証明書を置換 • MR：ポート 13292 のモバイル予備証明書を置換 • MCA：自動生成されたユーザー証明書のモバイルクライアント CA
-f <時刻>	証明書の変更の予定時刻。形式は「DD-MM-YYYY hh:mm」です（ポート 13000 と 13291 向け）。 有効期間の終了前に、共通証明書または予備の共通証明書を置換する場合は、このパラメータを使用します。 管理対象デバイスが新しい証明書で管理サーバーと同期する必要がある時間を指定します。
-i <入力ファイル>	PKCS#12 形式の証明書と秘密鍵を持つコンテナー（拡張子が .p12 または .pfx のファイル）。
-p <パスワード>	p12 コンテナーの保護に使用されるパスワード 証明書と秘密鍵はコンテナに保存されているため、コンテナでファイルを復号化するにはパスワードが必要です。
-o <証明書の検証パラメータ>	証明書の検証パラメータ（セミコロン区切り）。 証明書署名の権限なしにカスタム証明書を使用するには、klsetsrvcert ユーティリティで -o NoCA を指定します。これは、パブリック認証局（CA）によって発行された証明書に役立ちます。 証明書タイプ C または CR の暗号化鍵の長さを変更するには、klsetsrvcert ユーティリティで -o RsaKeyLen:<鍵長> を指定します。ここで、<鍵長>パラメータは必要な鍵の長さの値です。それ以外の場合は、現在の証明書の鍵の長さが使用されます。
-g <DNS 名>	指定した DNS 名に対する新しい証明書が作成されます。
-r <CA のリストファイル>	信頼済みのルート証明機関のリスト（PEM 形式）。
-l <ログファイル>	結果出力ファイル。既定では、出力は標準出力ストリームにリダイレクトされます

例えば、カスタム管理サーバー証明書を指定するには、次のコマンドを使用します。

```
klsetsrvcert -t C -i <入力ファイル> -p <パスワード> -o NoCA
```

証明書が置換されると、SSL を介して管理サーバーに接続されているすべてのネットワークエージェントの接続は切断されます。復元するには、コマンドライン klmover ユーティリティを使用します。

ネットワークエージェントの接続が切断されないようにするには、次のコマンドを使用します：

1. 新しい証明書をインストールするには、

```
klsetsrvcert.exe -t CR -i <入力ファイル> -p <パスワード> -o NoCA
```

2. 新しい証明書を適用する日付を指定するには、

```
klsetsrvcert.exe -f "DD-MM-YYYY hh:mm"
```

"DD-MM-YYYY hh:mm" は、現在より 3 ～ 4 週間先の日付です。時間を変えて証明書を新しいものに変更することにより、新しい証明書をすべてのネットワークエージェントに配信できます。

klmover ユーティリティを使用したネットワークエージェントの管理サーバーへの接続

コマンドラインで klsetsrvcert ユーティリティを使用して管理サーバー証明書を置換した後は、接続が切断されているため、ネットワークエージェントと管理サーバー間の SSL 接続を確立する必要があります。

新しい管理サーバー証明書を指定して接続を復元するには：

コマンドラインから、次のユーティリティを実行します：

```
klmover [-address <サーバーアドレス>] [-pn <ポート番号>] [-ps <SSL ポート番号>] [-nossl] [-cert <証明書ファイルのパス>]
```

ユーティリティを実行するには管理者権限が必要です。

このユーティリティは、ネットワークエージェントがクライアントデバイスにインストールされると、ネットワークエージェントのインストールフォルダーに自動的にコピーされます。

侵入者がデバイスを管理サーバーの制御外に移動するのを防ぐために、klmover ユーティリティを実行する際のパスワード保護を有効にすることを強く推奨します。パスワード保護を有効にするには、ネットワークエージェントポリシー設定で［**アンインストール用パスワードを使用する**］をオンにします。

klmover ユーティリティにはローカル管理者権限が必要です。ローカル管理者権限なしで操作されるデバイスの場合、klmover ユーティリティを実行するためのパスワード保護を省略できます。

アンインストール用パスワードを使用するを有効にすると、クリーナーツール（cleaner.exe）のパスワード保護も有効になります。

klsetsrvcert ユーティリティのパラメータの説明を次の表に示します。

klmover ユーティリティのパラメータ値

パラメータ	値
`-address <サーバーアドレス>`	接続する管理サーバーのアドレス。 デバイスの IP アドレス、NetBIOS 名、DNS 名を指定できます。
`-pn <ポート番号>`	管理サーバーへの暗号化されていない接続が確立されるポートの番号。 既定のポート番号は 14000 です。
`-ps <SSL ポート番号>`	SSL を使用した管理サーバーへの暗号化接続の確立に使用する SSL ポートの番号。 既定のポート番号は 13000 です。
`-nossl`	管理サーバーへの暗号化されていない接続を使用します。 このキーを使用しない場合、ネットワークエージェントは暗号化された SSL プロトコルを使用して管理サーバーに接続されます。
`-cert <証明書ファイルのパス>`	管理サーバーへのアクセス認証で使用する証明書ファイル。
`-virtserv`	仮想管理サーバー名。
`-cloningmode`	ネットワークエージェントのディスククローンモード。 次のパラメーターのいずれかを使用して、ディスクのクローンモードを構成します。 • `-cloningmode`：ディスククローンモードのステータスを要求します。 • `-cloningmode 1`：ディスククローンモードをオンにします。 • `-cloningmode 0`：ディスククローンモードをオフにします。

たとえば、ネットワークエージェントを管理サーバーに接続するには、次のコマンドを実行します。

```
klmover - アドレス kscserver.mycompany.com - ログファイル klmover.log
```

Web サーバー証明書の再発行

Kaspersky Security Center で使用される Web サーバー証明書は、後で管理対象デバイスにダウンロードするネットワークエージェントインストールパッケージの公開、および iOS MDM プロファイル、iOS アプリ、Kaspersky Endpoint Security forMobile インストールパッケージの公開に必要です。現在のアプリケーション設定に応じて、様々な証明書を Web サーバー証明書として機能させることができます（詳細については、Kaspersky Security Center 証明書についてを参照してください）。

アプリケーションのアップグレードを開始する前に、組織の特定のセキュリティ要件を満たすため、または管理対象デバイスの常時接続を維持するために、Web サーバー証明書を再発行する必要があります。Kaspersky Security Center では、Web サーバー証明書の再発行には 2 つの方法が用意されています。どちらを選択するかは、モバイルプロトコルを介して（つまり、モバイル証明書を使用して）モバイルデバイスを接続および管理しているかどうかによって異なります。

管理サーバーのプロパティウィンドウの［**Web サーバー**］セクションで独自のカスタム証明書を Web サーバー証明書として指定していなければ、モバイル証明書が Web サーバー証明書として機能します。この場合、Web サーバー証明書の再発行は、モバイルプロトコル自体の再発行を通じて行われます。

モバイルプロトコルを介して管理されているモバイルデバイスがない場合に Web サーバー証明書を再発行するには：

1. コンソールツリーで、該当する管理サーバーの名前を右クリックし、コンテキストメニューで［**プロパティ**］を選択します。
2. 管理サーバーのプロパティウィンドウが表示されるので、左側のペインで［**管理サーバー接続設定**］セクションを選択します。
3. サブセクションのリストで［**証明書**］サブセクションを選択します。
4. Kaspersky Security Center によって発行された証明書を引き続き使用する場合は、次の手順を実行します：
   a. 右側のペインの［**モバイルデバイスによる管理サーバー認証**］で、［**管理サーバーを使用して発行された証明書**］を選択し、［**再発行**］をクリックします。
   b. ［**証明書を再発行する**］が表示されるので、［**接続アドレス**］および［**アクティベーション期間**］で関連するオプションを選択し、［**OK**］をクリックします。
   c. 確認メッセージが表示されたら、［**はい**］をクリックします。

   または、独自のカスタム証明書を使用する場合は、次の手順を実行します：
   a. カスタム証明書が Kaspersky Security Center の要件および Apple による信頼済み証明書の要件を満たしているかどうかを確認します。必要に応じて、証明書を変更します。
   b. ［**その他の証明書**］を選択して、［**参照**］をクリックします。
   c. ［**証明書**］ウィンドウが表示されるので、［**証明書の種別**］で証明書の種類を選択して、証明書の場所と設定を指定します。
      - ［**PKCS #12 コンテナー**］を選択した場合、［**証明書ファイル**］の横の［**参照**］をクリックし、ハードディスク上の証明書ファイルを指定します。証明書ファイルがパスワードで保護されている場合は、［**パスワード（存在する場合）**］にパスワードを入力します。
      - ［**X.509 証明書**］を選択した場合、［**秘密鍵 (.prk, .pem)**］の横の［**参照**］をクリックし、ハードディスク上の秘密鍵を指定します。秘密鍵がパスワードで保護されている場合は、［**パスワード（存在する場合）**］にパスワードを入力します。次に、［**公開鍵 (.cer)**］の横の［**参照**］をクリックして、ハードディスク上の秘密鍵を指定します。

d. ［**証明書**］ウィンドウで、［**OK**］をクリックします。

e. 確認メッセージが表示されたら、［**はい**］をクリックします。

モバイル証明書が再発行され、Web サーバー証明書として使用できます。

モバイルプロトコルを介して管理されているモバイルデバイスがある場合に Web サーバー証明書を再発行するには：

1. カスタム証明書を生成し、Kaspersky Security Center で使用できるように準備します。カスタム証明書が Kaspersky Security Center の要件および Apple による信頼済み証明書の要件を満たしているかどうかを確認します。必要に応じて、証明書を変更します。

   kliossrvcertgen.exe ユーティリティを使用して証明書を生成できます。

2. コンソールツリーで、該当する管理サーバーの名前を右クリックし、コンテキストメニューで［**プロパティ**］を選択します。

3. 表示される管理サーバーのプロパティウィンドウの左側のペインで［**Web サーバー**］セクションを選択します。

4. ［**HTTPS 経由**］メニューで、［**他の証明書を指定する**］を選択します。

5. ［**HTTPS 経由**］メニューで、［**変更**］をクリックします。

6. ［**証明書**］が表示されるので、［**証明書の種別**］で証明書のタイプを選択します。

   - ［**PKCS #12 コンテナー**］を選択した場合、［**証明書ファイル**］の横の［**参照**］をクリックし、ハードディスク上の証明書ファイルを指定します。証明書ファイルがパスワードで保護されている場合は、［**パスワード（存在する場合）**］にパスワードを入力します。

   - ［**X.509 証明書**］を選択した場合、［**秘密鍵 (.prk, .pem)**］の横の［**参照**］をクリックし、ハードディスク上の秘密鍵を指定します。秘密鍵がパスワードで保護されている場合は、［**パスワード（存在する場合）**］にパスワードを入力します。次に、［**公開鍵 (.cer)**］の横の［**参照**］をクリックして、ハードディスク上の秘密鍵を指定します。

7. ［**証明書**］ウィンドウで、［**OK**］をクリックします。

8. 必要に応じて、管理サーバーのプロパティウィンドウの［**Web サーバーの HTTPS ポート**］で、Web サーバーの HTTPS ポートの番号を変更します。［**OK**］をクリックします。

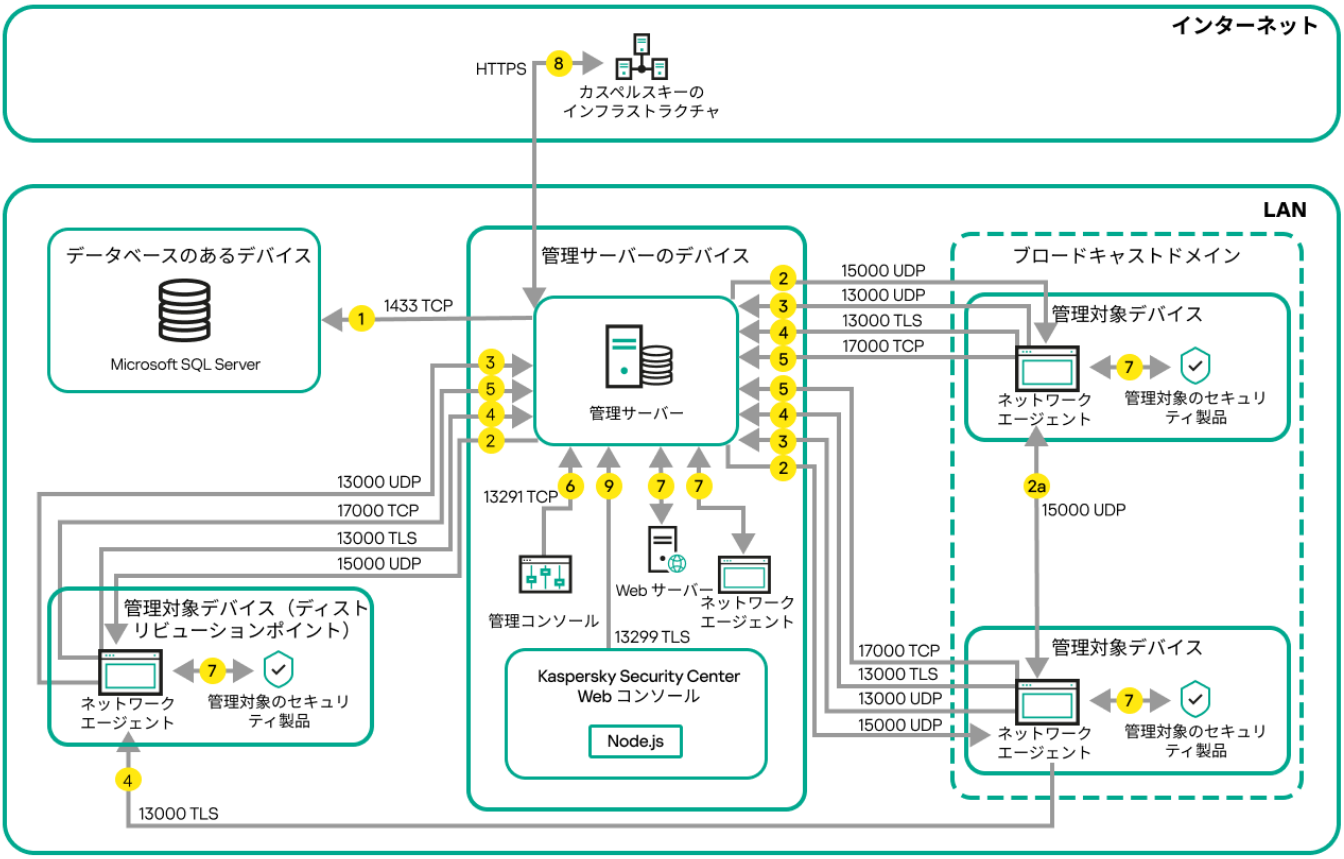
   Web サーバー証明書が再発行されます。

データトラフィックの流れと使用ポートの図解

このセクションでは、Kaspersky Security Center コンポーネント、セキュリティ製品、外部サーバーの構成に応じて、データトラフィックの流れを図解したスキーマを掲載しています。スキーマには、ローカルデバイスで利用可能になっている必要のあるポートの番号も記載されています。

LAN 内に管理サーバーと管理対象デバイスがある構成

次の図は、Kaspersky Security Center を LAN（ローカルエリアネットワーク）内に限定して導入した場合のデータトラフィックの流れを示しています。



LAN（ローカルエリアネットワーク）内に管理サーバーと管理対象デバイスがある構成

この図には複数の管理対象デバイスが存在し、管理サーバーに直接またはディストリビューションポイントを経由して接続しています。ディストリビューションポイントを利用することで、アップデート配信時の管理サーバーの負荷を軽減し、ネットワークトラフィックを最適化できます。ただし、ディストリビューションポイントは管理対象デバイスの数が一定数以上の場合にのみ必要です。管理対象デバイスの数が少ない場合、すべての管理対象デバイスは管理サーバーから直接アップデートを取得できます。

矢印の向きはトラフィックの流れを示しており、接続を開始するデバイスから接続要求に応答するデバイスに向けて矢印が引かれています。矢印の線に添えて、データの転送に使用されたポートの番号とプロトコルが示されています。また、矢印には黄色の丸数字が添えられています。それぞれのデータトラフィックの内容について詳しくは、各数字に対応する次の説明を参照してください：

1. 管理サーバーがデータベースにデータを送信します。管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MySQL Server 用のポート 3306、または Microsoft SQL Server 用のポート 1433 など）。関連する情報については、DBMS のドキュメントを参照してください。

2. 管理サーバーからの通信リクエストは、モバイルデバイス以外のすべての管理対象デバイスに対して UDP ポート 15000 で送信されます。

   ネットワークエージェントは、1つのブロードキャストドメイン内で相互にリクエストを送信します。その後、データは管理サーバーに送信され、ブロードキャストドメインの制限の定義およびディストリビューションポイントの自動割り当てに使用されます（このオプションが有効な場合）。

   管理サーバーが管理対象デバイスに直接アクセスできない場合、管理サーバーからこれらのデバイスへの通信リクエストは直接送信されません。

3. 管理対象デバイスのシャットダウンに関する情報は UDP ポート 13000 でネットワークエージェントから管理サーバーに転送されます。

4. ネットワークエージェントとセカンダリ管理サーバーから管理サーバーへの接続は TLS ポート 13000 で受信します。

   Kaspersky Security Center の以前のバージョンを使用している場合、ネットワーク上の管理サーバーがネットワークエージェントからの接続を非 TLS のポート 14000 で受信する場合があります。Kaspersky Security Center もポート 14000 を使用したネットワークエージェントとの接続をサポートしていますが、TLS ポート 13000 の使用が推奨されます。

   > ディストリビューションポイントは、以前のバージョンの Kaspersky Security Center では「アップデートエージェント」と呼ばれていました。

5. 管理対象デバイス（モバイルデバイス以外）は TCP ポート 17000 でアクティベーションを要求します。管理対象デバイスがインターネットに接続できる環境にある場合、デバイスはインターネット経由でカスペルスキーのサーバーに直接データを送信するので、このポートでの通信は必要ありません。

6. MMC ベースの管理コンソールからのデータは、ポート 13291 を介して転送されます（管理コンソールは、同じデバイスにも違うデバイスにもインストールが可能です）。

7. 1 台のデバイス内でのアプリケーション間でのデータ交換（管理サーバー内、または管理対象デバイス内）。このデータの流れに対して外部ポートを開く必要はありません。

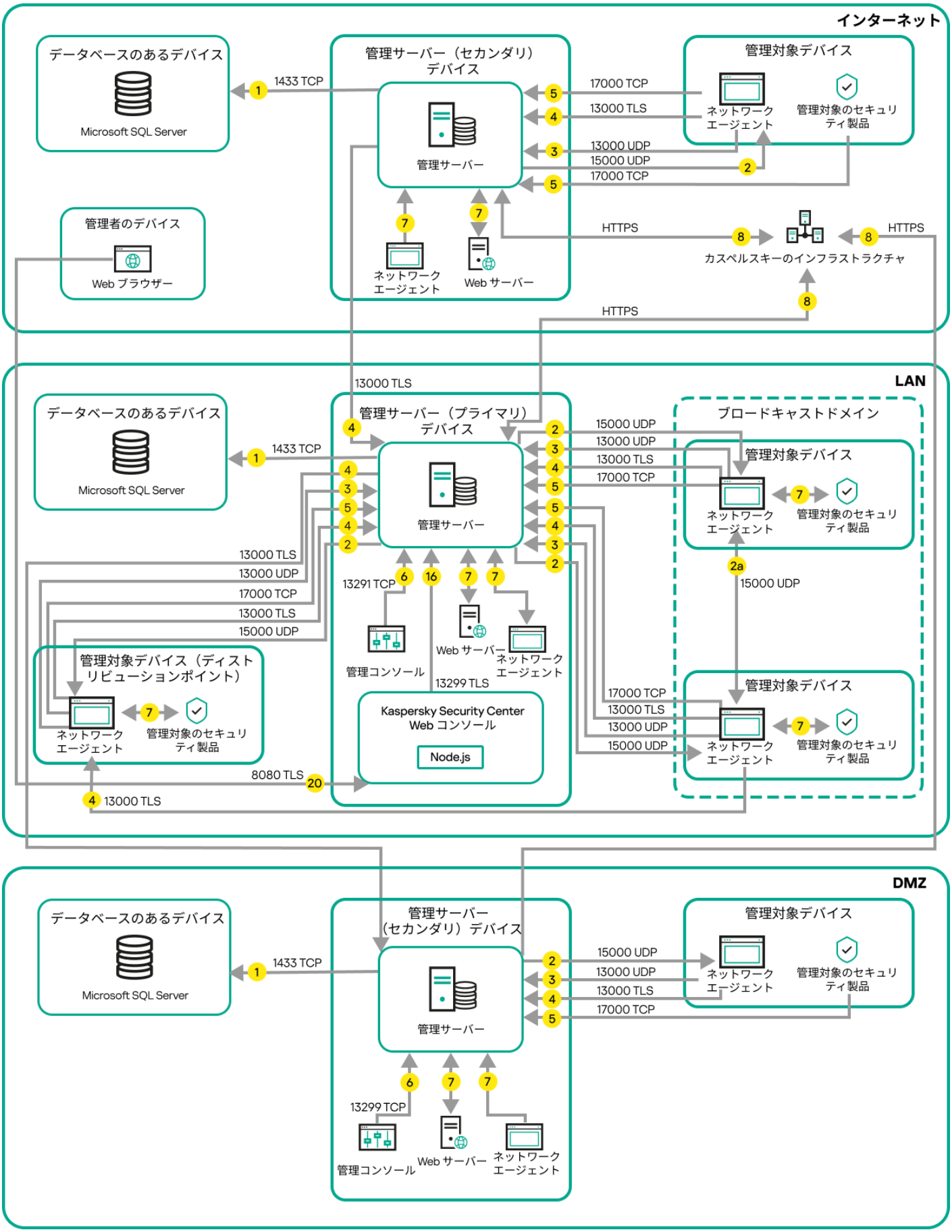
8. KSN データやライセンスに関する情報などの管理サーバーからカスペルスキーのサーバーへのデータの送信、および製品アップデートや定義データベースアップデートなどのカスペルスキーのサーバーから管理サーバーへのデータの送信には、HTTPS プロトコルが使用されます。

   管理サーバーをインターネットに接続しない場合、これらのデータを手動でやり取りする必要があります。

9. Kaspersky Security Center Web コンソールサーバーと管理デバイスは同じデバイスまたは別々のデバイスにインストールすることができますが、異なるデバイスにインストールした場合、Web コンソールは管理サーバーに TLS ポート 13299 でデータを送信します。

プライマリ管理サーバーが LAN 内にありセカンダリ管理サーバーが 2 台ある構成

次の図は、管理サーバーの階層構造の例を示しています。プライマリ管理サーバーがローカルエリアネットワーク（LAN）内にあります。セカンダリ管理サーバーのうち 1 台は DMZ 内にあります。もう 1 台のセカンダリ管理サーバーとはインターネット経由で接続しています。



管理サーバーの階層構造：プライマリ管理サーバーと 2 台のセカンダリ管理サーバー

矢印の向きはトラフィックの流れを示しており、接続を開始するデバイスから接続要求に応答するデバイスに向けて矢印が引かれています。矢印の線に添えて、データの転送に使用されたポートの番号とプロトコルが示されています。また、矢印には黄色の丸数字が添えられています。それぞれのデータトラフィックの内容について詳しくは、各数字に対応する次の説明を参照してください：

1. 管理サーバーがデータベースにデータを送信します。管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MySQL Server 用のポート 3306、または Microsoft SQL Server 用のポート 1433 など）。関連する情報については、DBMS のドキュメントを参照してください。

2. 管理サーバーからの通信リクエストは、モバイルデバイス以外のすべての管理対象デバイスに対して UDP ポート 15000 で送信されます。

   ネットワークエージェントは、1 つのブロードキャストドメイン内で相互にリクエストを送信します。その後、データは管理サーバーに送信され、ブロードキャストドメインの制限の定義およびディストリビューションポイントの自動割り当てに使用されます（このオプションが有効な場合）。

   管理サーバーが管理対象デバイスに直接アクセスできない場合、管理サーバーからこれらのデバイスへの通信リクエストは直接送信されません。

3. 管理対象デバイスのシャットダウンに関する情報は UDP ポート 13000 でネットワークエージェントから管理サーバーに転送されます。

4. ネットワークエージェントとセカンダリ管理サーバーから管理サーバーへの接続は TLS ポート 13000 で受信します。

   Kaspersky Security Center の以前のバージョンを使用している場合、ネットワーク上の管理サーバーがネットワークエージェントからの接続を非 TLS のポート 14000 で受信する場合があります。Kaspersky Security Center もポート 14000 を使用したネットワークエージェントとの接続をサポートしていますが、TLS ポート 13000 の使用が推奨されます。

   > ディストリビューションポイントは、以前のバージョンの Kaspersky Security Center では「アップデートエージェント」と呼ばれていました。

5. 管理対象デバイス（モバイルデバイス以外）は TCP ポート 17000 でアクティベーションを要求します。管理対象デバイスがインターネットに接続できる環境にある場合、デバイスはインターネット経由でカスペルスキーのサーバーに直接データを送信するので、このポートでの通信は必要ありません。

6. MMC ベースの管理コンソールからのデータは、ポート 13291 を介して転送されます（管理コンソールは、同じデバイスにも違うデバイスにもインストールが可能です）。

7. 1 台のデバイス内でのアプリケーション間でのデータ交換（管理サーバー内、または管理対象デバイス内）。このデータの流れに対して外部ポートを開く必要はありません。

8. KSN データやライセンスに関する情報などの管理サーバーからカスペルスキーのサーバーへのデータの送信、および製品アップデートや定義データベースアップデートなどのカスペルスキーのサーバーから管理サーバーへのデータの送信には、HTTPS プロトコルが使用されます。

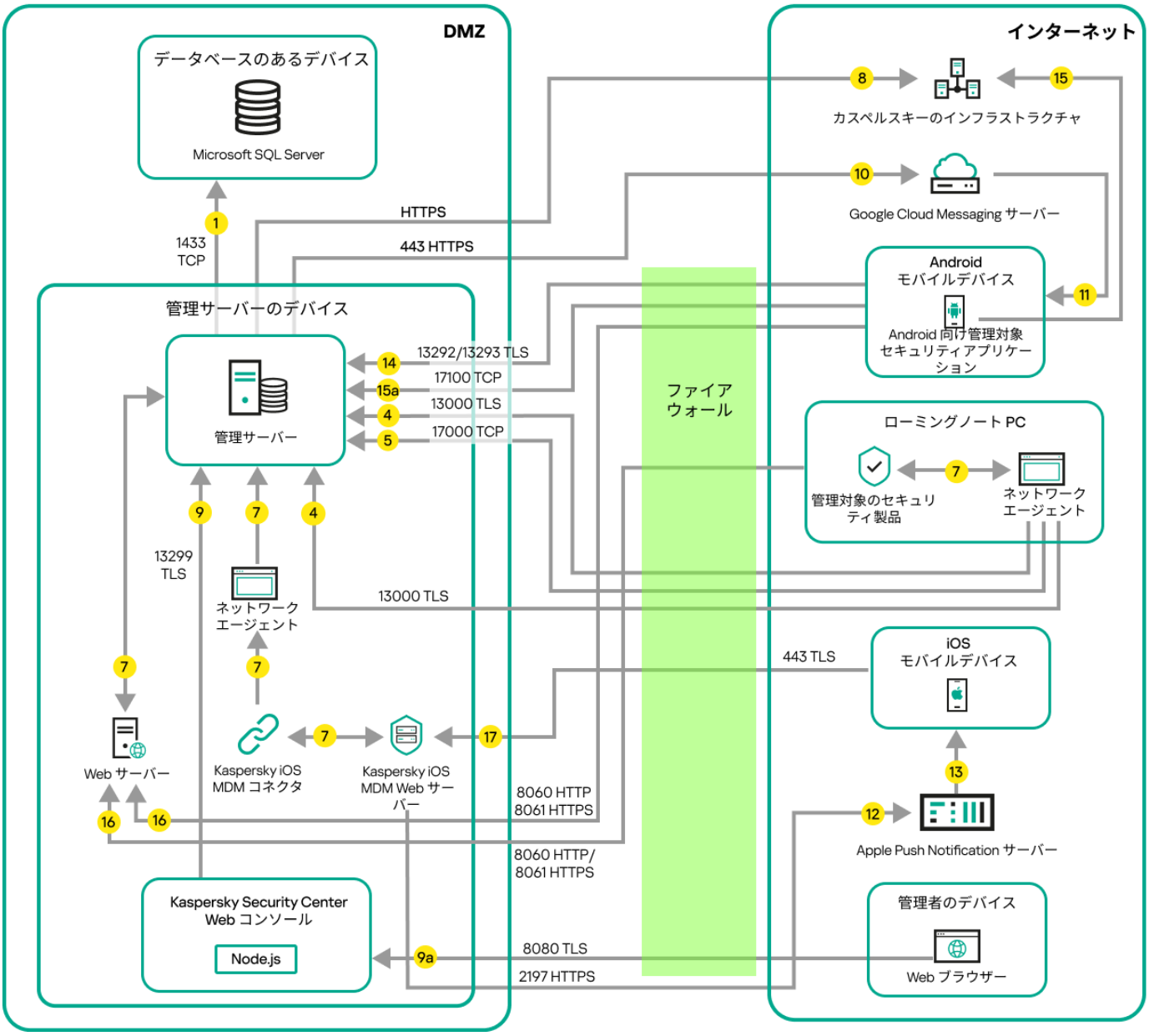
   管理サーバーをインターネットに接続しない場合、これらのデータを手動でやり取りする必要があります。

9. Kaspersky Security Center Web コンソールと管理デバイスは同じデバイスまたは別々のデバイスにインストールすることができますが、異なるデバイスにインストールした場合、Web コンソールは管理サーバーに TLS ポート 13299 でデータを送信します。

   9a.（Web コンソールがインストールされているのとは異なる）管理者用のデバイスにインストールされている Web ブラウザーからのデータは、Kaspersky Security Center Web コンソールサーバーに TLS 8080 ポートで送信されます。Kaspersky Security Center Web コンソールサーバーは管理サーバーと同じデバイスにインストールすることも、別のデバイスにインストールすることもできます。

管理サーバーが LAN 内にありインターネット経由で管理対象デバイスに接続している構成（リバースプロキシを使用）

次の図は、管理サーバーがローカルエリアネットワーク（LAN）内にありモバイルデバイスを含む管理対象デバイスにインターネット経由で接続している場合のデータトラフィックの流れを示しています。この図では、任意に選択したリバースプロキシが使用されています。詳細については、製品のドキュメントを参照してください。



ローカルエリアネットワーク上の管理対象デバイスはリバースプロキシ経由で管理サーバーに接続されています

モバイルデバイスが管理サーバーに直接接続しないように構成し、なおかつ DMZ 内に接続ゲートウェイを割り当てない場合は、この構成での導入が推奨されます。

矢印の向きはトラフィックの流れを示しており、接続を開始するデバイスから接続要求に応答するデバイスに向けて矢印が引かれています。矢印の線に添えて、データの転送に使用されたポートの番号とプロトコルが示されています。また、矢印には黄色の丸数字が添えられています。それぞれのデータトラフィックの内容について詳しくは、各数字に対応する次の説明を参照してください：

1. 管理サーバーがデータベースにデータを送信します。管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MySQL Server 用のポート 3306、または Microsoft SQL Server 用のポート 1433 など）。関連する情報については、DBMS のドキュメントを参照してください。

2. 管理サーバーからの通信リクエストは、モバイルデバイス以外のすべての管理対象デバイスに対して UDP ポート 15000 で送信されます。

   ネットワークエージェントは、1 つのブロードキャストドメイン内で相互にリクエストを送信します。その後、データは管理サーバーに送信され、ブロードキャストドメインの制限の定義およびディストリビューションポイントの自動割り当てに使用されます（このオプションが有効な場合）。

   管理サーバーが管理対象デバイスに直接アクセスできない場合、管理サーバーからこれらのデバイスへの通信リクエストは直接送信されません。

3. 管理対象デバイスのシャットダウンに関する情報は UDP ポート 13000 でネットワークエージェントから管理サーバーに転送されます。

4. ネットワークエージェントとセカンダリ管理サーバーから管理サーバーへの接続は TLS ポート 13000 で受信します。

   Kaspersky Security Center の以前のバージョンを使用している場合、ネットワーク上の管理サーバーがネットワークエージェントからの接続を非 TLS のポート 14000 で受信する場合があります。Kaspersky Security Center もポート 14000 を使用したネットワークエージェントとの接続をサポートしていますが、TLS ポート 13000 の使用が推奨されます。

   > ディストリビューションポイントは、以前のバージョンの Kaspersky Security Center では「アップデートエージェント」と呼ばれていました。

5. 管理対象デバイス（モバイルデバイス以外）は TCP ポート 17000 でアクティベーションを要求します。管理対象デバイスがインターネットに接続できる環境にある場合、デバイスはインターネット経由でカスペルスキーのサーバーに直接データを送信するので、このポートでの通信は必要ありません。

6. MMC ベースの管理コンソールからのデータは、ポート 13291 を介して転送されます（管理コンソールは、同じデバイスにも違うデバイスにもインストールが可能です）。

7. 1 台のデバイス内でのアプリケーション間でのデータ交換（管理サーバー内、または管理対象デバイス内）。このデータの流れに対して外部ポートを開く必要はありません。

8. KSN データやライセンスに関する情報などの管理サーバーからカスペルスキーのサーバーへのデータの送信、および製品アップデートや定義データベースアップデートなどのカスペルスキーのサーバーから管理サーバーへのデータの送信には、HTTPS プロトコルが使用されます。

   管理サーバーをインターネットに接続しない場合、これらのデータを手動でやり取りする必要があります。

9. Kaspersky Security Center Web コンソールと管理デバイスは同じデバイスまたは別々のデバイスにインストールすることができますが、異なるデバイスにインストールした場合、Web コンソールは管理サーバーに TLS ポート 13299 でデータを送信します。

   9a.（Web コンソールがインストールされているのとは異なる）管理者用のデバイスにインストールされている Web ブラウザーからのデータは、Kaspersky Security Center Web コンソールサーバーに TLS 8080 ポートで送信されます。Kaspersky Security Center Web コンソールサーバーは管理サーバーと同じデバイスにインストールすることも、別のデバイスにインストールすることもできます。

10. Android モバイルデバイスのみ：管理サーバーから Google のサーバーへのトラフィック。この接続は、Android モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。これにより、モバイルデバイスへのプッシュ通知が送信されます。

11. Android モバイルデバイスのみ：Google のサーバーからモバイルデバイスへのプッシュ通知の送信。この接続は、モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。

12. iOS モバイルデバイスのみ：iOS MDM サーバーから Apple のプッシュ通知サーバーへのデータ送信。これにより、モバイルデバイスへのプッシュ通知が送信されます。

13. iOS モバイルデバイスのみ：Apple のサーバーからモバイルデバイスへのプッシュ通知。この接続は、iOS モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。

14. モバイルデバイスのみ：管理対象アプリケーションは、管理サーバー（または接続ゲートウェイ）に TLS ポート 13292 / 13293 でデータを送信します（直接またはリバースプロキシ経由）。

15. モバイルデバイスのみ：モバイルデバイスからカスペルスキーのサーバーへのデータ送信。

    モバイルデバイスがインターネットに接続されていない場合、データはポート 17100 で管理サーバーに送信され、それから管理サーバーがカスペルスキーのサーバーにデータを送信します。ただし、こうした状況が実際に発生する頻度はそれほど高くありません。

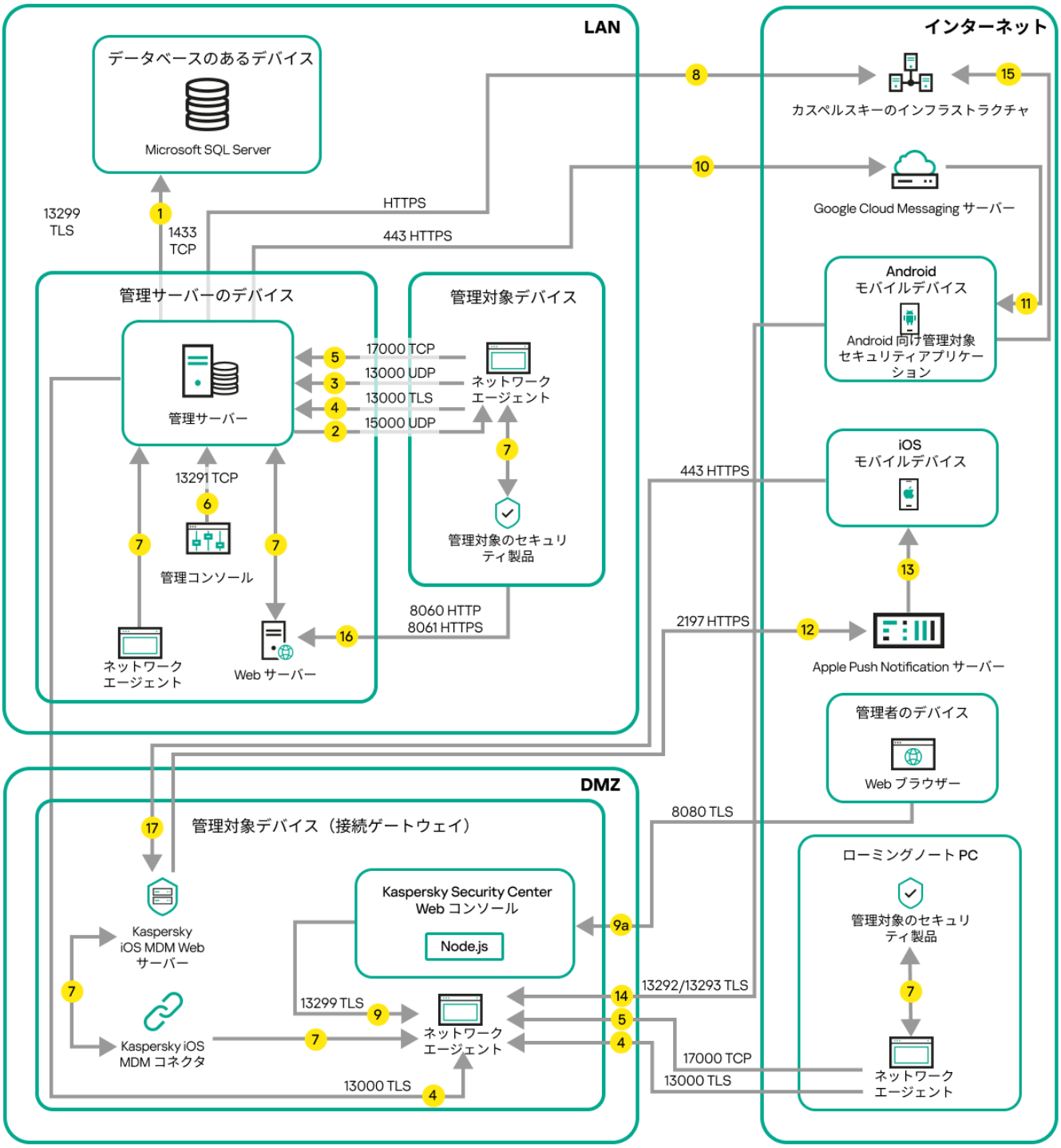
16. モバイルデバイスを含む管理対象デバイスから、管理サーバーと同じデバイス上の Web サーバーへのパッケージ要求の送信。

17. iOS モバイルデバイスのみ：モバイルデバイスは、管理サーバーまたは接続ゲートウェイと同じデバイス上の iOS MDM サーバーに TLS ポート 443 でデータを送信します。

管理サーバーが LAN 内にありインターネット経由で管理対象デバイスに接続している構成（接続ゲートウェイを使用）

次の図は、管理サーバーがローカルエリアネットワーク（LAN）内にありモバイルデバイスを含む管理対象デバイスにインターネット経由で接続している場合のデータトラフィックの流れを示しています。接続ゲートウェイが使用されています。

この導入方式は、モバイルデバイスを直接管理サーバーへ接続せず、リバースプロキシや企業ファイアウォールを使用したくない場合に推奨されます。



接続ゲートウェイを使用して管理サーバーに接続する管理対象のモバイルデバイス

この図では、管理対象デバイスは DMZ 内にある接続ゲートウェイを経由して管理サーバーに接続しています。リバースプロキシや企業ファイアウォールは使用されていません。

矢印の向きはトラフィックの流れを示しており、接続を開始するデバイスから接続要求に応答するデバイスに向けて矢印が引かれています。矢印の線に添えて、データの転送に使用されたポートの番号とプロトコルが示されています。また、矢印には黄色の丸数字が添えられています。それぞれのデータトラフィックの内容について詳しくは、各数字に対応する次の説明を参照してください：

1. 管理サーバーがデータベースにデータを送信します。管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MySQL Server 用のポート 3306、または Microsoft SQL Server 用のポート 1433 など）。関連する情報については、DBMS のドキュメントを参照してください。

2. 管理サーバーからの通信リクエストは、モバイルデバイス以外のすべての管理対象デバイスに対して UDP ポート 15000 で送信されます。

   ネットワークエージェントは、1 つのブロードキャストドメイン内で相互にリクエストを送信します。その後、データは管理サーバーに送信され、ブロードキャストドメインの制限の定義およびディストリビューションポイントの自動割り当てに使用されます（このオプションが有効な場合）。

   管理サーバーが管理対象デバイスに直接アクセスできない場合、管理サーバーからこれらのデバイスへの通信リクエストは直接送信されません。

3. 管理対象デバイスのシャットダウンに関する情報は UDP ポート 13000 でネットワークエージェントから管理サーバーに転送されます。

4. ネットワークエージェントとセカンダリ管理サーバーから管理サーバーへの接続は TLS ポート 13000 で受信します。

   Kaspersky Security Center の以前のバージョンを使用している場合、ネットワーク上の管理サーバーがネットワークエージェントからの接続を非 TLS のポート 14000 で受信する場合があります。Kaspersky Security Center もポート 14000 を使用したネットワークエージェントとの接続をサポートしていますが、TLS ポート 13000 の使用が推奨されます。

   > ディストリビューションポイントは、以前のバージョンの Kaspersky Security Center では「アップデートエージェント」と呼ばれていました。

   4a.DMZ 内の接続ゲートウェイは、TLS ポート 13000 を使用して管理サーバーからの接続も受信します。DMZ 内の接続ゲートウェイは管理サーバーのポートに到達できないため、管理サーバーは接続ゲートウェイとの永続的な信号接続を作成して維持します。信号接続はデータ転送には使用されません。これは、ネットワーク対話への招待の送信にのみ使用されます。接続ゲートウェイがサーバーに接続する必要がある場合、接続ゲートウェイはこの信号接続を介してサーバーに通知し、サーバーはデータ転送に必要な接続を作成します。

   社外のデバイスも同様に、TLS ポート 13000 を通じて接続ゲートウェイに接続します。

5. 管理対象デバイス（モバイルデバイス以外）は TCP ポート 17000 でアクティベーションを要求します。管理対象デバイスがインターネットに接続できる環境にある場合、デバイスはインターネット経由でカスペルスキーのサーバーに直接データを送信するので、このポートでの通信は必要ありません。

6. MMC ベースの管理コンソールからのデータは、ポート 13291 を介して転送されます（管理コンソールは、同じデバイスにも違うデバイスにもインストールが可能です）。

7. 1 台のデバイス内でのアプリケーション間でのデータ交換（管理サーバー内、または管理対象デバイス内）。このデータの流れに対して外部ポートを開く必要はありません。

8. KSN データやライセンスに関する情報などの管理サーバーからカスペルスキーのサーバーへのデータの送信、および製品アップデートや定義データベースアップデートなどのカスペルスキーのサーバーから管理サーバーへのデータの送信には、HTTPS プロトコルが使用されます。

   管理サーバーをインターネットに接続しない場合、これらのデータを手動でやり取りする必要があります。

9. Kaspersky Security Center Web コンソールと管理デバイスは同じデバイスまたは別々のデバイスにインストールすることができますが、異なるデバイスにインストールした場合、Web コンソールは管理サーバーに TLS ポート 13299 でデータを送信します。

   9a.（Web コンソールがインストールされているのとは異なる）管理者用のデバイスにインストールされている Web ブラウザーからのデータは、Kaspersky Security Center Web コンソールサーバーに TLS 8080 ポートで送信されます。Kaspersky Security Center Web コンソールサーバーは管理サーバーと同じデバイスにインストールすることも、別のデバイスにインストールすることもできます。

10. Android モバイルデバイスのみ：管理サーバーから Google のサーバーへのトラフィック。この接続は、Android モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。これにより、モバイルデバイスへのプッシュ通知が送信されます。

11. Android モバイルデバイスのみ：Google のサーバーからモバイルデバイスへのプッシュ通知の送信。この接続は、モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。

12. iOS モバイルデバイスのみ：iOS MDM サーバーから Apple のプッシュ通知サーバーへのデータ送信。これにより、モバイルデバイスへのプッシュ通知が送信されます。

13. iOS モバイルデバイスのみ：Apple のサーバーからモバイルデバイスへのプッシュ通知。この接続は、iOS モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。

14. モバイルデバイスのみ：管理対象アプリケーションは、管理サーバー（または接続ゲートウェイ）に TLS ポート 13292 / 13293 でデータを送信します（直接またはリバースプロキシ経由）。

15. モバイルデバイスのみ：モバイルデバイスからカスペルスキーのサーバーへのデータ送信。

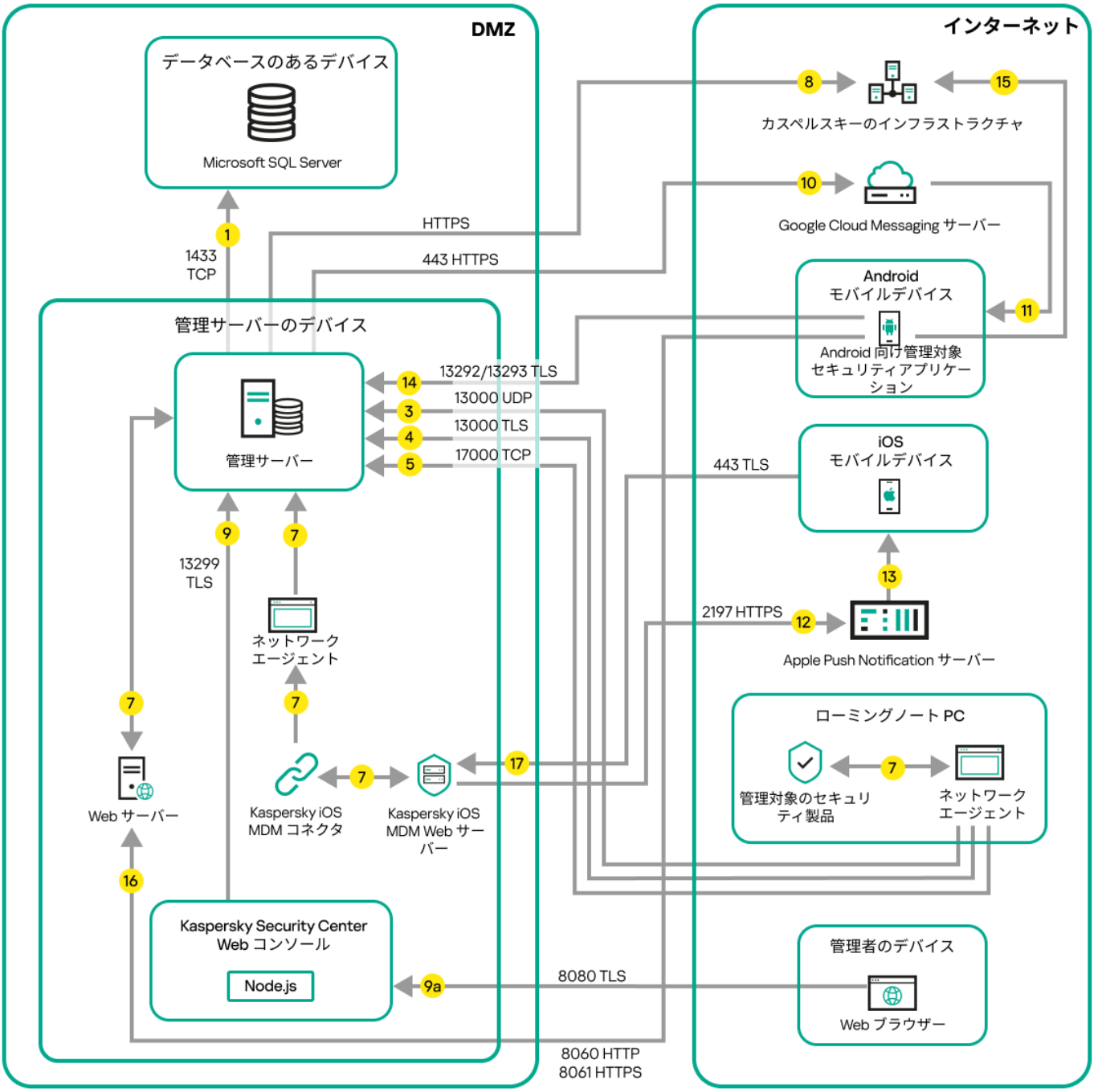
    モバイルデバイスがインターネットに接続されていない場合、データはポート 17100 で管理サーバーに送信され、それから管理サーバーがカスペルスキーのサーバーにデータを送信します。ただし、こうした状況が実際に発生する頻度はそれほど高くありません。

16. モバイルデバイスを含む管理対象デバイスから、管理サーバーと同じデバイス上の Web サーバーへのパッケージ要求の送信。

17. iOS モバイルデバイスのみ：モバイルデバイスは、管理サーバーまたは接続ゲートウェイと同じデバイス上の iOS MDM サーバーに TLS ポート 443 でデータを送信します。

管理サーバーが DMZ 内にありインターネット経由で管理対象デバイスに接続している構成

次の図は、管理サーバーが DMZ（非武装地帯）内にありモバイルデバイスを含む管理対象デバイスにインターネット経由で接続している場合のデータトラフィックの流れを示しています。



管理サーバーが DMZ 内にありインターネット経由で管理対象のモバイルデバイスに接続している構成

この図の構成では、接続ゲートウェイは使用されておらず、モバイルデバイスが管理サーバーに直接接続されています。

矢印の向きはトラフィックの流れを示しており、接続を開始するデバイスから接続要求に応答するデバイスに向けて矢印が引かれています。矢印の線に添えて、データの転送に使用されたポートの番号とプロトコルが示されています。また、矢印には黄色の丸数字が添えられています。それぞれのデータトラフィックの内容について詳しくは、各数字に対応する次の説明を参照してください：

1. 管理サーバーがデータベースにデータを送信します。管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MySQL Server 用のポート 3306、または Microsoft SQL Server 用のポート 1433 など）。関連する情報については、DBMS のドキュメントを参照してください。

2. 管理サーバーからの通信リクエストは、モバイルデバイス以外のすべての管理対象デバイスに対して UDP ポート 15000 で送信されます。

ネットワークエージェントは、1つのブロードキャストドメイン内で相互にリクエストを送信します。その後、データは管理サーバーに送信され、ブロードキャストドメインの制限の定義およびディストリビューションポイントの自動割り当てに使用されます（このオプションが有効な場合）。

管理サーバーが管理対象デバイスに直接アクセスできない場合、管理サーバーからこれらのデバイスへの通信リクエストは直接送信されません。

3. 管理対象デバイスのシャットダウンに関する情報は UDP ポート 13000 でネットワークエージェントから管理サーバーに転送されます。

4. ネットワークエージェントとセカンダリ管理サーバーから管理サーバーへの接続は TLS ポート 13000 で受信します。

   Kaspersky Security Center の以前のバージョンを使用している場合、ネットワーク上の管理サーバーがネットワークエージェントからの接続を非 TLS のポート 14000 で受信する場合があります。Kaspersky Security Center もポート 14000 を使用したネットワークエージェントとの接続をサポートしていますが、TLS ポート 13000 の使用が推奨されます。

   > ディストリビューションポイントは、以前のバージョンの Kaspersky Security Center では「アップデートエージェント」と呼ばれていました。

5. 管理対象デバイス（モバイルデバイス以外）は TCP ポート 17000 でアクティベーションを要求します。管理対象デバイスがインターネットに接続できる環境にある場合、デバイスはインターネット経由でカスペルスキーのサーバーに直接データを送信するので、このポートでの通信は必要ありません。

6. MMC ベースの管理コンソールからのデータは、ポート 13291 を介して転送されます（管理コンソールは、同じデバイスにも違うデバイスにもインストールが可能です）。

7. 1台のデバイス内でのアプリケーション間でのデータ交換（管理サーバー内、または管理対象デバイス内）。このデータの流れに対して外部ポートを開く必要はありません。

8. KSN データやライセンスに関する情報などの管理サーバーからカスペルスキーのサーバーへのデータの送信、および製品アップデートや定義データベースアップデートなどのカスペルスキーのサーバーから管理サーバーへのデータの送信には、HTTPS プロトコルが使用されます。

   管理サーバーをインターネットに接続しない場合、これらのデータを手動でやり取りする必要があります。

9. Kaspersky Security Center Web コンソールと管理デバイスは同じデバイスまたは別々のデバイスにインストールすることができますが、異なるデバイスにインストールした場合、Web コンソールは管理サーバーに TLS ポート 13299 でデータを送信します。

   9a.（Web コンソールがインストールされているのとは異なる）管理者用のデバイスにインストールされている Web ブラウザーからのデータは、Kaspersky Security Center Web コンソールサーバーに TLS 8080 ポートで送信されます。Kaspersky Security Center Web コンソールサーバーは管理サーバーと同じデバイスにインストールすることも、別のデバイスにインストールすることもできます。

10. Android モバイルデバイスのみ：管理サーバーから Google のサーバーへのトラフィック。この接続は、Android モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。これにより、モバイルデバイスへのプッシュ通知が送信されます。

11. Android モバイルデバイスのみ：Google のサーバーからモバイルデバイスへのプッシュ通知の送信。この接続は、モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。

12. iOS モバイルデバイスのみ：iOS MDM サーバーから Apple のプッシュ通知サーバーへのデータ送信。これにより、モバイルデバイスへのプッシュ通知が送信されます。

13. iOS モバイルデバイスのみ：Apple のサーバーからモバイルデバイスへのプッシュ通知。この接続は、iOS モバイルデバイスに、管理サーバーと接続する必要があることを通知するために使用されます。

14. モバイルデバイスのみ：管理対象アプリケーションは、管理サーバー（または接続ゲートウェイ）に TLS ポート 13292 / 13293 でデータを送信します（直接またはリバースプロキシ経由）。

15. モバイルデバイスのみ：モバイルデバイスからカスペルスキーのサーバーへのデータ送信。

    モバイルデバイスがインターネットに接続されていない場合、データはポート 17100 で管理サーバーに送信され、それから管理サーバーがカスペルスキーのサーバーにデータを送信します。ただし、こうした状況が実際に発生する頻度はそれほど高くありません。

16. モバイルデバイスを含む管理対象デバイスから、管理サーバーと同じデバイス上の Web サーバーへのパッケージ要求の送信。

17. iOS モバイルデバイスのみ：モバイルデバイスは、管理サーバーまたは接続ゲートウェイと同じデバイス上の iOS MDM サーバーに TLS ポート 443 でデータを送信します。

Kaspersky Security Center コンポーネントとセキュリティ製品の対話の図解

このセクションでは、Kaspersky Security Center コンポーネントと管理アプリケーションの対話スキームについて説明します。このスキームには、使用可能にする必要があるポートの番号と、それらのポートを開くプロセスの名前が含まれます。

対話スキームで使用される表記規則

下の表では、対話スキームで使用される表記規則を説明します。

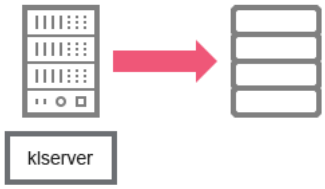
表記規則

アイコン	意味
	管理サーバー
	セカンダリ管理サーバー
	DBMS
	クライアントデバイス（ネットワークエージェントと Kaspersky Endpoint Security または Kaspersky Security Center が管理できるセキュリティ製品がインストールされているクライアントデバイス）
	接続ゲートウェイ
	ディストリビューションポイント
	Kaspersky Security for Mobile がインストールされているモバイルクライアントデバイス

	ユーザーのデバイスにあるブラウザー
klnagent	デバイスと開いているポートで実行しているプロセス
13000 TLS	ポートとポート番号
	TCP トラフィック（トラフィックの方向は矢印で示されます）
	UDP トラフィック（トラフィックの方向は矢印で示されます）
	COM の呼び出し
	DBMS トランスポート
	DMZ の境界

管理サーバーと DBMS

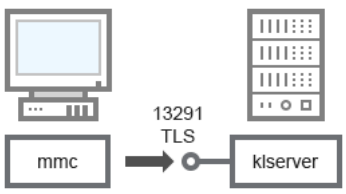
管理サーバーのデータは SQL Server、MySQL、MariaDB のいずれかのデータベースに登録されます。



管理サーバーと DBMS

管理サーバーとデータベースを異なるデバイス上にインストールする場合、データベースを配置したデバイス上で必要なポートを使用可能な状態に設定する必要があります（例：MySQL Server 用のポート 3306、または Microsoft SQL Server 用のポート 1433 など）。関連する情報については、DBMS のドキュメントを参照してください。

管理サーバーと管理コンソール



管理サーバーと管理コンソール

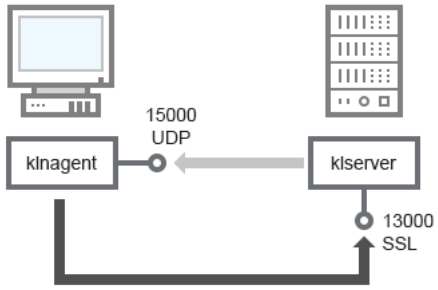
スキーマについては、下表を参照してください。

管理サーバーと管理コンソール（トラフィック）

デバイス	ポート番号	ポートを開くプロセスの名前	プロトコル	TLS	ポートの目的
管理サーバー	13291	klserver	TCP	使用する	管理コンソールから接続を受信する

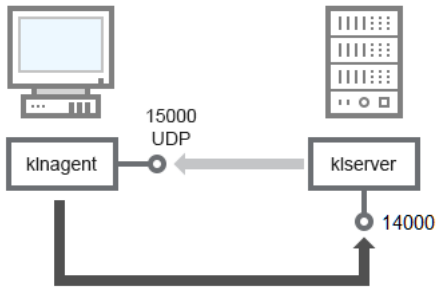
管理サーバーとクライアントデバイス：セキュリティ製品の管理

管理サーバーは、ネットワークエージェントからの接続を SSL ポート 13000 で受信します（次の図を参照）。



管理サーバーとクライアントデバイス：セキュリティ製品の管理、ポート 13000 を使用した接続（推奨）

Kaspersky Security Center の以前のバージョンを使用している場合、ネットワーク上の管理サーバーがネットワークエージェントからの接続を非 SSL ポート 14000 で受信する場合があります（次の図を参照）。Kaspersky Security Center 15.1 もポート 14000 を使用したネットワークエージェントとの接続をサポートしていますが、SSL ポート 13000 の使用が推奨されます。



管理サーバーとクライアントデバイス：セキュリティ製品の管理、ポート 14000 を使用した接続（低セキュリティ）

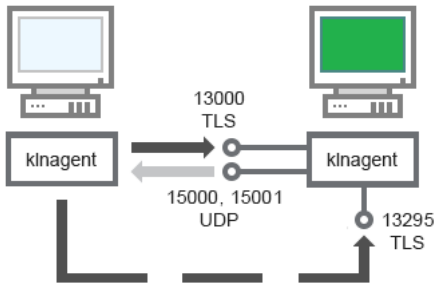
図の詳細については、次の表を参照してください。

管理サーバーとクライアントデバイス：セキュリティ製品の管理（トラフィック）

デバイス	ポート番号	ポートを開くプロセスの名前	プロトコル	TLS（TCP の場合のみ）	ポートの目的
ネットワークエージェント	15000	klnagent	UDP	Null	ネットワークエージェント用のマルチキャスト
管理サーバー	13000	klserver	TCP	使用する	ネットワークエージェントから接続を受信する
管理サーバー	14000	klserver	TCP	使用しない	ネットワークエージェントから接続を受信する

クライアントデバイスにあるソフトウェアをディストリビューションポイント経由でアップグレードする

クライアントデバイスは、ポート 13000（ディストリビューションポイントをプッシュサーバーとして使用している場合は、13295 も）を使用して、ディストリビューションポイントへ接続します。ディストリビューションポイントは、ポート 15000 を使用してネットワークエージェントへのマルチキャストを実行します（下の図を参照）。アップデートとインストールパッケージは、ポート 15001 経由でディストリビューションポイントから受信されます。



クライアントデバイスにあるソフトウェアをディストリビューションポイント経由でアップグレードする

スキーマについては、下表を参照してください。

ソフトウェアをディストリビューションポイント経由でアップグレードする（トラフィック）

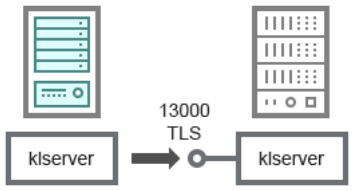
デバイス	ポート番号	ポートを開くプロセスの名前	プロトコル	TLS（TCP の場合のみ）	ポートの目的
ネットワークエージェント	15000	klnagent	UDP	Null	ネットワークエージェント用のマルチキャスト
ネットワークエージェント	15001	klnagent	UDP	Null	ディストリビューションポイントからアップデートとインストールパッケージを受信する
ディストリビューションポイント	13000	klnagent	TCP	使用する	ネットワークエージェントから接続を受信する
ディストリビューションポイント	13295	klnagent	TCP	使用する	クライアントデバイスからの接続の受信（サーバープッシュ）

管理サーバーの階層構造：プライマリ管理サーバーとセカンダリ管理サーバー

次の図は、1 つの階層にまとめられた管理サーバーがポート 13000 を使用して通信することを示しています。

2 つの管理サーバーを 1 つの階層内で組み合わせるときは、ポート 13291 が両方の管理サーバーで開放されていることを確認してください。管理コンソールから管理サーバーへの接続に、ポート 13291 を使用します。

それにより、管理サーバーを組み合わせて 1 つの階層にした時、両方の管理サーバーをプライマリ管理サーバーに接続された管理コンソールから管理できます。したがって、プライマリ管理サーバーのポート 13291 を使用できることが唯一の前提条件です。



管理サーバーの階層構造：プライマリ管理サーバーとセカンダリ管理サーバー

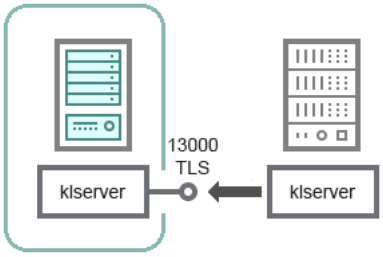
スキーマについては、下表を参照してください。

管理サーバーの階層（トラフィック）

デバイス	ポート番	ポートを開くプロセスの名	プロトコ	TLS	ポートの目的

	号	前	ル		
プライマリ管理サーバー	13000	klserver	TCP	使用する	セカンダリ管理サーバーから接続を受信する

DMZ にセカンダリ管理サーバーを持っている管理サーバーの階層構造



DMZ にセカンダリ管理サーバーを持っている管理サーバーの階層構造

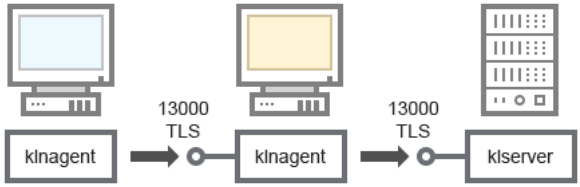
図に示す管理サーバーの階層構造では、DMZ にあるセカンダリ管理サーバーがプライマリ管理サーバーからの接続を受信します（図の詳細については次の表を参照）。2 つの管理サーバーを 1 つの階層内で組み合わせる時は、ポート 13291 が両方の管理サーバーで開放されていることを確認してください。管理コンソールから管理サーバーへの接続に、ポート 13291 を使用します。

それにより、管理サーバーを組み合わせて 1 つの階層にした時、両方の管理サーバーをプライマリ管理サーバーに接続された管理コンソールから管理できます。したがって、プライマリ管理サーバーのポート 13291 を使用できることが唯一の前提条件です。

DMZ にセカンダリ管理サーバーを持っている管理サーバーの階層構造（トラフィック）

デバイス	ポート番号	ポートを開くプロセスの名前	プロトコル	TLS	ポートの目的
セカンダリ管理サーバー	13000	klserver	TCP	使用する	プライマリ管理サーバーから接続を受信する

ネットワークセグメント内に接続ゲートウェイを持つ管理サーバーとクライアントデバイス



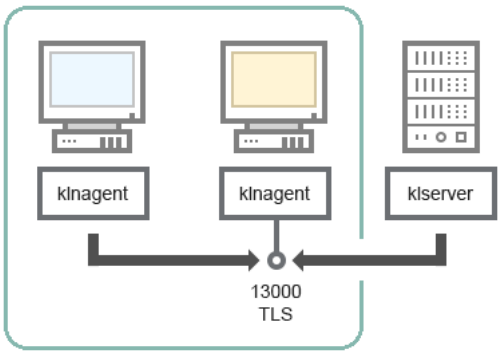
ネットワークセグメント内に接続ゲートウェイを持つ管理サーバーとクライアントデバイス

スキーマについては、下表を参照してください。

ネットワークセグメント内に接続ゲートウェイを持つ管理サーバーとクライアントデバイス（トラフィック）

デバイス	ポート番号	ポートを開くプロセスの名前	プロトコル	TLS	ポートの目的
管理サーバー	13000	klserver	TCP	使用する	ネットワークエージェントから接続を受信する
ネットワークエージェント	13000	klnagent	TCP	使用する	ネットワークエージェントから接続を受信する

DMZ に管理サーバーと 2 台のデバイス（接続ゲートウェイとクライアントデバイス）



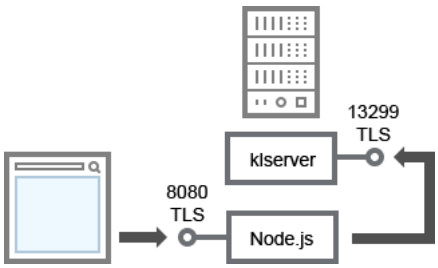
接続ゲートウェイのある管理サーバーと DMZ 内のクライアントデバイス

スキーマについては、下表を参照してください。

ネットワークセグメント内に接続ゲートウェイを持つ管理サーバーとクライアントデバイス（トラフィック）

デバイス	ポート番号	ポートを開くプロセスの名前	プロトコル	TLS	ポートの目的
ネットワークエージェント	13000	klnagent	TCP	使用する	ネットワークエージェントから接続を受信する

管理サーバーと Kaspersky Security Center Web コンソール



管理サーバーと Kaspersky Security Center Web コンソール

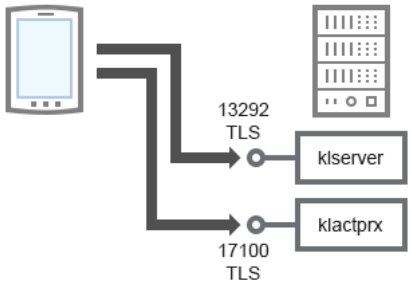
スキーマについては、下表を参照してください。

管理サーバーと Kaspersky Security Center Web コンソール（トラフィック）

デバイス	ポート番号	ポートを開くプロセスの名前	プロトコル	TLS	ポートの目的
管理サーバー	13299	klserver	TCP	使用する	Kaspersky Security Center Web コンソールから OpenAPI 経由での管理サーバーへの接続を受信する
Kaspersky Security Center Web コンソールサーバーまたは管理サーバー	8080	Node.js: Server-side JavaScript	TCP	使用する	Kaspersky Security Center Web コンソールから接続を受信する

Kaspersky Security Center Web コンソールは管理サーバーと同じデバイスにインストールすることも、別のデバイスにインストールすることもできます。

モバイルデバイス上のセキュリティソフトのアクティベーションと管理



モバイルデバイス上のセキュリティソフトのアクティベーションと管理

スキーマについては、下表を参照してください。

モバイルデバイス上のセキュリティソフトのアクティベーションと管理（トラフィック）

デバイス	ポート番号	ポートを開くプロセスの名前	プロトコル	TLS	ポートの目的
管理サーバー	13292	klserver	TCP	使用する	管理コンソールから管理サーバーへの接続を受信する
管理サーバー	17100	klactprx	TCP	使用する	モバイルデバイスから製品のアクティベーション用の接続を受信する

導入のベストプラクティス

Kaspersky Security Center は配信アプリケーションです。Kaspersky Security Center には次のアプリケーションが含まれます：

- 管理サーバー - 組織のデバイスを管理し、DBMS にデータを格納するためのコアコンポーネント。
- 管理コンソール - 管理者用の基本ツール。管理コンソールは管理サーバーに同梱されていますが、管理者が 1 台または複数台のデバイスに個別にインストールすることもできます。
- ネットワークエージェント - デバイスにインストールされているセキュリティ製品の管理、およびそのデバイスに関する情報の取得と管理サーバーへの送信を実行。組織のデバイスには、ネットワークエージェントがインストールされています。

組織ネットワークに Kaspersky Security Center を導入するには、次の作業を実行します：

- 管理サーバーのインストール
- 管理者のデバイスへの管理コンソールのインストール
- 企業のデバイスへのネットワークエージェントとセキュリティ製品のインストール

ハードニングガイド

Kaspersky Security Center は、組織のネットワークの基本的な管理と保守の一元化を目的として設計されています。本製品は、管理者が組織のネットワークセキュリティレベルに関する詳細な情報にアクセスすることを可能にします。Kaspersky Security Center では、カスペルスキー製品を使用することにより、構築されたすべての保護コンポーネントを設定することができます。

Kaspersky Security Center 管理サーバーは、クライアントデバイスの保護管理に完全にアクセスでき、組織のセキュリティシステムを構成する最も重要なコンポーネントです。そのため、管理サーバーにはより強化された保護方法が必要です。

設定する前に、管理サーバーデータのバックアップタスクまたは klbackup ユーティリティを使用して、Kaspersky Security Center 管理サーバーのバックアップコピーを作成し、安全な場所に保存してください。

ハードニングガイドでは、Kaspersky Security Center とそのコンポーネントの構成に関する推奨事項と機能について説明し、セキュリティ侵害のリスクを軽減することを目的としています。

ハードニングガイドには、次の情報が含まれています：

- 管理サーバーアーキテクチャの選択
- 管理サーバーへの安全な接続の設定
- 管理サーバーにアクセスするためのアカウントの設定
- 管理サーバーの保護管理
- クライアントデバイスの保護管理
- 管理対象アプリケーションの保護構成
- 管理サーバーのメンテナンス
- サードパーティ製品への情報の転送
- サードパーティの情報システムに関するセキュリティ推奨事項

管理サーバーの導入

管理サーバーアーキテクチャ

一般に、集中管理アーキテクチャの選択は、保護対象となるデバイスの場所、隣接するネットワークからのアクセス、データベースのアップデート配信方式などによって異なります。

アーキテクチャ開発の初期段階で、Kaspersky Security Center のコンポーネントとそれらの相互の対話、およびデータトラフィックとポートの使用に関する方式についてよく理解することを推奨します。

この情報をもとに、次の項目を指定するアーキテクチャを形成することができます：

- 管理サーバーの場所およびネットワーク接続
- 管理者のワークスペースの構成、および管理サーバーへの接続方法

- ネットワークエージェントと保護ソフトウェアの導入方法
- ディストリビューションポイントの使用
- 仮想管理サーバーの使用
- 管理サーバーの階層の使用
- 定義データベースのアップデート方式
- その他の情報の流れ

管理サーバーインストール用のデバイスの選択

組織インフラストラクチャ内の専用サーバーに管理サーバーをインストールすることを推奨します。サーバーに他のサードパーティ製ソフトウェアがインストールされていない場合は、サードパーティ製ソフトウェアの要件に依存せずに、Kaspersky Security Center の要件に基づいてセキュリティ設定を構成することができます。

管理サーバーは、物理サーバーまたは仮想サーバーに導入することができます。選択されたデバイスがハードウェアおよびソフトウェアの要件を満たしていることをご確認ください。

管理サーバーの位置

管理サーバーで管理されているデバイスは、以下のように配置することができます：

- ローカルエリアネットワーク（LAN）上
- インターネット上
- 非武装地帯（DMZ）内

同時に、管理サーバーは、産業用、企業用、DMZ 用など、異なるセグメントに配置することも可能です。

Kaspersky Security Center を使用して隔離されたネットワークセグメントの保護を管理する場合は、管理サーバーを非武装地帯（DMZ）のセグメントに導入することを推奨します。これにより、完全な管理機能とアップデートの配信を維持しながら、適切なネットワークセグメンテーションを編成し、保護されたセグメントへのトラフィックフローを最小限に抑えることができます。

管理サーバーをドメインコントローラー、ターミナルサーバー、またはユーザーデバイスに導入する際の制限

管理サーバーをドメインコントローラー、ターミナルサーバー、またはユーザーデバイスにインストールしないことを強く推奨します。

ネットワークキーノードの機能を分離することを推奨します。この方法により、ノードに障害が発生したり侵害されたりした場合でも、異なるシステムの運用性を維持することができます。同時に、ノードごとに異なるセキュリティポリシーを作成することができます。

たとえば、通常、ドメインコントローラーに適用されるセキュリティ制限は、管理サーバーのパフォーマンスを大幅に低下させ、管理サーバーの一部の機能を使用できなくする可能性があります。侵入者がドメインコントローラーへの特権アクセスを取得した場合、Active Directory ドメインサービス（AD DS）データベースが変更、破損、または破壊される可能性があります。また、Active Directory で管理されているすべてのシステムおよびアカウントが危険にさらされる可能性があります。

管理サーバーをインストールして実行するためのアカウント

ドメインアカウントを使用して管理サーバーデータベースにアクセスすることを避けるために、ローカル管理者アカウントで管理サーバーのインストールを実行することを推奨します。必要なアカウントとそのアカウントの権限は、選択した DBMS の種類、DBMS の場所、管理サーバーデータベースの作成方法によって異なります。

Kaspersky Security Center のインストール時に、KLAdmins グループおよび KLOperators グループが自動的に作成されます。これらのグループには、管理サーバーに接続し、管理サーバーオブジェクトを処理するための権限が与えられます。

Kaspersky Security Center のインストール時に使用されるアカウントの種類に応じて、以下のように KLAdmins グループと KLOperators グループが作成されます：

- ドメイン内に含まれるユーザーアカウントを使用してインストールする場合、グループは管理サーバーデバイス上と管理サーバーを含むドメイン内に作成されます。
- システムアカウントでインストールする場合、グループは管理サーバーデバイス上のみに作成されます。

ドメイン内に KLAdmins および KLOperators グループを作成し、結果として**管理サーバーを管理する権限を管理サーバーデバイス外のアカウントに与える**ことを避けるため、ローカルアカウントで Kaspersky Security Center をインストールすることを推奨します。

管理サーバーのインストール中、サービスとして管理サーバーを開始する場合に使用するアカウントを選択します。既定では、KL-AK-* という名前のローカルアカウントが作成され、このアカウントで管理サーバーサービス（klserver サービス）が実行されます。

必要に応じて、選択したアカウントで管理サーバーサービスを実行することができます。このアカウントには、DBMS にアクセスするために必要な権限が付与されている必要があります。セキュリティ上の理由から、管理サーバーサービスの実行には、非特権アカウントを使用してください。

誤ったアカウント設定の使用を避けるために、アカウントを自動的に生成することを推奨します。

ドメインから管理サーバーを除外する

管理サーバーを使用して重要度の高いシステムのデバイスグループを保護する場合、ドメインに管理サーバーデバイスを含めることは推奨しません。これにより、Kaspersky Security Center の管理権限を差別化し、ドメインアカウントが侵害された場合に管理サーバーへのアクセスを防止することができます。

ワークグループに含まれるデバイスに管理サーバーをインストールする場合、管理サーバーを使用する次のシナリオは使用できなくなることに注意してください：

- Kaspersky Security Center のフェイルオーバークラスタの使用
- Windows Server のフェールオーバークラスターの使用
- 別のデバイスでの SQL Server の使用

管理サーバーと SQL Server がドメインに含まれている場合にのみ、別のデバイスで SQL Server を使用できます。

- 管理サーバーツールによる、Active Directory グループポリシーを使用したリモートインストール

管理サーバーを Active Directory ドメインから切断する必要がある場合は：「Kaspersky Security Center の名前を変更する方法の」トピックで説明されている手順に従ってください。

ワークグループに含まれるデバイスに管理サーバーをインストールする必要がある場合は、Kaspersky Security Center Windows の代わりに Kaspersky Security Center Linux を使用できます。

接続の安全性

TLS の使用

管理サーバーへのセキュアでない接続を禁止することを推奨します。たとえば、管理サーバーの設定で HTTP を使用する接続を禁止することができます。

既定では、管理サーバーの HTTP ポートが閉じられていることに注意してください。残りのポートは、管理サーバーのウェブサーバー（8060）に使用されます。このポートは、管理サーバーデバイスのファイアウォール設定によって制限される場合があります。

厳密な TLS 設定

バージョン 1.2 以降の TLS プロトコルを使用し、セキュアでない暗号化アルゴリズムを制限または禁止することを推奨します。

管理サーバーが使用する暗号化プロトコル（TLS）を構成することができます。管理サーバーのバージョンのリリース時には、安全なデータ転送を確保するために暗号化プロトコルが既定で設定されていることに注意してください。

管理サーバーデータベースへのアクセスを制限する

管理サーバーデータベースへのアクセスを制限することを推奨します。たとえば、管理サーバーデバイスからのみアクセスを許可します。これにより、既知の脆弱性が原因で管理サーバーデータベースが危険にさらされる可能性が低くなります。

使用するデータベースの操作説明書に従ってパラメータを構成したり、ファイアウォールで閉じたポートを提供したりすることができます。

Windows アカウントによるリモート認証の禁止

LP_RestrictRemoteOsAuth フラグを使用して、リモートアドレスからの SSPI 接続を禁止することができます。このフラグを使用すると、ローカルまたはドメインの Windows アカウントを使用した管理サーバーでのリモート認証を禁止することができます。

LP_RestrictRemoteOsAuth フラグをリモートアドレスからの接続を禁止するモードに切り替えるには：

1. Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダ

ーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

2. コマンドラインで次のコマンドを実行して、LP_RestrictRemoteOsAuth フラグの値を指定します：

```
klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
```

3. 管理サーバーサービスを再起動します。

リモート認証が Kaspersky Security Center Web コンソールまたは管理サーバーデバイスにインストールされている管理コンソールを介して実行される場合、LP_RestrictRemoteOsAuth フラグは機能しません。

Microsoft SQL Server の認証

Kaspersky Security Center が Microsoft SQL Server を DBMS として使用する場合、データベースとの間で転送される Kaspersky Security Center のデータおよびデータベースに保存されているデータを不正アクセスから保護する必要があります。これを行うには、Kaspersky Security Center と SQL Server の間の通信を保護する必要があります。セキュアな通信を実現する最も確実な方法は、Kaspersky Security Center と SQL Server を同じデバイスにインストールし、両方のアプリケーションで共有メモリ機構を使用する方法です。それ以外の場合は、SSL または TLS 証明書を使用して SQL Server インスタンスを認証することを推奨します。

管理サーバーに接続するための IP アドレスの許可リストの設定

既定では、ユーザーは、Kaspersky Security Center Web コンソールを開くことができる、または MMC ベースの管理コンソールをインストールした任意のデバイスで Kaspersky Security Center にログインすることができます。ただし、管理サーバーを設定することで、ユーザーが許可された IP アドレスを持つデバイスからのみ管理サーバーに接続できるように設定できます。この場合、侵入者が Kaspersky Security Center アカウントを盗んだとしても、侵入者は許可リストに登録されている IP アドレス以外から Kaspersky Security Center にログインすることはできません。

アカウントおよび認証

以下の手順を実行する前に、KL ツール（管理サーバーデータのバックアップまたは klbackup ユーティリティ）を使用して Kaspersky Security Center 管理サーバーのバックアップコピーを作成し、安全な場所に保存します。

管理サーバーでの二段階認証の使用

Kaspersky Security Center は、RFC 6238 標準（TOTP：Time-Based One-Time Password アルゴリズム）に基づいて、Kaspersky Security Center Web コンソールおよび管理コンソールのユーザーに「**二段階認証**」を提供します。

自分のアカウントに二段階認証が適用されると、Kaspersky Security Center Web コンソールまたは管理コンソールにログインするたびに、ユーザー名、パスワード、および追加の単回使用セキュリティコードを入力することになります。自分のアカウントでドメイン認証を使用している場合、さらに追加で1度だけ使用するセキュリティコードを入力する必要があります。1度だけ使用するセキュリティコードを受け取るには、ご使用のコンピューターまたはモバイルデバイスなどに認証アプリがインストールされている必要があります。

RFC 6238 標準に対応したソフトウェアとハードウェアの両方の認証機能（トークン）があります。たとえば、ソフトウェア認証には、Google Authenticator、Microsoft Authenticator、FreeOTP などがあります。

管理サーバーへの接続が確立されているデバイスと同じデバイスに認証アプリをインストールすることは強く推奨しません。モバイルデバイスに認証アプリをインストールすることができます。

オペレーティングシステムの二要素認証の使用

管理サーバーデバイスでの認証には、トークン、スマートカード、またはその他の方法（可能な場合）を使用した多要素認証（MFA）を使用することを推奨します。

管理者パスワード保存の禁止

管理コンソールを使用する場合、管理サーバー接続ダイアログボックスに管理者パスワードを保存することは推奨しません。

Kaspersky Security Center Web コンソールを使用する場合、ユーザーのデバイスにインストールされているブラウザーに管理者パスワードを保存することは推奨しません。

内部ユーザーアカウントの認証

既定では、管理サーバーの内部ユーザーアカウントのパスワードは次の規則に従う必要があります：

- パスワードは、8 文字以上 256 文字以下にしてください。
- パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
  - アルファベット大文字（A-Z）
  - アルファベット小文字（a-z）
  - 数字（0 - 9）
  - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）
- パスワードに空白文字や Unicode 文字を含めることはできません。また「.」の後に続けて「@」を入力することは避けてください。

既定では、許可されるパスワードの入力試行回数の上限は 10 回です。パスワード入力の試行回数を変更することができます。

Kaspersky Security Center ユーザーが無効なパスワードを入力できる回数には上限があります。入力回数が上限に達すると、ユーザーアカウントが 1 時間ブロックされます。

管理サーバー専用の管理グループ

管理サーバー専用の管理グループを作成することを推奨します。このグループには特別なアクセス権限を付与し、特別なセキュリティポリシーを作成します。

管理サーバーのセキュリティレベルを意図的に下げることを避けるために、専用の管理グループを管理できるアカウントのリストを制限することを推奨します。

KLAdmins および KLOperators グループ

Kaspersky Security Center のインストール時に、KLAdmins および KLOperators グループが自動的に作成されます。KLAdmins グループには、すべてのアクセス権が付与されています。KLOperators グループには、読み取りと実行の権限のみが付与されます。KLAdmins グループに付与される権限は**ロック**されています。

オペレーティングシステムの標準の管理ツールを使用して、KLAdmins および KLOperators グループを表示したり、これらのグループに変更を加えたりすることができます。

管理サーバーを使用する際の規則を策定する場合、情報セキュリティの専門家が標準的なタスクを実行するためにフルアクセス（および KLAdmins グループへの参加）が必要かどうかを判断する必要があります。

基本的な管理タスクのほとんどは、会社の部門間（または同じ部門の異なる従業員）で分散させることができ、結果として異なるアカウント間で分散させることができます。Kaspersky Security Center で管理グループのアクセス差別化を設定することもできます。その結果、KLAdmins グループのアカウントでの認証が異常になり、インシデントと判断される可能性があるシナリオを実装することができます。

Kaspersky Security Center がシステムアカウントでインストールされた場合、グループは管理サーバーデバイスでのみ作成されます。この場合、Kaspersky Security Center のインストール時に作成されたエントリのみがグループに含まれるようにすることを推奨します。Kaspersky Security Center のインストール時に自動的に作成される KLAdmins グループ（ローカルおよび / またはドメイン）にグループを追加することは推奨しません。このグループを変更する権限も制限する必要があります。KLAdmins グループには、特権のない単一のアカウントのみを含める必要があります。

インストールがドメインユーザーアカウントで実行された場合、KLAdmins および KLOperators グループが管理サーバーと管理サーバーを含むドメインの両方に作成されます。ローカルアカウントのインストールなど、類似の方法を推奨します。

メイン管理者ロールのメンバーシップの制限

メイン管理者ロールのメンバーシップを制限することを推奨します。

既定では、管理サーバーのインストール後、メイン管理者ロールがローカル管理者グループと作成された KLAdmins グループに割り当てられます。これは管理には役立ちますが、セキュリティの観点からは重要です。メイン管理者ロールには広範な権限があるため、ユーザーへのこのロールの割り当ては厳密に規制する必要があります。

ローカル管理者は、Kaspersky Security Center の管理者権限を持つユーザーのリストから除外することができます。メイン管理者のロールを KLAdmins グループから削除することはできません。管理サーバーの管理に使用されるアカウントを KLAdmins グループに含めることができます。

ドメイン認証を使用する場合は、Kaspersky Security Center でドメイン管理者アカウントの権限を制限することを推奨します。既定では、これらのアカウントにはメイン管理者のロールがあります。また、ドメイン管理者は、自分のアカウントを KLAdmins グループに含めて、メイン管理者のロールを取得することができます。これを回避するには、Kaspersky Security Center のセキュリティ設定で Domain Admins グループを追加し、それに対する禁止ルールを定義します。これらのルールは、許可するルールよりも優先する必要があります。

設定済みの一連の権限を持つ定義済みのユーザーのロールを使用することもできます。

アプリケーション機能へのアクセス権の設定

ユーザーまたはユーザーグループごとに、Kaspersky Security Center の機能へのアクセス権を柔軟に設定することを推奨します。

ロールベースのアクセス制御により、事前定義された一連の権利を持つ標準ユーザーロールを作成し、職務の範囲に応じてこれらのロールをユーザーに割り当てることができます。

ロールベースのアクセス制御モデルの主な利点：

- 管理の容易さ
- ロール階層
- 最小特権方法
- 職務の分離

職位に基づいて特定の従業員に組み込みのロールを割り当てたり、まったく新しいロールを作成したりすることができます。

ロールを構成する際は、管理サーバーデバイスの保護状態の変更とサードパーティ製ソフトウェアのリモートインストールに関連する権限に注意してください：

- 管理グループの管理。
- 管理サーバー上での操作。
- リモートインストール。
- イベントを保存して通知を送信するためのパラメータの変更。

  この権限により、イベントの発生時に管理サーバーデバイスでスクリプトまたは実行可能モジュールを実行する通知を設定できます。

アプリケーションのリモートインストール用の個別のアカウント

アクセス権の基本的な差別化に加えて、すべてのアカウントに対してアプリケーションのリモートインストールを制限することを推奨します（メイン管理者または別の特殊なアカウントを除く）。

アプリケーションのリモートインストールには別のアカウントを使用することを推奨します。別のアカウントに役割または権限を割り当てることができます。

Windows 特権アクセスの保護

特権アクセスセキュリティを提供するための Microsoft の推奨事項を考慮することを推奨します。これらの推奨事項については、「特権アクセスの保護」の記事を参照してください。

推奨事項の重要なポイントの1つは、特権アクセスワークステーション（PAW）の実装です。

管理対象サービスアカウント（MSA）またはグループ管理対象サービスアカウント（gMSA）を使用して管理サーバーサービスを実行する

Active Directory には、「グループ管理対象サービスアカウント（MSA/gMSA）」と呼ばれるサービスを安全に実行するための特別な種類のアカウントがあります。Kaspersky Security Center は、管理対象サービスアカウント（MSA）とグループ管理対象サービスアカウント（gMSA）をサポートしています。これらの種別のアカウントをドメインで使用している場合は、それらの1つを管理サーバーのサービス用のアカウントとして選択できます。

すべてのユーザーの定期的な監査

管理サーバーデバイス上のすべてのユーザーを定期的に監査することを推奨します。これにより、デバイスが危険にさらされる可能性に関連する特定の種類のセキュリティ脅威に対応することができます。

管理サーバーの保護管理

管理サーバー保護ソフトウェアの選択

管理サーバーの導入種類と一般的な保護戦略に応じて、管理サーバーデバイスを保護するためのアプリケーションを選択します。

専用デバイスに管理サーバーを導入する場合は、Kaspersky Endpoint Security アプリケーションを選択して管理サーバーデバイスを保護することを推奨します。これにより、ふるまい分析モジュールなど、管理サーバーデバイスを保護するために使用可能なすべての技術を適用することができます。

インフラストラクチャに存在し、以前に他のタスクに使用されていたデバイスに管理サーバーがインストールされている場合は、次の保護ソフトウェアを検討することを推奨します：

- Kaspersky Industrial CyberSecurity for Nodes。産業用ネットワークに含まれるデバイスにこのアプリケーションをインストールすることを推奨します。Kaspersky Industrial CyberSecurity for Nodes は、産業用ソフトウェアの様々なメーカーとの互換性のある証明書を持つ製品です。

- 推奨するセキュリティソリューション。管理サーバーが他のソフトウェアと一緒にデバイスにインストールされている場合、セキュリティソリューションの互換性に関するそのソフトウェアベンダーの推奨事項を考慮することを推奨します（セキュリティソリューションを選択するための推奨事項が既に存在する場合があり、信頼ゾーンを構成する必要がある場合があります）。

保護アプリケーション用に別のセキュリティポリシーを作成

管理サーバーデバイスを保護するアプリケーション用に別のセキュリティポリシーを作成することを推奨します。このポリシーは、クライアントデバイスのセキュリティポリシーとは異なるものである必要があります。これにより、他のデバイスの保護レベルに影響を与えることなく、管理サーバーに最適なセキュリティ設定を指定することができます。

デバイスをグループに分けてから、特別なセキュリティポリシーを作成できる別のグループに管理サーバーデバイスを配置することを推奨します。

保護モジュール

管理サーバーと同じデバイスにインストールされているサードパーティ製ソフトウェアのベンダーから特別な推奨事項がない場合は、使用可能なすべての保護モジュールを有効化して構成することを推奨します（これらの保護モジュールの動作を一定時間チェックした後）。

管理サーバーデバイスのファイアウォールの構成

管理サーバーデバイスでは、ファイアウォールを設定して、管理者が管理コンソールまたは Kaspersky Security Center Web コンソールを介して管理サーバーに接続できるデバイスの数を制限することを推奨します。

既定では、管理サーバーはポート 13291 を使用して管理コンソールからの接続を受信し、ポート 13299 を使用して Kaspersky Security Center Web コンソールからの接続を受信します。これらのポートを使用して管理サーバーを管理できるデバイスの数を制限することを推奨します。

コントロールパネルの起動禁止

Microsoft Windows を実行しているデバイスに管理サーバーをインストールし、アプリケーション起動制御モジュールで保護アプリケーションを使用する場合、権限のないユーザー（管理者グループなど）によるコントロールパネル（control.exe）の起動を禁止することができます。

アプリケーションの起動を禁止する特定の制御ルールを作成すると、事前定義された管理者ロールの権限を持つユーザーは、ログインやパスワードの変更など、他のネットワークアカウントを制御することができなくなります。

クライアントデバイスの保護管理

インストールパッケージへのライセンスの追加制限

インストールパッケージは、管理サーバーの共有フォルダーのパッケージサブフォルダーに保存されます。ライセンスをインストールパッケージに追加すると、共有読み取りアクセス権がインストールパッケージのリポジトリに対して有効になるため、ライセンスが危険にさらされる可能性があります。

ライセンスへの侵害を避けるため、ライセンスをインストールパッケージに追加することは推奨しません。

管理対象デバイスへのライセンスの自動配布、管理対象アプリケーションのライセンスの追加タスクによる導入、アクティベーションコードまたはライセンス情報ファイルを手動でデバイスに追加することを推奨します。

管理グループ間でデバイスを移動するための自動ルール

管理グループ間でデバイスを移動するための自動ルールの使用を制限することを推奨します。

デバイスを移動するための自動ルールを使用すると、移動したデバイスに移動前のデバイスよりも多くの特権を与えるポリシーが伝搬する可能性があります。

また、クライアントデバイスを別の管理グループに移動すると、ポリシー設定が伝播される可能性があります。このポリシー設定は、ゲストデバイスや信頼できないデバイスへの配布には望ましくない場合があります。

この推奨事項は、管理グループへのデバイスの 1 回限りの初期割り当てには適用されません。

ディストリビューションポイントと接続ゲートウェイのセキュリティ要件

ネットワークエージェントがインストールされたデバイスは、ディストリビューションポイントとして機能し、次の機能を実行することができます：

- 管理サーバーから受信したアップデートとインストールパッケージをグループ内のクライアントデバイスに配布します。

- クライアントデバイスでサードパーティ製ソフトウェアとカスペルスキー製品のリモートインストールを実行します。
- 新しいデバイスを検出したり既存のデバイスの情報を更新するために、ネットワークを検索します。ディストリビューションポイントは、管理サーバーと同じデバイス検出方法を使用することができます。

次の目的で使用される組織のネットワークにディストリビューションポイントを配置します：

- 管理サーバーの負荷の低減
- トラフィックの最適化
- ネットワーク内の届きにくい場所にあるデバイスへの管理サーバーアクセスの提供

使用可能な機能を考慮して、ディストリビューションポイントとして機能するデバイスをあらゆる種類の不正アクセス（物理的アクセスなど）から保護することを推奨します。

ディストリビューションポイントの自動割り当ての制限

管理を簡素化し、ネットワークの操作性を維持するために、ディストリビューションポイントの自動割り当てを使用することを推奨します。ただし、産業用ネットワークや小規模なネットワークでは、たとえば、リモートインストールのプッシュタスクに使用するアカウントの個人情報が OS によってディストリビューションポイントに転送される可能性があるため、ディストリビューションポイントの自動割り当ては避けることを推奨します。

産業用ネットワークおよび小規模ネットワークの場合、ディストリビューションポイントとして機能するデバイスを手動で割り当てることができます。

また、『ディストリビューションポイントのアクティビティレポート』を表示することもできます。

管理対象アプリケーションの保護構成

管理対象アプリケーションポリシー

使用するアプリケーションと Kaspersky Security Center のコンポーネント（ネットワークエージェント、Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Agent など）の種別ごとにポリシーを作成することを推奨します。このポリシーは、すべての管理対象デバイス（ルート管理グループ）に適用するか、構成済みの移動ルールに従って新しい管理対象デバイスを自動的に移動させる別のグループに適用する必要があります。

保護を無効にしてアプリケーションをアンインストールするためのパスワードを指定

カスペルスキーのセキュリティ製品による保護の無効化を防止するために、パスワードによる保護を有効にして、保護の無効化およびカスペルスキーのセキュリティ製品のアンインストールの実行にはパスワードが必要となるよう設定することを強く推奨します。たとえば、Kaspersky Endpoint Security for Windows、Kaspersky Security for Windows Server、ネットワークエージェント、その他のカスペルスキー製品でパスワードを設定できます。パスワードによる保護を有効にした後、「ロック」を閉じてこれらの設定をロックすることを推奨します。

クライアントデバイスを管理サーバーに手動で接続するためのパスワードの指定（klmover ユーティリティ）

klmover ユーティリティを使用すると、クライアントデバイスを管理サーバーに手動で接続できます。クライアントデバイスにネットワークエージェントをインストールすると、このユーティリティは自動的にネットワークエージェントのインストールフォルダーにコピーされます。

侵入者がデバイスを管理サーバーの制御外に移動するのを防ぐために、klmover ユーティリティを実行する際のパスワード保護を有効にすることを強く推奨します。パスワード保護を有効にするには、ネットワークエージェントポリシー設定で［**アンインストール用パスワードを使用する**］をオンにします。

klmover ユーティリティにはローカル管理者権限が必要です。ローカル管理者権限なしで操作されるデバイスの場合、klmover ユーティリティを実行するためのパスワード保護を省略できます。

アンインストール用パスワードを使用するを有効にすると、クリーナーツール（cleaner.exe）のパスワード保護も有効になります。

Kaspersky Security Network の使用

管理対象アプリケーションのすべてのポリシーと管理サーバーのプロパティで、Kaspersky Security Network（KSN）の使用を有効にし、KSN 声明を受け入れることを推奨します。管理サーバーをアップデートまたはアップグレードすると、更新された KSN 声明を受け入れることができます。法律などによりクラウドサービスの使用が禁止されている場合は、KSN を無効にすることができます。

管理対象デバイスの定期スキャン

すべてのデバイスグループに対して、デバイスのフルスキャンを定期的に実行するタスクを作成することを推奨します。

新しいデバイスの検出

デバイスの検索を適切に設定することを推奨します：Active Directory との統合の設定、新規デバイスを検索する IP アドレス範囲の指定。

セキュリティ上の理由から、すべての新しいデバイスを含む既定の管理グループと、このグループに影響する既定のポリシーを使用することができます。

共有フォルダーの選択

既存の共有フォルダーを選択して（インストールパッケージの配置やアップデートされた定義データベースの保存などに使用される）Windows を実行しているデバイスに管理サーバーを導入する場合、Everyone グループに読み取り権限が、KLAdmins グループに書き込み権限が付与されていることを確認することを推奨します。

管理サーバーのメンテナンス

管理サーバーデータのバックアップコピー

データのバックアップにより、データを失うことなく管理サーバーのデータを復元することができます。

既定では、管理サーバーのインストール後にデータバックアップタスクが自動的に作成され、定期的に実行され、適切なディレクトリにバックアップが保存されます。

データバックアップタスクの設定は、次のように変更することができます：

- バックアップ頻度が上がります
- コピーを保存するための特別なディレクトリが指定されています
- バックアップコピーのパスワードが変更されます

既定のディレクトリとは異なる特別なディレクトリにバックアップコピーを保存する場合は、このディレクトリのアクセス制御リスト（ACL）を制限することを推奨します。管理サーバーアカウントと管理サーバーデータベースのアカウントには、このディレクトリへの書き込みアクセス権が必要です。

管理サーバーのメンテナンス

［管理サーバーのメンテナンス］により、データベースのボリュームを削減し、アプリケーションのパフォーマンスと操作の信頼性を向上させることができます。管理サーバーのメンテナンスは、少なくとも週に1回で実施することを推奨します。

管理サーバーのメンテナンスは、専用のタスクで実施されます。管理サーバーのメンテナンス時、次の処理が実行されます：

- データベースにエラーがないか確認する
- データベースインデックスを再編成する
- データベースの統計情報をアップデート
- データベースを縮小する（必要に応じて）

オペレーティングシステムのアップデートとサードパーティ製ソフトウェアのアップデートをインストール

オペレーティングシステムとサードパーティ製ソフトウェアのアップデートを管理サーバーデバイスに定期的にインストールすることを強く推奨します。

クライアントデバイスは管理サーバーへの継続的な接続を必要としないため、アップデートをインストール後に管理サーバーデバイスを再起動しても安全です。管理サーバーのダウンタイム中にクライアントデバイスに登録されたすべてのイベントは、接続が復元された後に管理サーバーに送信されます。

サードパーティシステムへのイベント転送

監視とレポート

セキュリティ問題にタイムリーに対応するために、監視とレポート機能を設定することを推奨します。

SIEM システムへのイベントのエクスポート

重大な損害が発生する前にセキュリティ問題を迅速に検知するには、SIEM システムでイベントエクスポートを使用することを推奨します。

監査イベントのメール通知

Kaspersky Security Center では、管理サーバーと管理対象デバイスにインストールされた他のカスペルスキー製品の動作中に発生したイベントの情報を受信できます。緊急事態にタイムリーに対応するために、公開する監査イベント、重要イベント、障害イベント、および警告に関する通知を送信するように管理サーバーを設定することを推奨します。

これらのイベントはシステム内のイベントであるため、少数のイベントが予想され、メーリングに非常に適しています。

管理サーバー機能の統計

セキュリティ問題にタイムリーに対応するために、簡易ネットワーク管理プロトコル（SNMP）を使用して、管理サーバー機能の統計情報をサードパーティアプリケーションに送信するように構成することを推奨します。

サードパーティの情報システムに関するセキュリティ推奨事項

CIS ベンチマークからのセキュリティ推奨事項

管理サーバーおよびネットワークエージェントでサポートされているオペレーティングシステム、仮想化プラットフォーム、または定義データベースサーバーのバージョンを使用する場合は、Center for Internet Security（CIS）のベストインフォメーションセキュリティプラクティスを適用して（存在する場合）、これらの情報システムを微調整することを推奨します。

Center for Internect Security（CIS）は、情報技術分野におけるセキュリティの向上に取り組む非営利団体です。特に、CIS は CIS コントロールや CIS ベンチマークなどの安全基準を開発し、配布しています。これらの標準は、情報システムのセキュリティを確保するための一連の推奨事項と方法です。

CIS ポータルには、管理サーバーおよびネットワークエージェントでサポートされている次の情報システムのバージョンに対する推奨事項が含まれています：

- 次のファミリーのオペレーティングシステム：
  - デスクトップ向け Windows
  - サーバー向け Windows
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS

- VMware 仮想化プラットフォーム
- データベースサーバー：
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

Astra Linux オペレーティングシステムのセキュリティに関する推奨事項

Astra Linux オペレーティングシステムを使用する場合は、対応するバージョンの Astra Linux の Red Book に記載されているセキュリティ推奨事項に従う必要があります。

RED OS オペレーティングシステムのセキュリティに関する推奨事項

RED OS オペレーティングシステムを使用する場合は、公式 RED OS ドキュメントに記載されているセキュリティ推奨事項に従う必要があります。

カスペルスキーセキュリティ製品の使用に関する推奨事項

Kaspersky Endpoint Security for Windows で KLAdmin パスワードを使用します

コンピューターリテラシーのレベルが異なる複数のユーザーが、Kaspersky Endpoint Security for Windows がインストールされたコンピューターを共有できます。ユーザーが Kaspersky Endpoint Security for Windows とその設定に無制限にアクセスできる場合、コンピューターの全体的な保護レベルが低下する可能性があります。パスワード保護を使用すると、ユーザーに付与された権限（アプリケーションを終了する権限など）に応じて、Kaspersky Endpoint Security for Windows へのユーザーのアクセスを制限できます。

Kaspersky Endpoint Security for Windows とそのパラメータへのアクセスを制限する方法の 1 つは、KLAdmin アカウントを使用することです。KLAdmin アカウントは、Kaspersky Endpoint Security for Windows への無制限のアクセス権を持つ管理者アカウントです。KLAdmin アカウントには、Kaspersky Endpoint Security for Windows でパスワードで保護されたすべてのアクションを実行する権限があります。KLAdmin アカウントの権限は取り消すことができません。Kaspersky Endpoint Security for Windows ポリシーのプロパティで KLAdmin アカウントのパスワードを設定できます。Kaspersky Endpoint Security for Windows 管理者は、KLAdmin アカウントのパスワードの安全使用について全責任を負います。組織に独自のパスワードポリシーがある場合は、そのポリシーの指示に従ってください。

KLAdmin パスワードの盗難から組織を保護するための推奨事項は次の通りです。

- **一般要件**
  アカウント名または名前の一部をパスワードとして使用しないでください。
- **パスワードの最小文字数要件**
  少なくとも 10 文字の長さのパスワードを作成してください。
- **複数の文字タイプを使用するための要件**

小文字、大文字、数字、特殊文字など、さまざまなカテゴリの文字を含む複雑なパスワードを設定します。

- **パスワードの有効期限要件**

  パスワードの有効期限を最小 90 日に設定します。新しいパスワードは、過去 24 個のパスワードのいずれとも一致してはなりません。

導入準備

このセクションでは Kaspersky Security Center の導入前に必要となる手順について説明します。

Kaspersky Security Center を導入するにあたって

このセクションでは、組織ネットワークに Kaspersky Security Center コンポーネントを導入する際に最適なオプションを、次の基準に基づいて説明します：

- デバイスの合計数
- 組織的または地理的に離れている組織単位（ローカルオフィス、支社、支店）
- 狭い帯域幅で接続されている個別のネットワーク
- 管理サーバーへのインターネットアクセス

保護システム導入の一般的なスキーム

このセクションでは、Kaspersky Security Center を使用して企業ネットワークに保護システムを導入する際の基本的なスキームについて説明します。

システムは、あらゆる不正アクセスから保護される必要があります。本製品をデバイスにインストールする前に、オペレーティングシステムで利用可能なすべてのセキュリティアップデートをインストールするとともに、管理サーバーとディストリビューションポイントが物理的な不正アクセスを受けないような保護対策を実施してください。

Kaspersky Security Center で以下の導入スキームを使用して、企業ネットワークに保護システムを導入できます：

- 次のいずれかの方法を使用して、Kaspersky Security Center により保護システムを導入します：
  - 管理コンソールを使用
  - Kaspersky Security Center Web コンソールを使用

  カスペルスキー製品は、自動でクライアントデバイスにインストールされ、Kaspersky Security Center を使用することによって自動的に管理サーバーに接続されます。

  基本的な導入スキームは、管理コンソールによる保護システムの導入です。Kaspersky Security Center Web コンソールを使用して、ブラウザーからカスペルスキー製品をインストールできます。

- Kaspersky Security Center によって生成されたスタンドアロンインストールパッケージを使用して、手動で保護システムを導入します。

  クライアントデバイスと管理コンピューターにカスペルスキー製品を手動でインストールし、ネットワークエージェントのインストール時にクライアントデバイスと管理サーバーの接続を設定します。

  この導入方法は、リモートインストールが実行できない場合に使用してください。

Kaspersky Security Center では、Microsoft Active Directory® グループポリシーを使用して保護システムを導入することもできます。

組織ネットワークへの Kaspersky Security Center の導入計画の策定

1 台の管理サーバーで最大 100,000 台のデバイスをサポートできます。組織ネットワーク上に合計で 100,000 台を超えるデバイスが存在する場合は、ネットワークに複数の管理サーバーを導入し、階層化して一元的に管理する必要があります。

組織に大規模なリモートローカルオフィス（支社、支店）が存在し、それぞれに独自の管理者が割り当てられている場合は、各オフィスに管理サーバーを導入するのが適切な方法です。そうしない場合は、そのようなオフィスは、低スループットチャネルによって接続された個別のネットワークとみなす必要があります（「標準設定：各オフィスの管理者によって運用されている少数の大規模なオフィス」を参照）。

狭い帯域幅で接続されている個別のネットワークを使用する際にトラフィック量を軽減するには、1 つまたは複数個のネットワークエージェントをディストリビューションポイントとして動作するように割り当てます（ディストリビューションポイントの数の計算表を参照してください）。この場合、個別のネットワーク上にあるすべてのデバイスは、それらのローカルアップデートセンターからアップデートを取得します。有効なディストリビューションポイントでは、管理サーバー（既定のシナリオ）とインターネット上のカスペルスキーのサーバーの両方からアップデートをダウンロードできます（「標準設定：複数の小規模なリモートオフィス」を参照）。

「Kaspersky Security Center の標準設定」では、Kaspersky Security Center の標準設定について詳しく説明されています。製品の導入を計画している場合は、組織の組織構造に応じて最適な標準設定を選択してください。

導入計画段階では、管理サーバーに対して特別な X.509 証明書を割り当てることを検討する必要があります。管理サーバーに対する X.509 証明書の割り当てが有効になるのは、次の場合です（部分的なリスト）：

- SSL Termination プロキシまたはリバースプロキシを使用して、セキュアソケットレイヤー（SSL）トラフィックをスキャンする場合
- 組織の公開鍵基盤（PKI）と統合する場合
- 証明書で必要な値を指定する場合
- 証明書で必要な暗号化強度を指定する場合

企業を保護する仕組みを選択する

企業組織を保護する仕組みは、次の要因に基づいて選択します：

- 組織のネットワークトポロジー
- 組織の構造

- ネットワーク保護対策の担当者数および担当者の役割
- 保護管理コンポーネントに割り当てることができるハードウェア資源
- 組織のネットワークで保護コンポーネントのメンテナンスに割り当てることができる通信チャネルの処理能力
- 組織のネットワークで重要な管理作業を実行する際の制限時間。重要な管理作業には、定義データベースの配信やクライアントデバイスについてのポリシーの変更などが含まれます

保護の仕組みを選択する際は、まず、一元的な保護システムの運用に使用できるネットワーク資源およびハードウェア資源を評価してください。

ネットワークおよびハードウェアインフラストラクチャを分析するには、以下のプロセスに従ってください：

1. 保護を導入するネットワークについて、次の設定を定義します：
   - ネットワークセグメントの数
   - 個々のネットワークセグメント間の通信チャネルの速度
   - 各ネットワークセグメントでの管理対象デバイスの数
   - 保護の運用を維持するために割り当てることができる各通信チャネルの処理能力
2. 管理対象のすべてのデバイスに対して重要な管理作業を実施する時の最大許容時間を決めます。
3. ステップ1および2からの情報、および管理システムの負荷試験のデータを分析します。分析に基づき、次の問いに回答します。
   - 1台の管理サーバーですべてのクライアントを管理することが可能か。または、管理サーバーの階層が必要か。
   - ステップ2に指定された制限時間内にすべてのクライアントを処理するには、管理サーバーのどのハードウェア構成が必要か。
   - 通信チャネルの負荷を減らすためにディストリビューションポイントを使用する必要があるか。

上記ステップ3の問いに対する回答を得たら、組織の保護の仕組みをまとめることができます。

組織のネットワークでは、次の標準的な保護の仕組みのいずれかを使用できます。

- 管理サーバー1台：すべてのクライアントデバイスを1台の管理サーバーに接続します。管理サーバーは、ディストリビューションポイントとして機能します。
- 1台の管理サーバーといくつかのディストリビューションポイント：すべてのクライアントデバイスを1台の管理サーバーに接続します。ネットワークに接続されたクライアントデバイスの一部がディストリビューションポイントとして機能します。
- 管理サーバーの階層：ネットワークセグメントごとに1台の管理サーバーを割り当て、管理サーバーの階層の一部にします。プライマリ管理サーバーがディストリビューションポイントとして機能します。
- 管理サーバーの階層といくつかのディストリビューションポイント：ネットワークセグメントごとに1台の管理サーバーを割り当て、管理サーバーの階層の一部にします。ネットワークに接続されたクライアントデバイスの一部がディストリビューションポイントとして機能します。

Kaspersky Security Center の標準設定

このセクションでは、組織ネットワークに Kaspersky Security Center コンポーネントを導入する際に使用する次の標準設定について説明します：

- 単一のオフィス
- 少数の大規模なオフィス。地理的に離れており、各管理者が運用
- 複数の小規模なオフィス。地理的に離れている

標準設定：単一のオフィス

組織ネットワークには、1台または複数台の管理サーバーを導入できます。管理サーバーの数は、使用可能なハードウェアまたは管理対象デバイスの合計数に基づき選択可能です。

1台の管理サーバーで最大 100,000 台のデバイスをサポートできます。導入後に管理対象デバイスを増やす可能性がある場合は、1台の管理サーバーに接続するデバイスの数を少なくしておきます。

管理サーバーに対するインターネットアクセスが必要かどうかに応じて、管理サーバーを内部ネットワーク上または DMZ 内に導入することができます。

複数台のサーバーを使用する場合は、1つの階層に統合してください。管理サーバーの階層を使用することによりポリシーとタスクが重複するのを防ぎ、管理対象デバイスの全セットを1台の管理サーバーで管理している場合と同様に処理できます。つまり、デバイスの検索、デバイス選択の構築、レポートの作成などの処理を、1台の管理サーバーで管理している場合と同様に実行できます。

標準設定：各オフィスの管理者によって運用されている少数の大規模なオフィス

組織が地理的に離れている少数の大規模なオフィスによって構成されている場合は、各オフィスに管理サーバーを導入する構成を検討する必要があります。クライアントデバイスの数と使用可能なハードウェアに応じて、各オフィスに1台または複数の管理サーバーを導入できます。この場合、個別のオフィスは「標準設定：単一のオフィス」として表示できます。管理を簡単にするために、すべての管理サーバーを管理サーバーの階層にまとめることを推奨します（場合によっては、3 層以上の階層にする必要があります）。

一部の従業員がデバイス（ノート PC）を持ってオフィス間を移動する場合は、ネットワークエージェントポリシーでネットワークエージェント接続プロファイルを作成します。ネットワークエージェント接続プロファイルは、Windows および macOS デバイスでのみサポートされています。

標準設定：複数の小規模なリモートオフィス

この標準設定は、インターネットを介して本社と通信する可能性のある多数の小規模なリモートオフィスと本社からなるネットワーク向けの設定です。各リモートオフィスのネットワークは、ネットワークアドレス変換（NAT）を介するように NAT の内側に構成することができます。その場合、2 つのリモートオフィスは分離されているため、それらのリモートオフィス間の接続は確立できません。

本社に1台の管理サーバーを導入すると同時に、その他のすべてのオフィスに対して1つまたは複数個のディストリビューションポイントを割り当てる必要があります。オフィス間がインターネットを経由して接続されている場合は、*ディストリビューションポイントでディストリビューションポイントのリポジトリにアップデートをダウンロードタスクを作成*しておくことが有用な場合があります。これにより、管理サーバーからではなくカスペルスキーのサーバー、ローカルまたはネットワークフォルダーから直接アップデートをダウンロードできるようになります。

リモートオフィスにあるデバイスが管理サーバーに直接にはアクセスできない場合（たとえば、管理サーバーへはインターネットを介してアクセスできるが、インターネットアクセスを備えていないデバイスがある場合）は、ディストリビューションポイントを接続ゲートウェイモードに切り替える必要があります。この場合、リモートオフィスにあるデバイスのネットワークエージェントは、直接にではなくゲートウェイを介して管理サーバーに接続され、緊密に同期します。

たいていの場合、管理サーバーはリモートオフィスのネットワークをポーリングできないため、ディストリビューションポイントに対してこの機能をオンにしておくと便利です。

管理サーバーは、リモートオフィスにある NAT よりも内側にある管理対象デバイスに対して、ポート 15000 UDP に通知を送信することはできません。この問題を解決するために、ディストリビューションポイントとして動作しているデバイスのプロパティで、管理サーバーへの常時接続モードを有効にしておくことができます（［**管理サーバーから切断しない**］）。このモードは、ディストリビューションポイントの合計数が 300 を超えていない場合に使用可能です。プッシュサーバーを使用して、管理対象デバイスと管理サーバー間の継続的な接続を確認できます。詳細については、「ディストリビューションポイントをプッシュサーバーとして使用する」のトピックを参照してください。

管理サーバー用 DBMS の選択

管理サーバーで使用するデータベース管理システム（DBMS）を選択する場合は、管理サーバーが対応できるデバイス数を考慮する必要があります。

次の表に、有効な DBMS オプションとその使用上の推奨事項と制限事項を示します。

DBMS に関する推奨事項と制限事項

DBMS	推奨事項と制限事項
SQL Server Express Edition 2016 以降	10,000 台未満のデバイスに対して単一の管理サーバーを実行する予定で、管理対象デバイスにアプリケーションコントロールコンポーネントを使用しない場合は、この DBMS を使用してください。 管理サーバーと別のアプリケーションで同時に SQL Server Express Edition DBMS を使用することは厳重に禁じられています。
Express を除く 2016 以降のローカル SQL Server Edition	制限なし。
Express を除く 2016 以降のリモート SQL Server Edition	両方のデバイスが同じ Windows® ドメインにある場合のみ有効。ドメインが異なる場合は、両方のデバイス間で双方向の信頼された接続を確立する必要があります。
ローカルまたはリモートの MySQL 5.5、5.6、5.7（MySQL バージョン 5.5.1、5.5.2、5.5.3、5.5.4、5.5.5 はサポートされません）	10,000 台未満のデバイスに対して単一の管理サーバーを実行する予定で、管理対象デバイスにアプリケーションコントロールコンポーネントを使用しない場合は、この DBMS を使用してください。
ローカルまたはリモート MySQL 8.0.20 以降	50,000 台未満のデバイスに対して単一の管理サーバーを実行する予定で、管理対象デバイスにアプリケーションコントロールコンポーネントを使用しない場合は、この DBMS を使用してください。
ローカルまたはリモートの MariaDB（サポートされているバージョンを参照）	20,000 台未満のデバイスに対して単一の管理サーバーを実行する予定で、管理対象デバイスにアプリケーションコントロールコンポーネントを使用しない場合は、この DBMS を使用してください。
PostgreSQL、Postgres Pro（サポートされているバージョンを参照）	50,000 台未満のデバイスに対して単一の管理サーバーを実行する予定で、管理対象デバイスにアプリケーションコントロールコンポーネントを使用しない場合は、これらの DBMS のいずれかを使用してください。

SQL Server 2019 を DBMS として使用しており、累積パッチ CU12 以降をインストールしていない場合、Kaspersky Security Center をインストールした後に次の手順を実行する必要があります：

1. SQL Management Studio を使用して、SQL Server に接続します。
2. 次のコマンドを実行します（データベース名に別の名前を選択し、「KAV」の代わりに使用する場合）：

```
USE KAV
GO
```

```
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. SQL Server 2019 サービスを再起動します。

再起動しないと、SQL Server 2019 の使用時に「There is insufficient system memory in resource pool 'internal' to run this query」などのエラーが発生する場合があります。

Kaspersky Security Center 15.1 と動作する MariaDB x64 サーバーの設定

Kaspersky Security Center 15.1 は、MariaDB DBMS をサポートしています。サポートされる MariaDB のバージョンの詳細は、「ハードウェアおよびソフトウェア要件」セクションを参照してください。

Kaspersky Security Center に MariaDB DBMS を使用する場合、InnoDB および MEMORY ストレージおよび UTF-8 と UCS-2 のエンコーディングのサポートを有効にします。

my.ini ファイルの推奨設定

my.ini ファイルを設定するには：

1. テキストエディターで my.ini ファイルを開きます。

2. ファイル my.ini の `[mysqld]` セクションに、次の行を追加します：

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=<値>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

`innodb_buffer_pool_size` の値は、想定される KAV データベースのサイズの 80% 以上に設定する必要があります。指定されたメモリは、サーバーの起動時に割り当てられることに注意してください。データベースのサイズが指定されたバッファサイズより小さい場合、必要なメモリのみが割り当てられます。MariaDB 10.4.3 以前を使用する場合、割り当てられたメモリの実際のサイズは、指定されたバッファー サイズよりも約 10% 大きくなります。

このパラメータの値を「1」または「2」にすると MariaDB の動作速度に悪影響を及ぼす可能性があるため、パラメータには「`innodb_flush_log_at_trx_commit=0`」を使用してください。
`innodb_file_per_table` パラメータが `1` に設定されていることを確認します。

MariaDB 10.6 の場合は、［mysqld］セクションに次の行を追加で入力します：

```
optimizer_prune_level=0
optimizer_search_depth=8
```

既定では、オプティマイザのアドオン「join_cache_incremental、「join_cache_hashed」および「join_cache_bka」は有効になっています。これらのアドオンが無効になっている場合は、有効にする必要があります。

オプティマイザのアドオンが有効になっているかどうかを確認するには：

1. MariaDB クライアントコンソールで、次のコマンドを実行してください：

   ```
   SELECT @@optimizer_switch;
   ```

2. 出力に次の行が含まれることを確認します：

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   これらの行が存在して値に「on」が指定されている場合は、オプティマイザのアドオンは有効です。

   これらの行が存在しない、または値に「off」が指定されている場合は、以下を実行してください：

   1. テキストエディターで my.ini ファイルを開きます。

   2. ファイル my.ini の [mysqld] セクションに、次の行を追加します：

      ```
      optimizer_switch='join_cache_incremental=on'
      optimizer_switch='join_cache_hashed=on'
      optimizer_switch='join_cache_bka=on'
      ```

アドオン「join_cache_incremental」、「join_cache_hash」および「join_cache_bka」が有効になりました。

Kaspersky Security Center 15.1 と動作する MySQL x64 サーバーの設定

Kaspersky Security Center に MySQL DBMSを使用する場合、InnoDB および MEMORY ストレージおよび UTF-8 と UCS-2 のエンコーディングのサポートを有効にします。

my.ini ファイルの推奨設定

my.ini ファイルを設定するには：

1. テキストエディターで my.ini ファイルを開きます。

2. ファイル my.ini の [mysqld] セクションに、次の行を追加します：

   ```
   sort_buffer_size=10M
   join_buffer_size=20M
   tmp_table_size=600M
   max_heap_table_size=600M
   key_buffer_size=200M
   innodb_buffer_pool_size= 実際の値は想定される KAV データベースのサイズの 80% 以上に設定する必要があります
   innodb_thread_concurrency=20
   innodb_flush_log_at_trx_commit=0（多くの場合、サーバーは少ないトランザクションを使用します）
   innodb_lock_wait_timeout=300
   max_allowed_packet=32M
   max_connections=151
   max_prepared_stmt_count=12800
   table_open_cache=60000
   table_open_cache_instances=4
   ```

```
table_definition_cache=60000
```

`innodb_buffer_pool_size` 値で指定されたメモリは、サーバーの起動時に割り当てられることに注意してください。データベースのサイズが指定されたバッファサイズより小さい場合、必要なメモリのみが割り当てられます。割り当てられたメモリの実際のサイズは、指定されたバッファサイズよりも約 10% 大きくなります。詳細は、MySQL のドキュメントを参照してください。

このパラメータの値を「1」または「2」にすると MySQL の動作速度に悪影響を及ぼす可能性があるため、パラメータには「`innodb_flush_log_at_trx_commit = 0`」を使用してください。
［`innodb_file_per_table`］パラメータが［`1`］に設定されていることを確認します。

Kaspersky Security Center 15.1 と動作する PostgreSQL または Postgres Pro サーバーの設定

Kaspersky Security Center 15.1 は、PostgreSQL および Postgres Pro DBMS をサポートしています。これらの DBMS のいずれかを使用する場合は、DBMS サーバーパラメータを設定して、Kaspersky Security Center と DBMS の連携を最適化することを検討してください。

設定ファイルの既定のパスは：`C:\Program Files\PostgreSQL\<バージョン>\data\postgresql.conf`

PostgreSQL および Postgres Pro の推奨パラメータ：

- `shared_buffers` = DBMS がインストールされているデバイスの RAM の値の 25%
  RAM が 1 GB 未満の場合は、既定値のままにします。
- `max_stack_depth = 2 MB`
- `temp_buffers = 24 MB`
- `work_mem = 16 MB`
- `max_connections = 151`
- `max_parallel_workers_per_gather = 0`
- `maintenance_work_mem = 128MB`

［`standard_conforming_strings`］パラメータが既定値の［`on`］に設定されていることを確認します。
postgresql.conf ファイルを更新した後、設定を再ロードするか、サーバーを再起動します。詳細は、PostgreSQL のドキュメントを参照してください。

Postgres Pro 15.7 または Postgres Pro 15.7.1 を使用する場合は、`enable_compound_index_stats` パラメータを無効にします：

```
enable_compound_index_stats = off
```

PostgreSQL および Postgres Pro サーバーパラメータの詳細とパラメータの指定方法については、該当する DBMS のドキュメントを参照してください。

PostgreSQL および Postgres Pro のアカウントを作成および構成する方法の詳細は、次のトピックを参照してください：「PostgreSQL と Postgres Pro で作業するためのアカウントの設定」。

Kaspersky Endpoint Security for Android によるモバイルデバイスの管理

Kaspersky Endpoint Security for Android™ がインストールされているモバイルデバイス（以降、KES デバイスと表記）は、管理サーバーによって管理されます。Kaspersky Security Center は、KES デバイスを管理するために次の機能をサポートしています：

- モバイルデバイスをクライアントデバイスとして処理：
  - 管理グループに所属
  - 監視（ステータス、イベント、レポートの表示など）
  - Kaspersky Endpoint Security for Android のローカル設定の変更とポリシーの割り当て
- 一元管理モードでのコマンドの送信
- リモートによるモバイルアプリパッケージのインストール

管理サーバーは、KES デバイスを TLS、TCP ポート 13292 を使用して管理します。

管理サーバーへのインターネットアクセス

以下のケースでは、管理サーバーへのインターネットアクセスが必要になります：

- 定義データベース、ソフトウェアモジュール、カスペルスキー製品の定期的なアップデート
- サードパーティ製ソフトウェアのアップデート

  既定では、管理サーバーが管理対象デバイスに Microsoft 製品のアップデートをインストールするためにインターネット接続は必要ありません。たとえば、管理対象デバイスは、Microsoft Update サーバーから直接、または組織のネットワークに展開されている Microsoft Windows Server Update Services（WSUS）を使用して WindowsServer から、Microsoft ソフトウェアのアップデートをダウンロードできます。次の場合は、管理サーバーをインターネットに接続する必要があります。
  - 管理サーバーを WSUS サーバーとして使用する
  - Microsoft ソフトウェア以外のサードパーティ製ソフトウェアのアップデートをインストールする
- サードパーティ製ソフトウェアの脆弱性の修正

  管理サーバーで次のタスクを実行する場合は、インターネット接続が必要になります。
  - Microsoft ソフトウェアの脆弱性に対して推奨される修正のリストを作成する。このリストは、カスペルスキーのスペシャリストにより作成され、定期的に更新されます。
  - Microsoft ソフトウェア以外のサードパーティ製ソフトウェアで脆弱性を修正する。
- モバイルユーザーのデバイス（ノート PC）の管理
- リモートオフィスでのデバイスの管理
- リモートオフィスのプライマリ管理サーバーまたはセカンダリ管理サーバーとの通信
- モバイルデバイスの管理

このセクションでは、インターネットを介して管理サーバーにアクセスする一般的な方法について説明します。管理サーバーにインターネット経由でアクセスすることに焦点が当てられている場合は、管理サーバーの専用証明書が必要とされます。

インターネットアクセス：ローカルネットワーク上の管理サーバー

組織の内部ネットワーク内に管理サーバーが配置されている場合は、管理サーバーの TCP ポート 13000 でポート転送を使用して、外部からのアクセスを可能にすることを検討してください。モバイルデバイス管理が必要な場合は、TCP ポート 13292 を開放します。

インターネットアクセス：DMZ 内の管理サーバー

組織ネットワークの DMZ 内に管理サーバーが置かれている場合、組織の内部ネットワークにはアクセスできません。この場合、次の制限事項が適用されます：

- 管理サーバーは新しいデバイスを検出できません。
- 管理サーバーは、組織の内部ネットワーク上のデバイスに対して、強制インストールによるネットワークエージェントの初期導入を実行できません。

これが適用されるのは、ネットワークエージェントの初期インストールに対してのみです。ただし、ネットワークエージェントに関する以降のアップグレードやセキュリティ製品のインストールは、管理サーバーで実行できます。同時に、ネットワークエージェントの初期導入は、Microsoft® Active Directory® のグループポリシーを使用するなどのその他の方法で実行可能です。

- 管理サーバーは、UDP ポート 15000 を介して管理対象デバイスに通知を送信できません。ただし、このことは Kaspersky Security Center の動作に関して重要ではありません。
- 管理サーバーは Active Directory をポーリングできません。ただし、たいていの場合、Active Directory をポーリングした結果は必要にはなりません。

上記の制限事項によって大きな問題が発生する場合は、組織ネットワーク内に置かれているディストリビューションポイントを使用して、これらの制限事項を取り除くことができます：

- 複数のデバイスでネットワークエージェントを使用せずに初期導入を実行するには、最初にいずれかのデバイスにネットワークエージェントをインストールしてから、そのネットワークエージェントにディストリビューションポイントステータスを割り当てます。そうすることにより、管理サーバーがこのディストリビューションポイントを使用して、その他のデバイスにネットワークエージェントを初期インストールできるようになります。
- 組織の内部ネットワーク上で新しいデバイスを検出して Active Directory をポーリングするには、いずれかのディストリビューションポイントで該当するデバイスの検出手法を有効にする必要があります。

組織の内部ネットワーク内にある管理対象デバイスから UDP ポート 15000 に対して正常に通知を送信するには、ネットワーク全体がディストリビューションポイントの管理下にある必要があります。割り当てたディストリビューションポイントのプロパティで、［**管理サーバーから切断しない**］をオンにします。その結果、管理サーバーがディストリビューションポイントに常時接続できるようになると同時に、ディストリビューションポイントは組織の内部ネットワーク（IPv4 または IPv6 ネットワーク）内のデバイスの UDP ポート 15000 に対して通知を送信できるようになります。

インターネットアクセス：DMZ 内でネットワークエージェントを接続ゲートウェイとして使用する

管理サーバーは組織の内部ネットワーク上に配置でき、そのネットワークの DMZ にはリバース接続の接続ゲートウェイとして実行中のネットワークエージェントをインストールしたデバイスを 1 台配置できます（管理サーバーはネットワークエージェントへの接続を確立します）。この場合、インターネットアクセスを確保するために次の条件を満たしている必要があります：

- ネットワークエージェントが、DMZ 内にあるデバイスにインストールされている。ネットワークエージェントのインストール時に、セットアップウィザードの［**接続ゲートウェイ**］ウィンドウで［**DMZ 内でネットワークエージェントを接続ゲートウェイとして使用する**］をオンにします。

- 接続ゲートウェイがインストールされているデバイスは、ディストリビューションポイントとして追加する必要があります。接続ゲートウェイを追加し、［**ディストリビューションポイントの追加**］ウィンドウで、［**選択**］→［**アドレスによる DMZ への接続ゲートウェイの追加**］をオンにします。

- インターネット接続を使用して外部デスクトップコンピューターを管理サーバーに接続するには、ネットワークエージェントのインストールパッケージの設定を修正する必要があります。作成したインストールパッケージのプロパティで、［**詳細**］→［**接続ゲートウェイを使用して管理サーバーに接続する**］をオンにし、新しく作成した接続ゲートウェイを指定します。

DMZ 内の接続ゲートウェイの場合、管理サーバーは管理サーバー証明書で署名された証明書を作成します。管理者が管理サーバーに対してカスタム証明書を割り当てる場合は、DMZ 内に接続ゲートウェイを作成する前に実行する必要があります。

ローカルネットワークまたはインターネットのいずれかを介して管理サーバーに接続可能なノート PC を使用している従業員がいる場合は、ネットワークエージェントのポリシー内でネットワークエージェント用の切り替えルールを作成しておくと便利です。

ディストリビューションポイントの概要

ネットワークエージェントがインストールされたデバイスはディストリビューションポイントとして使用できます。このモードでは、ネットワークエージェントは、次の機能を実行できます：

- アップデートの配信（アップデートは、管理サーバーまたはカスペルスキーのサーバーから取得します）。後者の場合、ディストリビューションポイントとして動作するデバイス上で*ディストリビューションポイントのリポジトリにアップデートをダウンロードタスク*を作成する必要があります：

  - その他のデバイスへのソフトウェアのインストール（ネットワークエージェントの初期導入を含む）。

  - 新しいデバイスを検出したり既存のデバイスの情報を更新するために、ネットワークを検索します。ディストリビューションポイントは管理サーバーと同じ方法でデバイスを検出できます。

組織ネットワークにディストリビューションポイントを導入する目的は次の通りです：

- 管理サーバーの負荷の低減

- トラフィックの最適化

- 組織ネットワークで接続経路を確保しにくい場所にあるデバイスへの管理サーバーアクセスの提供。NAT の内側に構成したネットワークでディストリビューションポイント（管理サーバーに関して）を使用すると、管理サーバーは次の処理を実行できます：

  - IPv4 または IPv6 ネットワークの UDP を経由したデバイスへの通知の送信

  - IPv4 または IPv6 ネットワークの検索

  - 初期導入の実行

  - プッシュサーバーとしての動作

1つの管理グループに対して、1つのディストリビューションポイントが割り当てられます。この場合、ディストリビューションポイントの範囲には、管理グループとそのすべてのサブグループ内にあるすべてのデバイスが含まれます。ただし、ディストリビューションポイントとして動作しているデバイスは、割り当てられている管理グループに含まれていなくてもかまいません。

ディストリビューションポイントを接続ゲートウェイとして動作させることができます。この場合、ディストリビューションポイントの範囲内のデバイスは、管理サーバーと直接接続されずゲートウェイを介して接続されます。このモードは、管理サーバーと管理対象デバイスの間を直接には接続できない場合に有効です。

Linux ベースのデバイスをディストリビューションポイントとして使用する場合、ディストリビューションポイントの対象範囲に多数のデバイスが含まれると、開くことができるファイルの既定の最大数では不十分になる可能性があるため、klnagent サービスのファイル記述子の上限を引き上げることを強く推奨します。

klnagent サービスのファイル記述子の上限を引き上げる

Linux ベースのディストリビューションポイントの対象範囲に多数のデバイスが含まれる場合、開くことができるファイル（ファイル記述子）の既定の制限では不十分な場合があります。これを回避するために、klnagent サービスのファイル記述子の上限を引き上げることができます。

klnagent サービスのファイル記述子の上限を引き上げるには：

1. ディストリビューションポイントとして機能する Linux ベースのデバイスで、ファイル `/lib/systemd/system/klnagent64.service` を開き、`[Service]` セクションの `LimitNOFILE` パラメータでファイル記述子のハード上限とソフト上限を指定します：

   `LimitNOFILE=<` ソフトリソース上限 `>:<` ハードリソース上限 `>`

   たとえば、`LimitNOFILE=32768:131072` と指定します。ファイル記述子のソフト上限はハード上限以下でなければならないことに注意してください。

2. パラメータが正しく指定されていることを確認するには、次のコマンドを実行します。

   ```
   systemd-analyze verify klnagent64.service
   ```

   パラメータが誤って指定されている場合、このコマンドは次のいずれかのエラーを出力する可能性があります：

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     このエラーが発生した場合、`LimitNOFILE` 行の記号が正しく指定されていません。入力した行を確認して修正する必要があります。

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     このエラーが発生した場合、入力したファイル記述子のソフト上限がハード上限を超えています。入力した行をチェックして、ファイル記述子のソフト上限がハード上限以下であることを確認する必要があります。

3. 次のコマンドを実行して、systemd プロセスを再読み込みします：

   ```
   systemctl daemon-reload
   ```

4. 次のコマンドを実行して、ネットワークエージェントサービスを再起動します：

   ```
   systemctl restart klnagent
   ```

5. 指定したパラメータが正しく適用されていることを確認するには、次のコマンドを実行します：

   ```
   less /proc/<nagent_proc_id>/limits
   ```

   `<nagent_proc_id>` パラメータは、ネットワークエージェントプロセスの識別子です。識別子を取得するには、次のコマンドを実行します：

```
ps -ax | grep klnagent
```

Linux ベースのディストリビューションポイントでは、開くことができるファイルの上限が引き上げられました。

ディストリビューションポイントの数の計算と設定

ネットワークに存在するクライアントデバイスの数に応じて、必要となるディストリビューションポイントの数も多くなります。ディストリビューションポイントの自動割り当ては、できるだけ使用しないでください。ディストリビューションポイントの自動割り当てが有効になっており、クライアントデバイスの数が非常に多い場合、管理サーバーがディストリビューションポイントの割り当てと設定を行います。

用途専用のディストリビューションポイントの使用

特定のデバイスをディストリビューションポイントとして使用する場合（たとえば、この用途専用で割り当てられたサーバー）、ディストリビューションポイントの自動割り当ては使用しないでください。また、ディストリビューションポイントとして使用するデバイスは、十分な空きディスク容量があること、定期的にシャットダウンされないこと、スリープモードが無効になっていることを確認してください。

単一のセグメントで構成されるネットワーク上での、デバイス数に応じた用途専用のディストリビューションポイントの数

ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
300 台未満	0（ディストリビューションポイントを割り当てない）
300 以上	許容：N/10,000 + 1、推奨：N/5,000 + 2（N はネットワーク上のデバイスの数）

複数のセグメントで構成されるネットワーク上での、デバイス数に応じた用途専用のディストリビューションポイントの数

各ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
10 台未満	0（ディストリビューションポイントを割り当てない）
10～100	1
100 以上	許容：N/10,000 + 1、推奨：N/5,000 + 2（N はネットワーク上のデバイスの数）

通常のクライアントデバイス（ワークステーション）のディストリビューションポイントとしての使用

通常のクライアントデバイス（ワークステーション）をディストリビューションポイントとして使用する場合、管理サーバーと通信チャネルの負荷低減のために、下表に従ってディストリビューションポイントを割り当ててください。

単一のセグメントで構成されるネットワーク上での、デバイス数に応じた、ディストリビューションポイントとして動作するワークステーションの数

ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
300 台未満	0（ディストリビューションポイントを割り当てない）
300 以上	N/300 + 1（N はネットワーク上のデバイスの数。ただし、ディストリビューションポイントは 3 台以上必要）

複数のセグメントで構成されるネットワーク上での、デバイス数に応じた、ディストリビューションポイントとして動作するワークステーションの数

各ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
10 台未満	0（ディストリビューションポイントを割り当てない）
10～30	1

31～300	2
300 以上	N/300 + 1（N はネットワーク上のデバイスの数。ただし、ディストリビューションポイントは 3 台以上必要）

ディストリビューションポイントがシャットダウンされた（もしくは、何らかの理由により使用できない）場合も、ディストリビューションポイントの対象範囲に含まれる管理対象デバイスは管理サーバーにアクセスしてアップデートを取得できます。

管理サーバーの階層構造

1 台の MSP で、複数台の管理サーバーを稼働させる場合があります。複数台の別の管理サーバーを管理するのは不便であるため、1 つの階層を適用することができます。2 台の管理サーバーのプライマリおよびセカンダリ設定には、次のオプションがあります：

- セカンダリ管理サーバーは、プライマリ管理サーバーからポリシーとタスクを継承することにより、設定の重複を防ぎます。
- プライマリ管理サーバーのデバイスには、セカンダリ管理サーバーのデバイスを含めることができます。
- プライマリ管理サーバーのレポートには、セカンダリ管理サーバーのデータ（詳細情報を含む）を含めることができます。

プライマリ管理サーバーは、上記のオプションの範囲内で非仮想セカンダリ管理サーバーからのみデータを受信します。この制限は、プライマリ管理サーバーと定義データベースを共有する仮想管理サーバーには適用されません。

仮想管理サーバー

物理管理サーバーに基づいて、複数台の仮想管理サーバーを作成できます。これは、セカンダリ管理サーバーと類似したものです。仮想管理サーバーモデルは、アクセス制御リスト（ACL）に基づいた任意のアクセスモデルと比較した場合、機能性が高く、高度の分離性を実現しています。ポリシーとタスクが存在する割り当て済みデバイスの管理グループ専用の構造に加えて、各仮想管理サーバーにも未割り当てデバイスのグループ、レポート、抽出されたデバイスとイベント、インストールパッケージ、移動ルールなどがあります。仮想管理サーバーの機能範囲は、サービスプロバイダー（xSP）が顧客の分離を最大化する用途でも、高度なワークフローと多くの管理者が存在する大規模な組織でも使用できます。

仮想管理サーバーはセカンダリ管理サーバーと非常に類似していますが、次の相違点があります：

- 仮想管理サーバーには、多数のグローバル設定と独自の TCP ポートが備えられていません。
- 仮想管理サーバーには、セカンダリ管理サーバーはありません。
- 仮想管理サーバーには、他の仮想管理サーバーはありません。
- 物理管理サーバーには、すべての仮想管理サーバーの管理対象デバイスに関するデバイス、グループ、およびオブジェクトが表示されます（隔離中の項目、アプリケーションレジストリなど）。
- 仮想管理サーバーがスキャンできるのは、ディストリビューションポイントが接続されているネットワークのみです。

Kaspersky Security Center の制限に関する情報

以下の表では、現在のバージョンの Kaspersky Security Center の制限事項を示しています。

Kaspersky Security Center の制限

制限の種別	値
管理サーバーあたりの管理対象デバイスの最大数	100000
［**管理サーバーから切断しない**］がオンになっているデバイス数の上限	300
管理グループ数の上限	10,000
保存するイベント数の上限	45,000,000
ポリシーの数の上限	2000
タスクの数の上限	2000
Active Directory オブジェクト（ユーザー、デバイス、セキュリティグループの組織単位（OU）とアカウント）の合計数の上限	1,000,000
ポリシーのプロファイル数の上限	100
単一のプライマリ管理サーバー上のセカンダリ管理サーバー数の上限	500
仮想管理サーバー数の上限	500
単一のディストリビューションポイントが対象にすることができるデバイス数の上限（ディストリビューションポイントはモバイルデバイス以外のみをサポートできます）	10,000
単一の接続ゲートウェイを使用できるデバイス数の上限	10,000（モバイルデバイスを含む）
管理サーバーあたりのモバイルデバイスの最大数	100,000 – モバイル以外の管理対象デバイスの数

ネットワーク負荷

このセクションでは、主要な管理処理中にクライアントデバイスと管理サーバーが交換するネットワークトラフィックの量について説明します。

主なネットワーク負荷は次の管理シナリオによって発生します：

- アンチウイルスによる保護の初期導入
- 定義データベースの初回アップデート
- クライアントデバイスと管理サーバーとの同期
- 定義データベースの定期的なアップデート
- クライアントデバイス上のイベントの管理サーバーによる処理

アンチウイルスによる保護の初期導入

このセクションでは、ネットワークエージェントおよび Kaspersky Endpoint Security for Windows をクライアントデバイスにインストールした後のトラフィック量について説明します（次の表を参照）。

セットアップに必要なファイルが管理サーバーからクライアントデバイス上の共有フォルダーにコピーされる場合、ネットワークエージェントが強制インストールでインストールされます。インストールが完了すると、ネットワークエージェントが管理サーバーへの接続を使用して Kaspersky Endpoint Security for Windows の配布パッケージを取得します（次の表を参照）。

トラフィック

シナリオ	1台のクライアントデバイスへのネットワークエージェントのインストール	1台のクライアントデバイスへの Kaspersky Endpoint Security for Windows のインストール（定義データベースのアップデートを含む）	ネットワークエージェントと Kaspersky Endpoint Security for Windows の同時インストール
クライアントデバイスから管理サーバーへのトラフィック（KB）	1638.4	7843.84	9707.52
管理サーバーからクライアントデバイスへのトラフィック（KB）	69,990.4	259,317.76	329,318.4
トラフィックの合計（クライアントデバイス1台）（KB）	71,628.8	267,161.6	339,025.92

ネットワークエージェントをクライアントデバイスにインストールしたら、管理グループ内のいずれかのデバイスをディストリビューションポイントとして割り当てることができます。それを使用してインストールパッケージを配布できます。この場合、アンチウイルスによる保護の初期導入におけるトラフィック量は、IP マルチキャストを使用するかどうかによって大幅に変わります。

IP マルチキャストを使用すると、インストールパッケージは、管理グループ内の稼働中のデバイスすべてに一度だけ配布されます。したがって、管理グループ内で動作中のデバイスの総数が N 台とすると、トラフィックの合計は N 分の 1 になります。IP マルチキャストを使用しないと、トラフィックの合計は、配布パッケージを管理サーバーからダウンロードする時のトラフィックと同一です。ただし、インストールパッケージは管理サーバーからではなくディストリビューションポイントからダウンロードされます。

定義データベースの初回アップデート

定義データベースの初回アップデート（定義データベースのアップデートタスクをクライアントデバイスで最初に実行する時）のトラフィックレートは、次の通りです：

- クライアントデバイスから管理サーバーへのトラフィック：1.8 MB。
- 管理サーバーからクライアントデバイスへのトラフィック：113 MB。
- トラフィックの合計（クライアントデバイス 1 台）：114 MB。

データは、定義データベースのバージョンによって若干異なることがあります。

クライアントと管理サーバーの同期

このシナリオは、クライアントデバイスと管理サーバーの間でデータの完全な同期が行われる場合の管理システムの状態を示します。クライアントデバイスは、管理者が定義した間隔で管理サーバーに接続します。管理サーバーは、クライアントデバイス上のデータの状態をサーバーと比較し、前回のクライアントデバイスとの接続に関する情報をデータベースに記録してデータを同期します。

このセクションでは、クライアントを管理サーバーに接続する基本的な管理シナリオを想定した時のトラフィック値の情報を記載しています（次の表を参照）。表中のデータは、定義データベースのバージョンによって若干異なることがあります。

トラフィック

シナリオ	クライアントデバイスから管理サーバーへのトラフィック（KB）	管理サーバーからクライアントデバイスへのトラフィック（KB）	トラフィックの合計（クライアントデバイス1台）（KB）
初回の同期（クライアントデバイスの定義データベースのアップデート前）	699.44	568.42	1267.86
初回の同期（クライアントデバイスの定義データベースのアップデート後）	735.8	4474.88	5210.68
クライアントデバイス（変更なし）	11.99	6.73	18.72

と管理サーバーの同期			
グループポリシーの設定値を変更した後の同期	9.79	11.39	21.18
グループタスクの設定値を変更した後の同期	11.27	11.72	22.99
クライアントデバイス（変更なし）の強制同期	77.59	99.45	177.04

合計トラフィック量は、管理グループで IP マルチキャストを使用するかどうかによって大幅に変わります。IP マルチキャストを使用した場合、管理グループ内で動作中のデバイスの総数が N 台であるとすると、そのグループのトラフィック量の合計は N 分の 1 になります。

定義データベースアップデート前後の初回同期時のトラフィック量は、次の場合に対して定義されます：

- ネットワークエージェントとセキュリティ製品をクライアントデバイスにインストールする
- クライアントデバイスを管理グループに移動する
- 既定のグループ用に作成されたポリシーやタスクを、クライアントデバイスに適用する

この表は、Kaspersky Endpoint Security のポリシー設定に含まれるプロテクション設定のいずれかを変更する場合のトラフィック量を示しています。他のポリシー設定についてのデータは、表に示されているデータとは異なることがあります。

定義データベースの追加アップデート

定義データベースの前回のアップデートから 20 時間後に増分アップデートを実行した場合のトラフィック量は次の通りです：

- クライアントデバイスから管理サーバーへのトラフィック：169 KB。
- 管理サーバーからクライアントデバイスへのトラフィック：113 MB。
- トラフィックの合計（クライアントデバイス 1 台）：16.3 MB。

表中のデータは、定義データベースのバージョンによって若干異なることがあります。

トラフィック量は、管理グループで IP マルチキャストを使用するかどうかによって大幅に変わります。IP マルチキャストを使用した場合、管理グループ内で動作中のデバイスの総数が N 台であるとすると、そのグループのトラフィック量の合計は N 分の 1 になります。

管理サーバーによるクライアントイベントの処理

このセクションでは、「ウイルスの検知」のイベントがクライアントデバイスで発生した場合のトラフィック量について記載しています（次の表を参照）。このイベントは、管理サーバーに転送され、管理サーバーのデータベースに登録されます。

トラフィック

シナリオ	ウイルスの検知イベント発生時の、管理サーバーへのデータ送信	ウイルスの検知イベント発生時（9 件）の管理サーバーへのデータ送信
クライアントデバイスから管理サーバーへのトラフィック（KB）	49.66	64.05
管理サーバーからクライアントデバイスへのトラフィック（KB）	28.64	31.97
トラフィックの合計（クライアントデバイス 1 台）（KB）	78.3	96.02

表中のデータは、アンチウイルス製品の現在のバージョン、および管理サーバーのデータベースに登録に使用するポリシーに定義されているイベントによって若干異なることがあります。

24 時間あたりのトラフィック

このセクションでは、管理システムの活動が平穏な状態（データの変更がクライアントデバイスでも管理サーバーでも発生していない）での、24 時間あたりのトラフィック率の情報を記載しています（次の表を参照）。

表中のデータは、Kaspersky Security Center の標準インストール、およびクイックスタートウィザードの完了後のネットワークの状態を示しています。クライアントデバイスと管理サーバーの同期間隔は 20 分です。アップデートは管理サーバーのリポジトリへ 1 時間に 1 回ダウンロードされます。

アイドル状態時の 24 時間ごとのトラフィック率

トラフィックフロー	値
クライアントデバイスから管理サーバーへのトラフィック（KB）	3235.84
管理サーバーからクライアントデバイスへのトラフィック（KB）	64,378.88
トラフィックの合計（クライアントデバイス 1 台）（KB）	67,614.72

モバイルデバイス管理の準備

このセクションでは、次の項目について説明します：

- 専用の iOS MDM プロファイルを iOS デバイスにインストールしてそれらのデバイスを管理する iOS MDM サーバーについて
- Kaspersky Endpoint Security for Android がインストールされたモバイルデバイスの管理について

iOS MDM サーバー

iOS MDM サーバーでは、iOS デバイスに専用 iOS MDM プロファイルをインストールすることにより、iOS デバイスを管理できます。次の機能がサポートされています：

- デバイスのロック
- パスワードのリセット
- データ消去
- アプリのインストールまたは削除
- 詳細設定による iOS MDM プロファイルの使用（VPN 設定、メール通知の設定、Wi-Fi 設定、カメラ設定、証明書など）

iOS MDM サーバーは、TLS ポート（既定では、ポート 443）を介してモバイルデバイスから受信接続を受け取る Web サービスです。これは、ネットワークエージェントを使用して Kaspersky Security Center で管理されます。ネットワークエージェントは、iOS MDM サーバーが導入されているデバイスにローカルにインストールされます。

iOS MDM サーバーの導入時、管理者は次の処理を実行する必要があります：

- ネットワークエージェントに対する管理サーバーへのアクセス権限の提供
- モバイルデバイスに対する iOS MDM サーバーの TCP ポートへのアクセス権限の提供

このセクションでは、iOS MDM サーバーの 2 つの標準設定について説明します。

標準設定：DMZ 内の Kaspersky Device Management for iOS

iOS MDM サーバーは、インターネットアクセスできる組織のローカルネットワークの DMZ 内に置かれています。この方法の利点は、デバイスからインターネットを介して iOS MDM Web サービスにアクセスした際に一切問題が発生しないということです。

iOS MDM サーバーを管理する際には、ネットワークエージェントをローカルにインストールする必要があるため、ネットワークエージェントと管理サーバーの間で対話が実行されていることを確認する必要があります。次のいずれかの方法で確認します：

- 管理サーバーを DMZ に移動します。
- 接続ゲートウェイを使用します：
  a. iOS MDM サーバーが導入されているデバイスで、接続ゲートウェイを介してネットワークエージェントを管理サーバーに接続します。
  b. iOS MDM サーバーが導入されているデバイスで、ネットワークエージェントを接続ゲートウェイとして動作するように割り当てます。

標準設定：組織のローカルネットワーク内の iOS MDM サーバー

iOS MDM サーバーは、組織の内部ネットワーク上に置かれています。たとえば、Kerberos 制約付き委任をサポートするリバースプロキシ上で iOS MDM Web サービスを公開することによって、ポート 443（既定ポート）を外部アクセスに対して有効にする必要があります。

標準設定では、TCP ポート 2197 を介して iOS MDM サーバー（範囲 17.0.0.0/8）の Apple Web サービスにアクセスする必要があります。このポートは、APNs と呼ばれる専用サービスにより、デバイスに新しいコマンドを通知するために使用されます。

Kaspersky Endpoint Security for Android によるモバイルデバイスの管理

Kaspersky Endpoint Security for Android™ がインストールされているモバイルデバイス（以降、KES デバイスと表記）は、管理サーバーによって管理されます。Kaspersky Security Center は、KES デバイスを管理するために次の機能をサポートしています：

- モバイルデバイスをクライアントデバイスとして処理：
  - 管理グループに所属
  - 監視（ステータス、イベント、レポートの表示など）
  - Kaspersky Endpoint Security for Android のローカル設定の変更とポリシーの割り当て
- 一元管理モードでのコマンドの送信
- リモートによるモバイルアプリパッケージのインストール

管理サーバーは、KES デバイスを TLS、TCP ポート 13292 を使用して管理します。

管理サーバーのパフォーマンスに関する情報

このセクションでは、各種ハードウェア設定での管理サーバーのパフォーマンステストの結果、および管理対象デバイスから管理サーバーへの接続の制限について説明します。

管理サーバーへの接続の制限

管理サーバーは、パフォーマンスを低下させることなく、最大 10 万台のデバイスの管理に対応します。

パフォーマンスを低下させずに管理サーバーへの接続に課す制限：

- 1 台の管理サーバーで最大 500 の仮想管理サーバーをサポートできます。
- プライマリ管理サーバーが同時にサポートするセッション数は 1000 以下です。
- 仮想管理サーバーが同時にサポートするセッション数は 1000 以下です。

管理サーバーパフォーマンステストの結果

管理サーバーのパフォーマンステストの結果により、管理サーバーが特定の時間内に同期できるクライアントデバイス数の上限を決定できます。この情報により、コンピューターネットワークにおけるアンチウイルスの実装に最適なスキームを選択できます。

テストに使用されたハードウェアの設定は下表の通りです：

管理サーバー用ハードウェアの設定

パラメータ	値
CPU	Intel Xeon CPU E5630、クロック速度：2.53 GHz、ソケット数：2 2、コア数：8、論理プロセッサ数：16
メモリ	26 GB
ハードディスク	IBM ServeRAID M5014 SCSI Disk Device、487 GB
オペレーティングシステム	Microsoft Windows Server 2019 Standard, バージョン 10.0.17763、ビルド 17763
ネットワーク	QLogic BCM5709C Gigabit Ethernet（NDIS VBD Client）

SQL Server デバイスのハードウェア設定

パラメータ	値
CPU	Intel Xeon CPU E5450、クロック速度：2.93 GHz、ソケット数：2、コア数：8、論理プロセッサ数：16
メモリ	32 GB
ハードディスク	Adaptec Array SCSI Disk Device、2047 GB
オペレーティングシステム	Microsoft Windows Server 2019 Standard, バージョン 10.0.17763、ビルド 17763
ネットワーク	Intel 82576 Gigabit

管理サーバーは、500 台の仮想管理サーバーの作成をサポートしていました。

同期は、10,000 台の管理対象デバイスに対して 15 分間隔でした（下表参照）。

管理サーバー負荷のテスト結果概要

同期間隔（分）	管理対象デバイスの数
15	10,000

30	20000
45	30,000
60	40,000
75	50,000
90	60,000
105	70,000
120	80,000
135	90,000
150	100000

管理サーバーから接続しているデータベースサーバーが、MySQL または SQL Express の場合、10,000 台を超えるデバイスを管理しないようにすることを推奨します。MariaDB のデータベース管理システムでは、推奨される最大の管理対象デバイス数は 20,000 台です。

KSN プロキシサーバーのパフォーマンステストの結果

社内ネットワークに多数のクライアントデバイスが含まれており、これらのクライアントデバイスが管理サーバーを KSN プロキシサーバーとして使用している場合、クライアントデバイスからのリクエストを処理するために管理サーバーのハードウェアは一定の要件を満たす必要があります。ネットワーク上の管理サーバーの負荷を評価し、KSN プロキシサービスが正常に動作するようにハードウェアリソースの計画を策定することを目的として、以下のテスト結果を使用できます。

下の表に管理サーバーと SQL Server のハードウェア構成を示します。構成はテストで使用されていました。

管理サーバー用ハードウェアの設定

パラメータ	値
CPU	Intel Xeon CPU E5450、クロック速度：3.00 GHz、ソケット数：2、コア数：8、論理プロセッサ数：16
メモリ	32 GB
オペレーティングシステム	Microsoft Windows Server 2016 Standard

SQL Server 用ハードウェアの設定

パラメータ	値
CPU	Intel Xeon CPU E5450、クロック速度：3.00 GHz、ソケット数：2、コア数：8、論理プロセッサ数：16
メモリ	32 GB
オペレーティングシステム	Microsoft Windows Server 2019 Standard

次の表にテスト結果をまとめています。

KSN プロキシサーバーのパフォーマンステストの結果概要

パラメータ	値
1秒あたりに処理できるリクエストの最大数	4914
CPU の最大使用率	36%

外部サービスとの相互対話のためのネットワーク設定

Kaspersky Security Center は、外部サービスと対話するために次のネットワーク設定を使用します。

ネットワーク設定

ネットワーク設定	アドレス	説明
ポート：443 プロトコル：HTTPS	activation-v2.kaspersky.com/activationservice/activationservice.svc	アプリケーションのアクティベーション。
ポート：443 プロトコル：HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデート。
ポート：443 プロトコル：HTTPS	https://www.kaspersky.co.jp/downloads	• 定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデート。 • カスペルスキーサーバーにアクセスできるかどうかを確認しています。 Kaspersky Security Center は、カスペルスキーのデータベースとソフトウェアをダウンロードする前にカスペルスキーのサーバーがアクセス可能かどうかをチェックします。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。
ポート：80 プロトコル：HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com	定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデート

	http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	
ポート：443 プロトコル：HTTPS	ds.kaspersky.com	Kaspersky Security Network の使用。
ポート：443、1443 プロトコル：HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Kaspersky Security Network の使用。
プロトコル：HTTPS	click.kaspersky.com redirect.kaspersky.com	インターフェイスからリンクをたどります。
ポート：80 プロトコル：HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	これらのサーバーは公開鍵インフラストラクチャ (PKI) の一部であり、カスペルスキーのデジタル署名証明書の有効性ステータスを確認するために必要です。CRL は失効した証明書のリストです。OCSP を使用すると、特定の証明書のステータスをリアルタイムで要求できます。これらのサーバーは、デジタル証明書との対話のセキュリティを確保し、起こり得る攻撃から保護するのに役立ちます。
ポート：443 プロトコル：HTTPS	https://ipm-klca.kaspersky.com	マーケティング関連告知。

Kaspersky Security Center と外部サービスとを適切に連携させるには、次の推奨事項を考慮してください：
- 組織のネットワーク機器およびプロキシサーバーのポート 443 および 1443 で、暗号化されていないネットワークトラフィックを許可する必要があります。
- 管理サーバーがカスペルスキーのアップデートサーバーおよび Kaspersky Security Network サーバーと通信する場合、証明書の置換によるネットワークトラフィックのハイジャック（MITM 攻撃）を回避する必要があります。

klscflag ユーティリティを使用して、HTTP または HTTPS プロトコル経由でアップデートをダウンロードするには、次の手順を実行します：

1. Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

2. HTTP プロトコル経由でアップデートをダウンロードする場合は、次のコマンドのいずれかを実行します：

   - 管理サーバーがインストールされたデバイスで：

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - ディストリビューションポイントについて：

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   HTTPS プロトコル経由でアップデートをダウンロードする場合は、次のコマンドのいずれかを実行します：

   - 管理サーバーがインストールされたデバイスで：

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - ディストリビューションポイントについて：

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

ネットワークエージェントとセキュリティ製品の導入

組織内でデバイスを管理するには、各デバイスにネットワークエージェントをインストールする必要があります。組織用デバイスに配信された Kaspersky Security Center を導入すると、通常はそのデバイスでネットワークエージェントのインストールが開始されます。

Microsoft Windows XP では、ネットワークエージェントが次の動作を正常に実行できない可能性があります：カスペルスキーのサーバーからのアップデートの直接ダウンロード（ディストリビューションポイントとして動作している場合）、KSN プロキシサーバーとしての動作（ディストリビューションポイントとして動作している場合）、サードパーティ製品の脆弱性の検知（脆弱性とパッチ管理機能を使用している場合）

初期導入

デバイスに既にネットワークエージェントがインストールされている場合は、このネットワークエージェントを使用してデバイスにアプリケーションがリモートインストールされます。インストールするアプリケーションの配布パッケージは、管理者が定義したインストール設定とともに、ネットワークエージェントと管理サーバー間の通信チャネルを介して転送されます。配布パッケージを転送するには、転送配布用のノードを使用します。例：ディストリビューションポイント、マルチキャストによる配布など。ネットワークエージェントがインストール済みである管理対象デバイスへのアプリケーションのインストール方法に関する詳細は、このセクションの下を参照してください。

次のいずれかの手法を使用して、Windows を実行中のデバイスにネットワークエージェントの初期インストールを実行できます：

- アプリケーションをリモートインストールするためにサードパーティ製のツールを使用する。
- オペレーティングシステムとネットワークエージェントをインストールした管理者のハードディスクのイメージをクローン化する：ディスクイメージ処理用として Kaspersky Security Center から提供されたツールを使用するか、またはサードパーティ製のツールを使用する。
- Windows のグループポリシーを使用する：グループポリシー用の標準の Windows 管理ツールを使用するか、または Kaspersky Security Center のリモートインストールタスクで、対応する専用オプションを自動的に使用する。
- Kaspersky Security Center のリモートインストールタスクで、特別なオプションを強制的に使用する。
- Kaspersky Security Center が生成したスタンドアロンパッケージに対して、デバイスユーザーリンクを送信する。スタンドアロンパッケージは、選択したアプリケーションの配布パッケージを含む、設定が定義された実行モジュールです。
- デバイスで手動によりアプリケーションインストーラーを実行する。

Microsoft Windows 以外のプラットフォームを実行している管理対象デバイスでは、ネットワークエージェントのリモートインストールを実行できます。Linux または macOS が動作しているデバイスにネットワークエージェントをリモートインストールする前に、デバイスを準備する必要があります。応答ファイルを使用して、サイレントモードで Linux デバイスにネットワークエージェントをインストールすることもできます。ネットワークエージェントを新しいバージョンにアップグレードする、または Windows 以外のプラットフォームに他のカスペルスキー製品をインストールするには、デバイス上にインストール済みのネットワークエージェントを使用してリモートインストールタスクを実行します。この場合、インストール方法は Microsoft Windows を実行しているデバイスの場合と同じです。

管理対象ネットワーク内に製品を導入するための方法と戦略を選択する際には、いくつかの要素について検討する必要があります（部分的なリスト）：

- 組織ネットワークの設定
- デバイスの合計数
- 組織ネットワーク上で、いずれの Active Directory ドメインにも属していないデバイスの有無、およびそのデバイスに関して管理者権限を付与されている統一アカウントの有無
- 管理サーバーとデバイス間のチャネルの容量
- 管理サーバーとリモートサブネット間の通信の種別、およびそのサブネット内のネットワークチャネルの容量
- 導入開始時にリモートデバイスに適用されているセキュリティ設定（UAC および簡易ファイルの共有モードの使用など）

インストーラーを設定する

ネットワーク上へのカスペルスキー製品の導入を開始する前に、アプリケーションのインストール時に定義するインストール設定を指定する必要があります。ネットワークエージェントをインストールする際には、最低でも管理サーバーへの接続に使用するアドレスを指定する必要があり、いくつかの詳細設定が必要になる場合もあります。選択したインストール方法に応じて、いくつかの方法で設定を定義できます。最も簡単な方法（選択したデバイスへの手動による対話式インストール）では、インストーラーのユーザーインターフェイスを使用して、関連するすべての設定を定義できます。

この方法で設定を定義するのは、デバイスグループにサイレントでアプリケーションをインストールする場合には適切ではありません。一般には、管理者が一元管理モードで設定の値を指定する必要があります。この値は、選択したネットワーク接続デバイスでサイレントインストールを実行する際に引き続き使用できます。

インストールパッケージ

最初に説明するアプリケーションのインストール設定を定義する主な方法は汎用性があり、Kaspersky Security Center のツールおよび多数のサードパーティ製のツールを使用した、すべてのインストール方法に適しています。この方法は、Kaspersky Security Center にアプリケーションのインストールパッケージを作成する処理から構成されています。

インストールパッケージを作成するには、次の方法を使用します：

- 含まれている*記述子*を基にして、指定した配布パッケージから自動的に作成（インストールと結果分析のルール、およびその他の情報を含む kud 拡張子のファイル）
- 標準またはサポートされているアプリケーションのインストーラーの実行ファイルまたはネイティブ形式（.msi、.deb、.rpm）のインストーラーから

作成されたインストールパッケージは、サブフォルダーとファイルが格納されているフォルダーとして階層的に編成されます。インストールパッケージには元の配布パッケージの他に、編集可能な設定（インストールを完了するために必要なオペレーティングシステムの再起動を処理するための、インストーラーの設定とルールを含む）と小規模な予備モジュールが含まれています。

サポートされている個別のアプリケーションに固有のインストール設定の値は、インストールパッケージの作成時に管理コンソールのユーザーインターフェイスで定義できます。Kaspersky Security Center のツールを使用してアプリケーションをリモートインストールする際には、インストールパッケージをデバイスに配布します。これで、アプリケーションのインストーラーを実行することにより、すべての管理者定義の設定がアプリケーションで使用できるようになります。カスペルスキー製品のインストールにサードパーティ製のツールを使用する際に必要になるのは、デバイスでインストールパッケージ全体（つまり、配布パッケージとその設定）を使用できるようにすることだけです。Kaspersky Security Center によってインストールパッケージが作成され、共有フォルダーの専用サブフォルダーに保存されます。

> インストールパッケージの設定では、特別な権限を持つアカウントを指定しないでください。

サードパーティ製のツールを使用して導入する前にカスペルスキー製品にこの設定方法を使用する方法については、「Microsoft Windows のグループポリシーを使用した導入」を参照してください。

Kaspersky Security Center のインストール直後には、自動的にいくつかのインストールパッケージが作成されます。これらのインストールパッケージはインストールの準備が完了しており、Microsoft Windows 用のネットワークエージェントパッケージとセキュリティ製品パッケージを含んでいます。

インストールパッケージのプロパティでアプリケーション用のライセンスを設定できますが、インストールパッケージへの読み取り権限は簡単に取得されてしまうため、このライセンス配信方法は避けるのが適切です。この場合、ライセンスの自動配信またはライセンスのインストールタスクを使用する必要があります。

MSI プロパティと変換ファイル

Windows プラットフォームでインストールを設定する別の方法は、MSI プロパティと変換ファイルを定義することです。この方法は次の場合に適用できます：

- Windows のグループポリシーを処理するために正規の Microsoft ツールまたはその他のサードパーティ製のツールを使用して、Windows のグループポリシーによりインストールを実行する場合
- Microsoft インストーラー形式のインストーラーを取り扱うためのサードパーティ製のツールを使用してアプリケーションをインストールする場合

アプリケーションのリモートインストールにおけるサードパーティ製のツールを使用した導入

組織でアプリケーションのリモートインストール用ツール（Microsoft System Center など）が使用可能な場合は、これらのツールを使用して初期導入を実行するのが便利です。

次の処理を実行する必要があります：

- 使用する導入ツールに最適なインストール設定方法を選択します。
- インストールパッケージの設定の変更（管理コンソールインターフェイスを使用）とインストールパッケージデータからのアプリケーション導入用として選択したサードパーティ製のツールの操作との間の同期メカニズムを定義します。
- 共有フォルダーからのインストールを実行する際には、このファイルリソースに十分な容量が存在することを確認する必要があります。

Kaspersky Security Center でのリモートインストールタスクの概要

Kaspersky Security Center には、アプリケーションのリモートインストール用の様々なメカニズムが用意されており、これらはリモートインストールタスクとして実装されています（強制インストール、ハードディスクイメージのコピーによるインストール、Microsoft Windows のグループポリシーを使用したインストール）。リモートインストールタスクは、特定のデバイスまたは選択したデバイスと指定した管理グループの両方に対して作成できます（このタスクは管理コンソールの［**タスク**］フォルダーに表示されます）。タスクを作成する際には、このタスク内にインストールする（ネットワークエージェントや別のアプリケーン用の）インストールパッケージを選択し、リモートインストール方法を定義するための特定の設定を指定することができます。さらに、リモートインストールタスクの作成と結果の監視に基づいた、リモートインストールウィザードも使用できます。

管理グループのタスクは、指定したグループに含まれるデバイスと、その管理グループ内のすべてのサブグループにあるすべてのデバイスの両方に影響を与えます。タスクは、対応する設定がそのタスク内で有効な場合、1つのグループまたはそのサブグループのいずれかに含まれるセカンダリ管理サーバーのデバイスに対応しています。

特定のデバイスに対するタスクでは、タスクが開始された時点での選択内容に従って、実行ごとにクライアントデバイスのリストが更新されます。選択内容に、セカンダリ管理サーバーに接続されているデバイスが含まれている場合は、そのデバイスでもタスクが実行されます。これらの設定とインストール方法の詳細については、このセクションの後半を参照してください。

セカンダリ管理サーバーに接続されているデバイスでリモートインストールタスクの操作を正常に実行するには、対応するセカンダリ管理サーバーに対して前もって、タスクで使用するインストールパッケージをリレーしておく必要があります。

デバイスのイメージの取得とコピーを使用した導入

オペレーティングシステムとその他のソフトウェアもインストール（または再インストール）する必要があるデバイスにネットワークエージェントをインストールする必要がある場合は、そのデバイスのイメージをキャプチャしてコピーするメカニズムを使用できます。

ハードディスクイメージの取得とコピーによる導入を実行するには：

1. オペレーティングシステムと関連するソフトウェア（ネットワークエージェントとセキュリティ製品を含む）がインストールされた基準デバイスを作成します。

2. デバイスの基準イメージを取得し、Kaspersky Security Center の専用タスクを使用して、そのイメージを新しいデバイスに配信します。

   ディスクイメージを取得してインストールするには、組織で使用可能なサードパーティ製のツールと、Kaspersky Security Center によって（脆弱性とパッチ管理ライセンスの下に）提供される機能のいずれかを使用できます。

サードパーティ製のツールを使用してディスクイメージを処理する場合は、デバイスで基準イメージからの導入を実行する際に、Kaspersky Security Center が管理対象デバイスの識別に使用している情報を削除する必要があります。そうしないと、同じイメージをコピーして作成されたデバイスを、管理サーバーが適切に区別できません。

Kaspersky Security Center のツールを使用してディスクイメージを取得する際は、この問題が自動的に解決されます。

サードパーティ製のツールを使用したディスクイメージのコピー

ネットワークエージェントがインストールされたデバイスのイメージの取得にサードパーティ製のツールを適用する際には、次のいずれかの方法を使用します：

- 推奨される方法。基準デバイスにネットワークエージェントをインストールする際には、ネットワークエージェントサービスを最初に実行する前にデバイスイメージを取得します（最初にネットワークエージェントを管理サーバーに接続する際に、デバイスを識別する一意の情報が作成されるため）。その後は、イメージ取得の操作が完了するまで、ネットワークエージェントサービスを実行しないでしてください。

- 基準デバイスでネットワークエージェントサービスを停止し、-dupfix キーにより klmover ユーティリティを実行します。klmover ユーティリティは、ネットワークエージェントのインストールパッケージに含まれています。イメージ取得の操作が完了するまで、ネットワークエージェントサービスを引き続き実行しないでください。

- イメージの導入後にオペレーティングシステムを初めて起動する際には、対象デバイスでネットワークエージェントサービスを最初に実行する前（必須要件）に、-dupfix キーにより klmover が実行されていることを確認してください。klmover ユーティリティは、ネットワークエージェントのインストールパッケージに含まれています。

- ネットワークエージェントのディスククローンモードを使用します。

ハードディスクイメージが正しくコピーされていない場合は、この問題を解決できます。

ネットワークエージェントがインストールされていないデバイスのイメージをキャプチャすることもできます。これを行うには、対象デバイスでイメージの導入を実行してから、ネットワークエージェントを導入します。この方法を使用する場合は、デバイスからスタンドアロンイントールパッケージを含むネットワークフォルダーへのアクセスを提供します。

ハードディスクイメージの誤ったコピー

ネットワークエージェントがインストールされたハードディスクイメージが導入ルールに従わずにコピーされた場合は、管理コンソールで、名前が常に変更される 1 つのアイコンの下にいくつかのデバイスがまとめて表示されることがあります。

この問題は、次のいずれかの方法で解決できます：

- ネットワークエージェントの削除

  この方法は最も信頼性があります。サードパーティ製のツールを使用して、イメージから適切にコピーされていないデバイスのネットワークエージェントを削除し、再度インストールする必要があります。ネットワークエージェントは、Kaspersky Security Center ツールから削除できません。管理サーバーが不完全なデバイスを識別できないためです（すべてのデバイスは、管理コンソールで同じアイコンを共有します）。

- 「-dupfix」キーを使用した klmover ユーティリティの実行

  サードパーティ製のツールを使用して、ネットワークエージェントのインストールフォルダーにある klmover ユーティリティを、「-dupfix」キーを使用して（klmover -dupfix）、不完全なデバイス（イメージから適切にコピーされていないデバイス）で一度実行します。このユーティリティは、Kaspersky Security Center ツールでは実行できません。管理サーバーが不完全なデバイスを識別できないためです（すべてのデバイスは、管理コンソールで同じアイコンを共有します）。

  その後、ユーティリティを実行する前に、不完全なデバイスが表示されているアイコンを削除します。

- 適切にコピーされていないデバイスの検出ルールの強化

  この方法は、バージョン 10 Service Pack 1 以降の管理サーバーとネットワークエージェントがインストールされている場合にのみ適用できます。

  適切にコピーされていないネットワークエージェントの検出ルールを強化する必要があります。そうすることで、デバイスの NetBIOS 名を変更すると、それらのネットワークエージェントが自動的に「修正」されます（コピーされたデバイスはすべて、一意の NetBIOS 名を持つことが前提）。

管理サーバーがインストールされたデバイスでは、以下に示す reg ファイルをレジストリにインポートしてから、管理サーバーサービスを再起動する必要があります。

- 管理サーバーがインストールされたデバイスに 32 ビットのオペレーティングシステムがインストールされている場合：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

- 管理サーバーがインストールされたデバイスに 64 ビットのオペレーティングシステムがインストールされている場合：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

Microsoft Windows のグループポリシーを使用した導入

次の条件を満たしている場合は、Microsoft Windows のグループポリシーを使用してネットワークの初期導入を実行してください：

- デバイスが Active Directory ドメインに属している。
- 対象デバイスへのネットワークエージェントの導入を開始する前に、導入スキームを使用して、対象デバイスの次回の定期的な再起動を待機できる（または、これらのデバイスに対して、Windows のグループポリシーを強制的に適用できる）。

この導入スキームは以下で構成されます：

- Microsoft インストーラー形式（MSI パッケージ）のアプリケーション配布パッケージは、共有フォルダー（対象デバイスの LocalSystem アカウントに読み取り権限が付与されているフォルダー）に置かれています。
- インストールオブジェクトは、Active Directory のグループポリシー内で配布パッケージ用として作成されます。
- インストール対象を設定するには、対象デバイスが含まれている、組織単位（OU）またはセキュリティグループを指定します。
- 対象デバイスの次回のドメインへのログイン時に（デバイスユーザーがシステムにログインする前）、必要なアプリケーションの有無を調べるために、インストールされているすべてのアプリケーションがチェックされます。アプリケーションが見つからない場合は、ポリシーで指定したリソースから配布パッケージがダウンロードされてインストールされます。

この導入スキームの利点は、オペレーティングシステムの読み込み時に、ユーザーがシステムにログインする前であっても、割り当て済みアプリケーションが対象デバイスにインストールされることです。十分な権限を付与されたユーザーがアプリケーションを削除した場合でも、次回のオペレーティングシステム起動時にアプリケーションが再インストールされます。一方、この導入スキームの欠点は、デバイスが再起動されるまで、グループポリシーに対して管理者が行った変更内容が有効にならないことです（別のツールが含まれていない場合）。

ネットワークエージェントとその他のアプリケーションは、それぞれのインストーラーが Windows インストーラー形式である場合、グループポリシーを使用して両方をインストールできます。

この導入スキームを選択する際は、Windows のグループポリシー適用後に、ファイルをデバイスにコピーする元のファイルリソースの負荷についても評価する必要があります。

Kaspersky Security Center のリモートインストールタスクを使用した Microsoft Windows のポリシーの処理

Microsoft Windows のグループポリシーを使用してアプリケーションをインストールする最も簡単な方法は、Kaspersky Security Center のリモートインストールタスクのプロパティで［**Active Directory のグループポリシーにパッケージのインストールを割り当てる**］をオンにすることです。この場合、タスクの実行時に管理サーバーが自動的に次の処理を実行します：

- Microsoft Windows のグループポリシー内に必要なオブジェクトを作成する。
- 専用のセキュリティグループを作成し、そのグループに対象デバイスを含めてから、そのデバイスに選択したアプリケーションのインストールを割り当てる。タスクを実行するごとに、実行時点でのデバイスのプールに従って、セキュリティグループのセットをアップデートする。

この機能を有効にするには、タスクのプロパティで、Active Directory のグループポリシーで書き込み権限が付与されたアカウントを指定します。

同じタスクを使用してネットワークエージェントと別のアプリケーションの両方をインストールする場合は、［**Active Directory のグループポリシーにパッケージのインストールを割り当てる**］をオンにすることにより、アプリケーションがネットワークエージェントのみに対応するインストールオブジェクトを Active Directory のポリシー内に作成します。別のアプリケーションがデバイスにインストールされるとすぐに、ネットワークエージェントのツールを使用して、タスクで選択した 2 番目のアプリケーションがインストールされます。Windows のグループポリシーを使用してネットワークエージェント以外のアプリケーションをインストールする場合は、このインストールパッケージに対してのみ（ネットワークエージェントパッケージなしで）インストールタスクを作成する必要があります。Microsoft Windows のグループポリシーではインストールできないアプリケーションもあります。インストールの不可を確かめるには、アプリケーションのインストール方法に関する情報を参照してください。

Kaspersky Security Center のツールを使用して、グループポリシー内に必要なオブジェクトを作成する場合は、インストールパッケージのソースとして Kaspersky Security Center の共有フォルダーが使用されます。導入の計画時には、このフォルダーの読み取り速度と、デバイスの数およびインストールする配布パッケージのサイズを相互に関連付ける必要があります。高速の専用ファイルリポジトリで Kaspersky Security Center の共有フォルダーを見つける場合に便利です。

Kaspersky Security Center を使用した Windows のグループポリシーの自動作成は、使いやすさに加えて次の利点があります：ネットワークエージェントのインストールを計画している際には、インストールの完了後にデバイスが自動的に移動される先の Kaspersky Security Center の管理グループを簡単に指定できます。このグループは、新規タスクウィザードまたはリモートインストールタスクの設定ウィンドウで指定できます。

Kaspersky Security Center を使用して Windows のグループポリシーを処理する際には、セキュリティグループを作成することにより、グループポリシーオブジェクト用のデバイスを指定できます。Kaspersky Security Center は、セキュリティグループの内容をタスク内にあるデバイスの現在のセットと同期します。グループポリシーの処理に他のツールを使用する際には、グループポリシーのオブジェクトを Active Directory で選択した OU に直接関連付けることができます。

Microsoft Windows のポリシーを使用した、アプリケーションのサポートされていないインストール

管理者は自分用に、Windows のグループポリシー内にインストールに必要なオブジェクトを作成できます。この場合、管理者は Kaspersky Security Center の共有フォルダーに格納されているパッケージへのリンクを指定するか、またはこのパッケージを専用ファイルサーバーにアップロードしてから、そのパッケージへのリンクを指定することができます。

可能なインストールシナリオは次の通りです：

- 管理者がインストールパッケージを作成し、管理コンソールでそのプロパティをセットアップします。グループポリシーオブジェクトにより、Kaspersky Security Center の共有フォルダーに格納されている、このパッケージの MSI ファイルへのリンクを指定します。

- 管理者がインストールパッケージを作成し、管理コンソールでそのプロパティをセットアップします。次に、管理者はこのパッケージの EXEC サブフォルダー全体を、Kaspersky Security Center の共有フォルダーから組織の専用ファイルリソースのフォルダーにコピーします。グループポリシーオブジェクトにより、組織の専用ファイルリソースのサブフォルダーに格納されている、このパッケージの MSI ファイルへのリンクを指定します。

- 管理者がインターネットを介してアプリケーション配布パッケージ（ネットワークエージェント用も含む）をダウンロードし、そのパッケージを組織の専用ファイルリソースにアップロードします。グループポリシーオブジェクトにより、組織の専用ファイルリソースのサブフォルダーに格納されている、このパッケージの MSI ファイルへのリンクを指定します。インストール設定は、MSI プロパティを設定するか、または MST 変換ファイルを設定することによって定義されます。

Kaspersky Security Center のリモートインストールタスクを使用した強制的な導入

ネットワークエージェントやその他のアプリケーションの初期導入を実行するには、各デバイスにローカル管理者権限を持つユーザーアカウントがあることを前提として、Kaspersky Security Center のリモートインストールタスクを使用して、選択したインストールパッケージを強制的にインストールできます。

管理サーバーがデバイスに直接アクセスできない場合は、強制インストールを適用することもできます。たとえば、デバイスが分離されたネットワーク上に配置されている場合や、管理サーバーが DMZ にあり、デバイスがローカルネットワーク上に配置されている場合が考えられます。

初期導入の場合、ネットワークエージェントはインストールされません。そのため、リモートインストールタスクの設定では、ネットワークエージェントを使用してアプリケーションのインストールに必要なファイルの配布を選択することはできません。管理サーバーまたはディストリビューションポイントを介してオペレーティングシステムリソースを使用してファイルを配布することのみを選択できます。

管理サーバーサービスは、ターゲットデバイスに対する管理者権限を持つアカウントで実行する必要があります。または、リモートインストールタスクの設定で、admin$ 共有にアクセスできるアカウントを指定することもできます。

> 既定では、リモートインストールタスクは、管理サーバーが実行されているアカウントの資格情報を使用してデバイスに接続します。これは、リモートインストールタスクが実行されるアカウントではなく、admin$ 共有にアクセスするために使用されるアカウントであることを明確にすることが重要です。インストールは LocalSystem アカウントで実行されます。

対象デバイスを指定する方法として、明示的に指定する（リストを使用）、対象デバイスが属する Kaspersky Security Center の管理グループを選択する、または特定の基準に基づいてデバイスの抽出内容を作成するのいずれかを使用できます。インストールの開始時刻は、タスクのスケジュールによって定義されます。タスクのプロパティで［**未実行のタスクを実行する**］設定をオンにすると、対象デバイスの電源をオンにした直後または対象デバイスを対象管理グループに移動した際に、タスクを実行できます。

強制インストールは、インストールパッケージの対象デバイスへの送信、その後の各対象デバイスの admin$ リソースへのファイルコピー、これらのデバイス上でのサポートデバイスのリモート登録で構成されます。インストールパッケージの対象デバイスへの送信は、ネットワーク対話を保証する Kaspersky Security Center 機能を介して実施されます。この場合、次の条件を満たしている必要があります：

- 対象デバイスには、管理サーバー側またはディストリビューションポイント側からアクセスできます。
- ネットワーク上で、対象デバイスの名前解決が正常に機能しています。
- 対象デバイスで、管理共有（admin$）が有効のままである。
- 対象デバイスでは次のシステムサービスが実行されています：
  - サーバー（LanmanServer）

    既定では、このサービスは実行されています。
  - DCOM サーバープロセスランチャー（DcomLaunch）
  - RPC エンドポイントマッパー（RpcEptMapper）
  - リモートプロシージャコール（RpcSs）
- Windows ツールを介したリモートアクセスを可能にするために、対象デバイスでポート TCP 445 が開かれます。

  > TCP 139、UDP 137、および UDP 138 は古いプロトコルで使用されており、現在のアプリケーションには必要ありません。

  管理サーバーおよびディストリビューションポイントから対象デバイスへの接続には、ファイアウォールで動的な送信アクセスポートを許可する必要があります。
- ネットワークエージェントを導入する時、Active Directory ドメインポリシーのセキュリティ設定により、NTLM プロトコルの動作が可能になります。
- Microsoft Windows XP を実行している対象デバイスで、シンプルファイル共有モードが無効になっている。
- 対象デバイスでは、アクセス共有とセキュリティモデルは「*クラシック – ローカルユーザーはローカルユーザー自身として認証*」に設定されます。決して「*ゲストのみ – ローカルユーザーはゲストとして認証*」に設定できません。
- 対象デバイスをドメインに属させるか、または管理者権限を付与された統一アカウントを対象デバイスで前もって作成する。

> Windows Server 2003 以降の Active Directory ドメインに参加していないデバイスにネットワークエージェントまたはその他のアプリケーションを正常に展開するには、そのデバイスでリモート UAC を無効にする必要があります。リモート UAC は、ネットワークエージェントやその他のアプリケーションの強制導入に必要な admin$ にローカル管理アカウントがアクセスできない原因の 1 つです。リモート UAC を無効にしても、ローカル UAC には影響しません。

まだいずれの Kaspersky Security Center の管理グループにも割り当てられていない新しいデバイスへのインストール時には、リモートインストールタスクのプロパティを開き、ネットワークエージェントのインストール後にデバイスの移動先の管理グループを指定できます。

グループタスクの作成時には、選択したグループ内のネストされたすべてのグループにあるすべてのデバイスに対して、各グループタスクが影響を与えることに注意してください。このため、サブグループ内でインストールタスクが重複しないようにする必要があります。

アプリケーションを強制インストールするためのタスクを作成する簡単な方法は、自動インストールです。この処理を実行するには、管理グループのプロパティを開いてから、インストールパッケージのリストを開き、このグループのデバイスにインストールする必要があるパッケージを選択しなければなりません。そうすると、このグループとそのすべてのサブグループ内にあるすべてのデバイスに、選択したインストールパッケージが自動的にインストールされます。パッケージのインストールに要する時間は、ネットワークのスループットとネットワーク接続されているデバイスの合計数に応じて異なります。

インストールパッケージを対象デバイスに配信する際に管理サーバーの負荷を軽減するには、インストールタスクでディストリビューションポイント経由のインストールを選択できます。ただし、このインストール方法では、ディストリビューションポイントとして動作しているデバイスの負荷が大幅に増大するのでご注意ください。したがって、ディストリビューションポイントの要件を満たすデバイスを選択することを推奨します。ディストリビューションポイントを使用する場合は、対象デバイスをホストする分離された各サブネットにディストリビューションポイントが存在することを確認する必要があります。

小容量チャネルを介して管理サーバーと通信するサブネット内のデバイスへのインストールを実行する際に、同じサブネット内のデバイス間で大容量チャネルが使用できる場合は、ディストリビューションポイントをローカルインストールのセンターとして使用することも役に立ちます。

%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit フォルダーのパーティションの空きディスク容量は、インストールされたアプリケーションの配布パッケージの合計サイズより何倍も大きな容量にする必要があります。

Kaspersky Security Center で作成された実行中のスタンドアロンパッケージ

上述のネットワークエージェントとその他のアプリケーションの初期導入方法は、適用される条件をすべて満たすことができないため、常に実装できるわけではありません。そのような場合は、Kaspersky Security Center で、管理者によって適切なインストール設定が行われているインストールパッケージを使用して、*スタンドアロンインストールパッケージ*と呼ばれる共通の実行ファイルを作成できます。スタンドアロンインストールパッケージは、Kaspersky Security Center の共通フォルダーに保存されています。

Kaspersky Security Center を使用して、共通フォルダーのこのファイルのリンクを記載したメールメッセージを、特定のユーザーに送信できます。そうすることで、（対話モードで、またはサイレントインストールのキー「-s」を使用して）ファイルを実行するようユーザーに促すことができます。Kaspersky Security Center の共有フォルダーにアクセスできないデバイスのユーザーには、スタンドアロンインストールパッケージをメールメッセージに添付して送信できます。管理者は、スタンドアロンパッケージをリムーバブルドライブにコピーし、関連のデバイスに配布し、後で実行することもできます。

スタンドアロンパッケージは、ネットワークエージェントパッケージ、別のアプリケーションのパッケージ（セキュリティ製品のパッケージなど）、またはその両方から作成できます。スタンドアロンパッケージをネットワークエージェントパッケージと別のアプリケーションから作成した場合、インストールはネットワークエージェントを使用して起動されます。

スタンドアロンパッケージをネットワークエージェントから作成する場合、ネットワークエージェントのインストールが完了した際に、新しいデバイス（管理グループのいずれにも割り当てられていないデバイス）が自動的に割り当てられる管理グループを指定できます。

スタンドアロンパッケージは、パッケージに含まれるアプリケーションのインストール結果が表示される対話モードで実行することも（既定）、サイレントモードで実行することもできます（キー「-s」を使用して実行した場合）。サイレントモードは、スクリプト（オペレーティングシステムイメージが導入された後に実行されるように設定されているスクリプトなど）からインストールする場合に使用できます。サイレントモードでは、インストール結果はプロセスのリターンコードから判断します。

アプリケーションの手動インストールのオプション

管理者や経験豊富なユーザーは、アプリケーションを対話モードにより手動でインストールできます。元の配布パッケージ、または元の配布パッケージから作成され、Kaspersky Security Center の共通フォルダーに保存されているインストールパッケージのいずれかを使用します。既定では、インストーラーは対話モードで実行され、必要な値をすべて入力するようユーザーに促します。ただし、キー「-s」を使用してインストールパッケージのルートからプロセス setup.exe を実行した場合は、インストーラーは、インストールパッケージの設定時に定義された設定を使用して、サイレントモードで実行されます。

Kaspersky Security Center の共通フォルダーに保存されているインストールパッケージのルートから setup.exe を実行した場合、まずパッケージが一時的なローカルフォルダーにコピーされ、その後、アプリケーションインストーラーがローカルフォルダーから実行されます。

MST ファイルの作成

MSI パッケージの内容を変換し、既存の MSI ファイルにカスタム設定を適用するには、MST 形式の変換ファイルを作成する必要があります。これを行うには、Windows SDK に含まれている Orca.exe エディターを使用します。

MST ファイルを作成するには：

1. Orca.exe エディターを実行します。
2. ［**ファイル**］タブに移動し、メニューで［**開く**］をクリックします。
3. ファイル Kaspersky Network Agent.msi を選択します。
4. ［**変換**］タブに移動し、メニューで［**新しい変換**］を選択します。
5. ［**テーブル**］列で［**プロパティ**］を選択し、次の値を入力します：
   - *EULA=1*
   - *SERVERADDRESS=<管理サーバーアドレス>*

   ［**保存**］をクリックします。
6. ［**変換**］タブに移動し、メニューで［**変換の生成**］を選択します。
7. 開いたウィンドウで、作成する変換ファイルの名前を指定し、［**保存**］をクリックします。

MST ファイルが保存されます。

ネットワークエージェントがインストールされたデバイスへのアプリケーションのリモートインストール

プライマリ管理サーバー（またはそのセカンダリ管理サーバーのいずれか）に接続された操作可能なネットワークエージェントがデバイスにインストールされた場合、このデバイスのネットワークエージェントのアップグレードや、ネットワークエージェント経由でサポートされる任意のアプリケーションのインストール、アップグレード、削除が可能です。

このオプションは、リモートインストールタスクのプロパティで［**ネットワークエージェントを使用する**］をオンにすることができます。

このオプションをオンにすると、管理者によってインストール設定が定義されたインストールパッケージは、ネットワークエージェントと管理サーバー間の通信チャネルを経由して対象デバイスに送信されます。

管理サーバーの負荷を最適化し、管理サーバーとデバイス間のトラフィックを最小化するには、すべてのリモートネットワークまたはすべてのブロードキャストドメインでディストリビューションポイントを割り当てるのが適切な方法です（「ディストリビューションポイントについて」および「管理グループの構造の構築とディストリビューションポイントの割り当て」を参照）。この場合、インストールパッケージとインストーラーの設定は、ディストリビューションポイント経由で管理サーバーから対象デバイスに配布されます。

さらに、ディストリビューションポイントをインストールパッケージのブロードキャスト（マルチキャスト）配信に使用できるため、アプリケーション導入時のネットワークトラフィックを大幅に削減できます。

ネットワークエージェントと管理サーバー間の通信チャネルを経由してインストールパッケージを対象デバイスに送信する場合、送信の準備が整っているすべてのインストールパッケージは、%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer フォルダーにもキャッシュされます。複数の様々な種別の大規模インストールパッケージと、多数のディストリビューションポイントを使用する場合、このフォルダーのサイズは急増する可能性があります。

FTServer フォルダーからファイルを手動で削除することはできません。元のインストールパッケージが削除された場合、FTServer フォルダーから関連データが自動的に削除されます。

ディストリビューションポイントが受信したデータはすべて、%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp フォルダーに保存されます。

$FTCITmp フォルダーからファイルを手動で削除することはできません。このフォルダーのデータを使用するタスクが完了すると、このフォルダーの中身は自動的に削除されます。

インストールパッケージは、管理サーバーとネットワークエージェント間の通信チャネルを経由して、ネットワーク送信用に最適化されたフォーマットで中間リポジトリから配布されるため、各インストールパッケージの元のフォルダーに保存されたインストールパッケージへの変更は許可されていません。そのような変更は、管理サーバーによって自動的に登録されません。インストールパッケージのファイルを手動で変更する必要がある場合は、管理コンソールでインストールパッケージの設定を編集しなければなりません（ただし、このようなシナリオは回避することが推奨されます）。管理コンソールでインストールパッケージの設定を編集すると、対象デバイスへの送信準備が整っているキャッシュ内のパッケージイメージが、管理サーバーによってアップグレードされてしまいます。

リモートインストールタスクに含まれるデバイス再起動を管理する

アプリケーションのリモートインストールを完了するには（特に Windows では）、通常はデバイスの再起動が必要です。

Kaspersky Security Center のリモートインストールタスクを使用する場合、新規タスクウィザード、または作成したタスクのプロパティウィンドウ（［**OS の再起動**］セクション）で、Windows デバイスに再起動が必要な際に実行する以下の操作を選択できます：

- **デバイスを再起動しない**：自動再起動は実行されません。インストールを完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、サーバーや、継続的な操作が不可欠なその他のデバイスのインストールタスクに適切です。

- **デバイスを再起動する**：インストールの完了に再起動が必要な場合は常に、デバイスは自動的に再起動されます。このオプションは、定期的に操作が一時停止（シャットダウンまたは再起動）されるデバイスのインストールタスクに有用です。

- **ユーザーに処理を確認する**：手動での再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。［**ユーザーに処理を確認する**］は、ユーザーにとって最も好都合な時間に再起動できることが要求されるワークステーションに最適です。

セキュリティ製品のインストールパッケージで定義データベースをアップデートする

セキュリティ製品の配布パッケージと一緒に出荷された定義データベース（自動パッチのモジュールを含む）は、保護の導入を開始する前にアップデートすることが可能です。導入を開始する前に、（選択したインストールパッケージのコンテキストメニューで関連コマンドを使用するなどして）アプリケーションのインストールパッケージ内のデータベースをアップデートすることは有用です。そうすることで、対象デバイスへの保護製品の導入を完了するために必要な再起動の回数が低減されます。

管理対象デバイスで関連する実行ファイルを実行するために、Kaspersky Security Center でアプリケーションのリモートインストール用ツールを使用する

新規パッケージウィザードを使用して、任意の実行ファイルを選択し、実行ファイルのコマンドラインの設定を定義できます。これを行うには、選択したファイルそのもの、またはこのファイルが保存されているフォルダー全体のいずれかを、インストールパッケージに追加します。次に、リモートインストールタスクを作成し、作成されたインストールパッケージを選択する必要があります。

タスクの実行中に、指定した実行ファイルが、定義したコマンドプロンプトの設定を使用して、対象デバイスで実行されます。

Microsoft Windows インストーラー（MSI）形式のインストーラーを使用する場合、Kaspersky Security Center では、標準ツールを使用してインストールの結果が分析されます。

脆弱性とパッチ管理が使用可能なライセンスがある場合、Kaspersky Security Center は、（社内の環境でサポートされるアプリケーションのインストールパッケージを作成する際に）インストールのルールと、アップデート可能な定義データベース内のインストール結果の分析も使用します。

そうでない場合は、実行ファイルの既定のタスクは、プロセスとすべての子プロセスの実行が完了するのを待ちます。実行中のプロセスがすべて完了すると、初期プロセスのリターンコードに依存せず、タスクは正常に終了します。このタスクのこのような動作を変更するには、タスクを作成する前に、新たに作成されたインストールパッケージのフォルダー内で Kaspersky Security Center が生成した kpd ファイルを手動で修正する必要があります。

実行中のプロセスの完了を待たないタスクでは、次のように、[SetupProcessResult] セクションで Wait 設定の値を 0 に設定します：

例：
[SetupProcessResult]
Wait=0

すべての子プロセスの完了を待たずに、Windows で実行中プロセスの完了のみを待つタスクでは、たとえば次のように、[SetupProcessResult] セクションで WaitJob 設定の値を 0 に設定します：

例：
[SetupProcessResult]
WaitJob=0

実行中のプロセスのリターンコードに応じて正常に終了する、またはエラーを返すタスクでは、たとえば次のように、[SetupProcessResult_SuccessCodes] セクションで正常なリターンコードを一覧表示します：

例：
[SetupProcessResult_SuccessCodes]
0=
3010=

この場合、一覧表示されたコード以外のコードではすべて、エラーが返されます。

タスク結果でタスクの正常終了やエラーのコメント文字を表示するには、たとえば次のように、[SetupProcessResult_SuccessCodes] および [SetupProcessResult_ErrorCodes] セクションで、プロセスのリターンコードに対応する簡単なエラーの説明を入力します：

例：
[SetupProcessResult_SuccessCodes]
0= インストールが正常に完了しました
3010= インストールを完了するには再起動が必要です
[SetupProcessResult_ErrorCodes]
1602= ユーザーによってインストールがキャンセルされました
1603= インストール中に致命的なエラーが発生しました

Kaspersky Security Center ツールを使用してデバイスの再起動を管理するには（操作の完了に再起動が必要な場合）、次のように、[SetupProcessResult_NeedReboot] セクションで、再起動が必要であることを示すプロセスのリターンコードを一覧表示します：

例：
[SetupProcessResult_NeedReboot]
3010=

製品導入を監視する

Kaspersky Security Center の導入を監視し、セキュリティ製品とネットワークエージェントが管理対象デバイスにインストールされていることを確認するには、［**製品の導入**］セクションのステータス信号を確認する必要があります。このステータス信号は、管理コンソールのメインウィンドウに表示される管理サーバーフォルダーの作業領域に配置されます。ステータス信号は、現在の製品導入ステータスを反映しています。ネットワークエージェントとセキュリティ製品がインストールされているデバイスの数が、ステータス信号の隣に表示されます。インストールタスクが実行中の場合は、ここで進捗状況を監視できます。インストールエラーが発生した場合は、ここにエラーの数が表示されます。リンクをクリックすると、エラーの詳細が表示されます。

［**管理対象デバイス**］フォルダーの作業領域の［**グループ**］タブにある導入状況の概要を使用することもできます。この表は、導入プロセスを反映しており、ネットワークエージェントがインストールされていないデバイス、ネットワークエージェントがインストールされているデバイス、またはネットワークエージェントとセキュリティ製品がインストールされているデバイスの数を表示します。

導入（または特定のインストールタスクの操作）の進捗状況の詳細を表示するには、該当のリモートインストールタスクの履歴ウィンドウを開きます（タスクを右クリックして、コンテキストメニューで［**履歴**］を選択）。ウィンドウには、2 つの一覧が表示されます。上の一覧には、デバイス上のタスクのステータスが表示され、下の一覧には、現在上の一覧で選択されているデバイスでのタスクイベントが表示されます。

導入エラーに関する情報は、管理サーバーの Kaspersky イベントログに追加されます。エラーに関する情報は、［管理サーバー］フォルダーの［**イベント**］タブの関連イベントの抽出で参照することも可能です。

インストーラーを設定する

このセクションでは、Kaspersky Security Center インストーラーのファイルとインストールの設定、および管理サーバーとネットワークエージェントをサイレントモードでインストールする方法に関する推奨事項を説明します。

一般情報

Kaspersky Security Center 15.1 のコンポーネント（管理サーバー、ネットワークエージェント、および管理コンソール）のインストーラーは、Windows インストーラー技術に基づき構築されています。MSI パッケージは、インストーラーの核です。このパッケージ形式により、Windows インストーラーの提供するすべての利点、すなわち拡張性、パッチ適用システムの可用性、変換システム、サードパーティ製ソリューションを使用したインストールの一元管理、およびオペレーティングシステムによる透過的な登録を享受できます。

サイレントモードでのインストール（応答ファイルを使用した場合）

管理サーバーとネットワークエージェントのインストーラーには、応答ファイル（ss_install.xml）を利用した機能があります。応答ファイルは、ユーザーが介入しないサイレントモードでのインストールのパラメータを統合したファイルです。ss_install.xml ファイルは、MSI パッケージと同じフォルダーにあり、サイレントモードでのインストール中に自動的に使用されます。サイレントインストールモードは、コマンドラインのキー「/s」を使用して有効にできます。

実行例の概要は次の通りです：

```
setup.exe /s
```

> サイレントモードでインストーラーを起動する前に、使用許諾契約書 (EULA) をお読みください。Kaspersky Security Center Linux 配布キットに EULA のテキストを含む TXT ファイルが含まれていない場合は、カスペルスキーの Web サイト からファイルをダウンロードできます。

ss_install.xml ファイルは、Kaspersky Security Center インストーラーの内部形式のパラメータのインスタンスです。配布パッケージには、既定のパラメータを含む ss_install.xml ファイルが含まれます。

> ファイル ss_install.xml は手動で変更しないでください。このファイルは、管理コンソールでインストールパッケージのパラメータを編集する際に、Kaspersky Security Center のツールを使用して変更できます。

管理サーバーのインストール用の応答ファイルを変更するには：

1. Kaspersky Security Center 配布パッケージを開きます。完全なパッケージの EXE ファイルを使用する場合は解凍します。

2. フォルダー Server からコマンドラインを開き、次のコマンドを実行します：

```
setup.exe /r ss_install.xml
```

Kaspersky Security Center のインストーラーが起動します。

3. ウィザードの手順に従って、Kaspersky Security Center のインストールを設定します。

ウィザードを終了すると、指定した新しい設定に従って応答ファイルが自動的に変更されます。

サイレントモードでのネットワークエージェントのインストール（応答ファイルを使用しない場合）

単一の msi パッケージを使用してネットワークエージェントをインストールすることで、標準的な方法で MSI プロパティの値を指定できます。このシナリオでは、グループポリシーを使用してネットワークエージェントをインストールできます。

インストールパッケージ Kaspersky Network Agent.msi の名前を変更しないでください。このパッケージの名前を変更すると、ネットワークエージェントの将来のアップデート時にインストールエラーが発生する可能性があります。

MSI プロパティを使用して定義されたパラメータと、応答ファイルで定義されたパラメータが競合するのを回避するには、プロパティ `DONT_USE_ANSWER_FILE=1` に設定して、応答ファイルを無効にすることができます。MSI ファイルは、Kaspersky Security Center 配布パッケージのフォルダー Packages\NetAgent\exec にあります。msi パッケージを使用したネットワークエージェントのインストーラーの実行例は次の通りです。

サイレントモードでのネットワークエージェントのインストールには、使用許諾契約書の条項への同意が必要です。 `EULA=1` パラメータは、使用許諾契約書の内容をすべて確認し、理解した上で条項に同意する場合にのみ使用してください。

```
例：
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

応答ファイル（拡張子が mst のファイル）を事前に準備することで、msi パッケージのインストールパラメータを定義することもできます。このコマンドは次のようになります：

```
例：
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

単一のコマンドで複数の応答ファイルを指定できます。

setup.exe を使用した部分インストールの設定

setup.exe を使用してアプリケーションのインストールを実行する場合、MSI の任意のプロパティ値を msi パッケージに追加できます。

このコマンドは次のようになります：

```
例：
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

管理サーバーのインストールパラメータ

以下の表では、管理サーバーをインストールする際に設定できる MSI プロパティについて説明しています。EULA と PRIVACYPOLICY を除き、すべてのパラメータの指定は省略可能です。

サイレントモードでの管理サーバーのインストールのパラメータ

MSI プロパティ	説明	設定可能な値
EULA	使用許諾契約書の条項の同意（必須）	• 1 – 使用許諾契約書の内容をすべて確認し、理解した上で条項に同意します。 • その他の値または値なし – 使用許諾契約書に同意しません（インストールは実行されません）。
PRIVACYPOLICY	プライバシーポリシーの条項の同意（必須）	• 1 – プライバシーポリシーに従ってデータが処理されて送信されること（第三国への送信を含む）を理解しました。プライバシーポリシーの内容をすべて確認し、理解した上で同意します。 • その他の値または値なし – プライバシーポリシーの条項に同意しません（インストールは実行されません）。
INSTALLATIONMODETYPE	管理サーバーのインストールの種別	• 標準 • カスタム
INSTALLDIR	アプリケーションのインストールフォルダー	文字列値
ADDLOCAL	インストールする機能一覧（カンマで区切ります）	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86 管理サーバーの適切なインストールに最小限必要なコンポーネントは次の通りです： `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	ネットワークの規模	• NRT_1_100：デバイスが 1 ～ 100 台 • NRT_100_1000：デバイスが 101 ～ 1000 台 • NRT_GREATER_1000：デバイスが 1000 台以上
SRV_ACCOUNT_TYPE	管理サーバーサービスを操作するユーザーを指定する方法	• SrvAccountDefault – ユーザーアカウントを自動的に作成する • SrvAccountUser – ユーザーアカウントを手動で定義する
SERVERACCOUNTNAME	サービスのユーザー名	文字列値
SERVERACCOUNTPWD	サービスのユーザーパスワード	文字列値
DBTYPE	データベースの種別	• MySQL – MySQL データベースまたは MariaDB データベースを使用する • MSSQL – Microsoft SQL Server (SQL Express) データベースを使用する
MYSQLSERVERNAME	MySQL サーバーまたは MariDB サーバーの完全名	文字列値
MYSQLSERVERPORT	MySQL サーバーまたは MariaDB サーバーに接続するためのポートの番号	数値

MYSQLDBNAME	MySQL サーバーデータベースまたは MariaDB サーバーデータベースの名前	文字列値
MYSQLACCOUNTNAME	MySQL サーバーデータベースまたは MariaDB サーバーデータベースに接続するためのユーザー名	文字列値
MYSQLACCOUNTPWD	MySQL サーバーデータベースまたは MariaDB サーバーデータベースに接続するためのユーザーのパスワード	文字列値
MSSQLCONNECTIONTYPE	MSSQL データベースの使用種別	• InstallMSSEE – パッケージからインストールする • ChooseExisting – インストール済みサーバーを使用する
MSSQLSERVERNAME	SQL Server インスタンスの名前	文字列値
MSSQLDBNAME	SQL Server データベースの名前	文字列値
MSSQLAUTHTYPE	SQL Server に接続するための認証方法	• Windows • SQLServer
MSSQLACCOUNTNAME	SQLServer モードで SQL Server に接続するためのユーザー名	文字列値
MSSQLACCOUNTPWD	SQLServer モードで SQL Server に接続するためのユーザーのパスワード	文字列値
CREATE_SHARE_TYPE	共有フォルダーを指定する方法	• Create – 新しい共有フォルダーを作成する。この場合、次のプロパティを定義する必要があります： • SHARELOCALPATH – ローカルフォルダーへのパス • SHAREFOLDERNAME – フォルダーのネットワーク名 • Null – EXISTSHAREFOLDERNAME プロパティを指定する必要があります
EXISTSHAREFOLDERNAME	既存の共有フォルダーの完全パス	文字列値
SERVERPORT	管理サーバーに接続するためのポート番号	数値
SERVERSSLPORT	管理サーバーとの SSL 接続を確立するためのポートの番号	数値
SERVERADDRESS	管理サーバーアドレス	文字列値
SERVERCERT2048BITS	管理サーバー証明書の鍵のサイズ（ビット）	• 1 – 管理サーバー証明書の鍵のサイズは 2048 ビット • 0 – 管理サーバー証明書の鍵のサイズは 1024 ビット • 値が指定されていない場合、管理サーバー証明書の鍵のサイズは 1024 ビットです
MOBILESERVERADDRESS	モバイルデバイスの接続用管理サーバーのアドレス（MobileSupport コンポーネントが選択されていない場合は無視されます）	文字列値

ネットワークエージェントのインストールパラメータ

以下の表では、ネットワークエージェントをインストールする際に設定できる MSI プロパティについて説明しています。EULA と SERVERADDRESS を除き、すべてのパラメータの指定は省略可能です。

サイレントモードでのネットワークエージェントのインストールのパラメータ

MSI プロパティ	説明	設定可能な値
EULA	使用許諾契約書の条項の同意	• 1 – 使用許諾契約書の内容をすべて確認し、理解した上で条項に同意します。 • 0 – 使用許諾契約書の条件に同意しません（インストールは実行されません）。 • 値なし – 使用許諾契約書の条件に同意しません（インストールは実行されません）。
DONT_USE_ANSWER_FILE	応答ファイルからインストールの設定を読み込む	• 1 – 使用しない。 • その他の値または値なし – 読み取り。
INSTALLDIR	ネットワークエージェントのインストールフォルダーへのパス	文字列値
SERVERADDRESS	管理サーバーのアドレス（必須）	文字列値
SERVERPORT	管理サーバーに接続するためのポートの番号	数値
SERVERSSLPORT	SSL プロトコルを使用した管理サーバーへの暗号化接続用ポートの番号	数値
USESSL	SSL 接続を使用するかどうか	• 1 – 使用する • その他の値または値なし – 使用しない
OPENUDPPORT	UDP ポートを開くかどうか	• 1 – 開く • その他の値または値なし – 開かない
UDPPORT	UDP ポート番号	数値
USEPROXY	プロキシサーバーを使用するかどうか。 互換性のため、ネットワークエージェントのインストールパッケージ設定でプロキシ接続設定を指定することは推奨されません。	• 1 – 使用する • その他の値または値なし – 使用しない
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	プロキシサーバーに接続するためのプロキシアドレスとポートの番号	文字列値
PROXYLOGIN	プロキシサーバーに接続するためのアカウント	文字列値
PROXYPASSWORD	プロキシサーバーに接続するためのアカウントのパスワード（インストールパッケージの設定では、特別な権限を持つアカウントを指定しないでください。）	文字列値
GATEWAYMODE	接続ゲートウェイの使用モード	• 0 – 接続ゲートウェイを使用しない • 1 – このネットワークエージェントを接続ゲートウェイとして使用する • 2 – 接続ゲートウェイを使用して管理サーバーに接続する
GATEWAYADDRESS	接続ゲートウェイアドレス	文字列値
CERTSELECTION	証明書を取得する方法	• GetOnFirstConnection – 管理サーバーから証明書を取得する • GetExistent – 既存の証明書を選択する。このオプションを選択する場合、CERTFILE プロパティを指定する必要があります

CERTFILE	証明書ファイルのパス	文字列値
VMVDI	仮想デスクトップインフラストラクチャ（VDI）向け動的モードを有効にする	• 1 – 有効にする • 0 – 有効にしない • 値なし – 有効にしない
VMOPTIMIZE	ネットワークエージェントの設定をハイパーバイザー向けに最適化するかどうか	• 1 – 有効にする • 0 – 有効にしない • 値なし – 有効にしない
LAUNCHPROGRAM	インストール後にネットワークエージェントサービスを開始するかどうか。VMVDI=1 の場合、パラメータは無視されます。	• 1 – 開始する • その他の値または値なし – 開始しない
NAGENTTAGS	ネットワークエージェントのタグ（応答ファイルで付与されているタグよりも優先されます）	文字列値

仮想インフラストラクチャ

Kaspersky Security Center では仮想マシンの使用をサポートします。ネットワークエージェントとセキュリティ製品を各仮想マシンにインストールできます。また、ハイパーバイザーレベルで仮想マシンを保護できます。前者の場合、標準セキュリティ製品または Kaspersky Security for Virtualization Light Agent のいずれかを使用して、仮想マシンを保護できます。後者の場合、Kaspersky Security for Virtualization Agentless を使用できます。

Kaspersky Security Center は、以前の状態への仮想マシンのロールバックをサポートします。

仮想マシンの負荷を軽減するヒント

Kaspersky Security Center の一部の機能は、仮想マシンに対してはそれほど有効性がないと考えられます。ネットワークエージェントを仮想マシンにインストールする場合は、それらの機能の無効化を検討することが推奨されます。

ネットワークエージェントを仮想マシンまたは仮想マシンの生成を目的とするテンプレートにインストールする場合、以下の操作を実行してください：

- リモートインストールを実行している場合、ネットワークエージェントのインストールパッケージのプロパティウィンドウの［**詳細**］セクションで、［**VDI 向けに設定を最適化する**］をオンにします。
- ウィザードを使用して対話型インストールを実行している場合、ウィザードウィンドウで［**ネットワークエージェントの設定を仮想インフラストラクチャ用に最適化します**］をオンにします。

これらのオプションを選択すると、ネットワークエージェントの設定が変更されるため、以下の機能は（ポリシーを適用する前に）既定で引き続き無効化されます：

- インストールされたソフトウェアに関する情報の取得
- ハードウェアに関する情報の取得
- 検知された脆弱性に関する情報の取得

- 必要なアップデートに関する情報の取得

これらの機能は同一のソフトウェアと仮想ハードウェアを使用しているため、通常は仮想マシンでは必須ではありません。

機能の無効化は取り消すことができます。無効にした機能が必要になった場合、ネットワークエージェントのポリシーを使用して、またはネットワークエージェントのローカル設定を使用して有効にすることができます。ネットワークエージェントのローカル設定は、管理コンソールで関連デバイスのコンテキストメニューからアクセスできます。

動的仮想マシンのサポート

Kaspersky Security Center では動的仮想マシンをサポートします。仮想インフラストラクチャが組織ネットワークに導入されている場合、動的（一時）仮想マシンを特定の条件下で使用できます。動的仮想マシンは、管理者が準備したテンプレートに基づき、一意の名前で作成されます。ユーザーがしばらくの間仮想マシンで作業して、仮想マシンの電源をオフにすると、その仮想マシンは仮想インフラストラクチャから削除されます。Kaspersky Security Center が組織ネットワークに導入されている場合、動的（一時）仮想マシンを特定の条件下で使用できます。仮想マシンの電源をオフにした後は、対応するエントリも管理サーバーのデータベースから削除する必要があります。

仮想マシンのエントリの自動削除機能を活用するには、動的仮想マシンのテンプレートにネットワークエージェントをインストールする際に、次の場所で［**VDI 向け動的モードを有効にする**］をオンにします：

- リモートインストールの場合 – ネットワークエージェントのインストールパッケージのプロパティウィンドウで（［**詳細**］セクション）
- 対話型インストールの場合 – ネットワークエージェントのインストールウィザードで

> ネットワークエージェントを物理デバイスにインストールする場合は、［**VDI 向け動的モードを有効にする**］をオンにしないでください。

動的仮想マシンのイベントを、それらの仮想マシンを削除した後もしばらくの間管理サーバーに保存したい場合、管理サーバーのプロパティウィンドウの［**イベントリポジトリ**］セクションで、［**デバイスの削除後にイベントを保管する**］をオンにし、イベントの最大保管時間（日数）を指定します。

仮想マシンのコピーのサポート

ネットワークエージェントがインストールされた仮想マシンをコピーする、またはネットワークエージェントがインストールされたテンプレートを使用して仮想マシンを作成する作業は、ハードディスクイメージを取得し、コピーしてネットワークエージェントを導入する場合と同一です。通常、仮想マシンをコピーする場合は、ディスクイメージをコピーしてネットワークエージェントを導入する場合と同じアクションを実行する必要があります。

ただし、以下に説明する 2 つの方法では、ネットワークエージェントでコピーが自動的に検出されます。そのため、「デバイスのハードディスクの取得とコピーによる導入」で説明する高度な操作を実行する必要はありません：

- ネットワークエージェントのインストール時に［**VDI 向け動的モードを有効にする**］をオンにした場合：オペレーティングシステムを再起動するたびに、この仮想マシンは、コピーされたかどうかに依存せず、新しいデバイスとして認識されます。

- VMware™、HyperV®、Xen® のいずれかのハイパーバイザーが使用されている場合：ネットワークエージェントでは、変更された仮想ハードウェアの ID によって、仮想マシンのコピーが検出されます。

仮想ハードウェアにおける変更の分析機能は、完全に信頼できるわけではありません。この方法を広く採用する前に、組織が現在使用しているハイパーバイザーのバージョンを用いて、小規模な仮想マシンのプールでテストする必要があります。

ネットワークエージェントをインストールしたデバイスでのファイルシステムロールバックのサポート

Kaspersky Security Center は配信アプリケーションです。ネットワークエージェントがインストールされたデバイスでファイルシステムを以前の状態にロールバックすると、データの非同期を引き起こし、Kaspersky Security Center が正しく機能しなくなります。

ファイルシステム（またはその一部）をロールバックできるのは、次の場合です：

- ハードディスクのイメージをコピーする場合
- 仮想インフラストラクチャを使用して仮想マシンの状態を復元する場合
- バックアップコピーまたは復元ポイントからデータを復元する場合

ネットワークエージェントがインストールされたデバイスのサードパーティ製ソフトウェアが、%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ フォルダーに影響を及ぼすシナリオのみが、Kaspersky Security Center にとって重要なシナリオです。そのため、可能な場合は復元手順からこのフォルダーを常に除外する必要があります。

一部の組織では、職場のルールでデバイスのファイルシステムのロールバックが規定されているため、バージョン 10 Maintenance Release 1 より、Kaspersky Security Center では、ネットワークエージェントがインストールされたデバイスでのファイルシステムのロールバックがサポートされるようになりました（管理サーバーとネットワークエージェントはバージョン 10 Maintenance Release 1 以降でなければなりません）。これらのデバイスは検出されると、完全にデータがクレンジングおよび同期化された管理サーバーに自動的に再接続されます。

Kaspersky Security Center 15.1 では、ファイルシステムのロールバック検出機能のサポートは既定で有効になっています。

ネットワークエージェントがインストールされたデバイスにおける %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ フォルダーのロールバックは、データの完全な再同期化に大量のリソースを必要とするため、可能な限り避けてください。

管理サーバーがインストールされたデバイスでは、システムステータスのロールバックは禁じられています。管理サーバーが使用するデータベースのロールバックも同様に禁じられています。

管理サーバーの状態は、標準の klbackup ユーティリティを使用する場合にのみバックアップコピーから復元できます。

アプリケーションのローカルインストール

このセクションでは、ローカルデバイスにのみインストール可能なアプリケーションのインストール手順について説明します。

特定のクライアントデバイスでアプリケーションのローカルインストールを実行するには、このデバイスの管理者権限が必要です。

特定のクライアントデバイスにアプリケーションをローカルインストールするには：

1. クライアントデバイスにネットワークエージェントをインストールし、クライアントデバイスと管理サーバー間の接続を設定します。
2. アプリケーションのガイドに従って、必要なアプリケーションをデバイスにインストールします。
3. インストールしたすべてのアプリケーションの管理プラグインを管理コンピューターにインストールします。

Kaspersky Security Center は、スタンドアロンインストールパッケージを使用したローカルインストールも実行可能です。一部のカスペルスキー製品については、Kaspersky Security Center によるインストールがサポートされません。

ネットワークエージェントのローカルインストール

ネットワークエージェントをデバイスにローカルインストールするには：

1. インターネットからダウンロードした配布パッケージにある setup.exe ファイルをデバイスで実行します。詳細については、以下のトピックを参照してください：Kaspersky Security Center 配布キットからのネットワークエージェントのインストールパッケージの入手。

   ウィンドウが開き、インストールするカスペルスキー製品の選択を要求されます。

2. 製品の選択ウィンドウで、［**Kaspersky Security Center ネットワークエージェントのみのインストール**］をクリックしてネットワークエージェントのセットアップウィザードを起動します。ウィザードの指示に従います。

   a. **管理サーバー**

ポート

管理サーバーがネットワークエージェントからの接続を受信するために使用する非 SSL ポートを指定します。

既定では、このオプションは 14000 に設定されています。

SSL ポート

管理サーバーがネットワークエージェントからの接続を受信するために使用する SSL ポートを指定します。

既定では、このオプションは 13000 に設定されています。

管理サーバーへの接続に SSL を使用する

このオプションをオンにすると、SSL を使用してセキュアなポート経由で管理サーバーへの接続が確立されます。

既定では、このオプションはオンです。

ネットワークエージェントに UDP ポートを開くことを許可する

このオプションをオンにすると、インストーラーは、管理サーバーがクライアントデバイスを管理し、クライアントデバイスに関する情報を受信するために使用するポートを自動的に開きます。

既定では、このオプションはオンです。

UDP ポート

管理サーバーがクライアントデバイスを管理し、そのデバイスに関する情報を受信するために使用するポートを構成できます。

既定では、このオプションは 15000 に設定されています。

b. **プロキシサーバーの設定**

プロキシサーバーを使用する

このオプションをオンにすると、プロキシサーバー認証の資格情報を指定できます。

プロキシサーバー認証に必要な最小限の権限が付与されているアカウントの資格情報を指定することを推奨します。

既定では、このオプションはオフです。

アドレス

ポート

アカウント

プロキシサーバーへの接続の確立に使用されるアカウントのユーザー名。

プロキシサーバー認証に必要な最小限の権限が付与されているアカウントの資格情報を指定することを推奨します。

パスワード

プロキシサーバーへの接続の確立に使用されるアカウントのパスワード。

プロキシサーバー認証に必要な最小限の権限が付与されているアカウントの資格情報を指定することを推奨します。

c. **接続ゲートウェイ**

接続ゲートウェイを使用しない

DMZ 内でネットワークエージェントを接続ゲートウェイとして使用する

このオプションをオンにすると、ネットワークエージェントが非武装地帯（DMZ）の接続ゲートウェイとして使用され、管理サーバーへの接続、通信、およびデータ転送中のネットワークエージェント上のデータの安全が確保されます。

接続ゲートウェイを使用して管理サーバーに接続する

このオプションをオンにし、接続ゲートウェイとして機能するデバイスを指定します。

d. **管理サーバー証明書**

e. **エージェントタグ**

f. **詳細設定**

コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする

このオプションをオンのままにすることを推奨します。このオプションをオフにして、Kaspersky Security Center コンポーネントの自動アップデートとパッチ適用を無効にすることができます。管理者は、ポリシーを使用することで、後で自動アップデートとパッチを再度有効にすることができます。

既定では、このオプションはオフです。

ネットワークエージェントサービスの保護を有効にする

このオプションをオンにすると、管理対象デバイスにネットワークエージェントのインストールされた後、必要な権限がない場合はコンポーネントの削除や再設定が行えなくなります。また、ネットワークエージェントサービスを停止できなくなります。このオプションはドメインコントローラーに影響しません。

ローカル管理者権限で操作されているワークステーション上のネットワークエージェントを保護するには、このオプションをオンにします。

既定では、このオプションはオフです。

VDI 向け動的モードを有効にする

このオプションをオンにすると、仮想マシンにインストールされたネットワークエージェントで仮想デスクトップインフラストラクチャ（VDI）向け動的モードが有効になります。

既定では、このオプションはオフです。

Kaspersky Security Center ネットワークエージェントの設定を VDI 用に最適化します。アプリケーションとハードウェアの脆弱性スキャンとインベントリを無効にします。ネットワークエージェントポリシーを通じて現在の設定を編集できます。

このオプションをオンにすると、ネットワークエージェントの設定で次の機能が無効にされます：

- インストールされたソフトウェアに関する情報の取得
- ハードウェアに関する情報の取得
- 検知された脆弱性に関する情報の取得
- 必要なアップデートに関する情報の取得

既定では、このオプションはオフです。

g. **アプリケーションの開始**

セットアップウィザードが終了すると、ネットワークエージェントがデバイスにインストールされます。

これで Kaspersky Security Center ネットワークエージェントサービスのプロパティを表示したり、Microsoft Windows の標準ツール（コンピューターの管理 / サービス）でネットワークエージェントのアクティビティの開始、終了、監視をしたりすることができるようになります。

サイレントモードでのネットワークエージェントのインストール

ネットワークエージェントは、サイレントモードでインストールできます。インストール中にパラメータを対話形式で入力する必要はありません。サイレントインストールでは、ネットワークエージェント用の Windows インストーラーパッケージ（MSI）が使用されます。MSI ファイルは、Kaspersky Security Center 配布パッケージのフォルダー Packages\NetAgent\exec にあります。

インストールパッケージ Kaspersky Network Agent.msi の名前を変更しないでください。このパッケージの名前を変更すると、ネットワークエージェントの将来のアップデート時にインストールエラーが発生する可能性があります。

MSI パッケージからのネットワークエージェントのインストールはサイレントモードでのみ可能であり、MSI パッケージからの対話型インストールはサポートされていません。

ネットワークエージェントをサイレントモードでローカルデバイスにインストールするには：

1. 使用許諾契約書をお読みください。以下のコマンドは、使用許諾契約書の内容を理解して条項に同意する場合にのみ使用してください。

2. 次のコマンドを実行します：

   `msiexec /i "Kaspersky Network Agent.msi" /qn <セットアップパラメータ>`

   ここで、<セットアップパラメータ>には、パラメータと対応する値のペアをスペースで区切って並べます（例：`PROP1=PROP1VAL PROP2=PROP2VAL`）。

   パラメータ部分には、「`EULA=1`」というパラメータを含める必要があります。そうしない場合、ネットワークエージェントがインストールされません。

Kaspersky Security Center の標準接続設定、およびリモートデバイスのネットワークエージェントを使用している場合は、コマンドを実行します：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` はログ記録のためのキーです。ログはネットワークエージェントのインストール中に作成され、C:\windows\temp\nag_inst.log に保存されます。

nag_inst.log に加えて、アプリケーションはインストールログを含む $klssinstlib.log ファイルを作成します。このファイルは、%windir%\ temp フォルダーまたは %temp% フォルダーに保存されます。トラブルシューティングの目的で、お客様またはカスペルスキーテクニカルサポートのスペシャリストが、nag_inst.log と $klssinstlib.log の両方のログファイルを必要とする場合があります。

管理サーバーに接続するポートを追加で指定する必要がある場合、次のコマンドを実行します：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

パラメータ `SERVERPORT` は管理サーバーに接続するためのポート番号に対応しています。

ネットワークエージェントをサイレントモードでインストールする時に使用可能なパラメータの名前と値を［ネットワークエージェントのインストールパラメータ］セクションに示します。

Linux 用ネットワークエージェントのサイレントモードでのインストール（応答ファイルを使用）

Linux デバイスにネットワークエージェントをインストールするには、インストールパラメータのカスタムセット（変数と各変数の値）を含むテキストファイルである応答ファイルを使用します。この応答ファイルを使用すると、インストールをサイレントモードで、つまりユーザーの参加なしで実行できます。

Linux 用ネットワークエージェントのインストールをサイレントモードで実行するには：

1. リモートインストールを行う関連する Linux デバイスを準備します。ネットワークエージェントの deb パッケージまたは rpm パッケージを使用し、適切なパッケージ管理システムを用いて、リモートインストールパッケージをダウンロードし作成します。

2. SUSE Linux Enterprise Server 15 オペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントの設定前に、insserv-compat パッケージをインストールします。

   RED OS 7.3.4 以降のオペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントが正しく機能するために libxcrypt-compat パッケージをインストールしてください。

3. 使用許諾契約書をお読みください。次の手順は、使用許諾契約書の内容を理解して条項に同意する場合にのみ使用してください。

4. たとえば、次のように、応答ファイルの完全名（パスを含む）を入力して、KLAUTOANSWERS 環境変数の値を設定します。

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

5. 環境変数で指定したディレクトリに応答ファイル（TXT 形式）を作成します。応答ファイルに、VARIABLE_NAME=variable_value 形式の変数のリストを追加します。各変数は個別の行に配置します。

   応答ファイルを正しく使用するには、3 つの必須変数の最小セットをファイルに含める必要があります：

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   オプションの変数を追加して、リモートインストールに関するより具体的なパラメータを使用することもできます。次の表に、応答ファイルに含めることができるすべての変数を一覧で示します：

   サイレントモードでの Linux 用ネットワークエージェントインストールのパラメータとして使用される応答ファイルの変数

サイレントモードでの Linux 用ネットワークエージェントインストールのパラメータとして使用される応答ファイルの変数

変数名	必須	説明	指定可能な値
KLNAGENT_SERVER	使用する	完全修飾ドメイン名（FQDN）または IP アドレスとして提示される管理サーバー名が含まれます。	DNS 名または IP アドレス。
KLNAGENT_AUTOINSTALL	使用する	サイレントインストールモードを有効にするかどうかを定義します。	1 - サイレントモードが有効です。ユーザーが、インストール中に操作を要求されることはありません。 その他 - サイレントモードは無効です。ユーザーは、インストール中に操作を要求される場合があります。
EULA_ACCEPTED	使用する	ユーザーがネットワークエージェントの使用許諾契約書（EULA）に同意するかどうかを定義します。定義されていない場合は、EULA に同意しないものとして解釈できます。	1 - この使用許諾契約書の内容をすべて確認し、理解した上で条項に同意する その他の値または値なし - 使用許諾契約書の条項に同意しない（インストールは実行されません）
KLNAGENT_PROXY_USE	使用しない	管理サーバーとの接続でプロキシ設定を使用するかどうかを定義します。既定値は 0 です。	1 - プロキシ設定が使用されます。 その他 - プロキシ設定は使用されません。
KLNAGENT_PROXY_ADDR	使用しない	管理サーバーとの接続に使用されるプロキシサーバーのアドレスを定義します。	DNS 名または IP アドレス。
KLNAGENT_PROXY_LOGIN	使用しない	プロキシサーバーへのログインに使用するユーザー名を定義します。	既存のユーザー名。
KLNAGENT_PROXY_PASSWORD	使用しない	プロキシサーバーへのログインに使用するパスワードを定義します。	オペレーティングシステムのパスワード形式で許可されている英数字のセット。
KLNAGENT_VM_VDI	使用しない	動的仮想マシンを作成するために、ネットワークエージェントをイメージにインストールするかどうかを定義します。	1 - ネットワークエージェントがイメージにインストールされ、その後、動的仮想マシンの作成に使用されます。 その他 - インストール中にイメージは使用されません。
KLNAGENT_VM_OPTIMIZE	使用しない	ネットワークエージェントの設定をハイパーバイザー向けに最適化するかどうかを定義します。	1 - ネットワークエージェントの既定のローカル設定が変更され、ハイパーバイザーでの使用が最適化されます。
KLNAGENT_TAGS	使用しない	ネットワークエージェントのインスタンスに割り当てられたタグを一覧表示します。	セミコロンで区切られた 1 つまたは複数のタグ名。
KLNAGENT_UDP_PORT	使用しない	ネットワークエージェントが使用する UDP ポートを定義します。既定値は 15000 です。	既存のポート番号。

KLNAGENT_PORT	使用しない	ネットワークエージェントが使用する非 TLS ポートを定義します。既定値は 14000 です。	既存のポート番号。
KLNAGENT_SSLPORT	使用しない	ネットワークエージェントが使用する TLS ポートを定義します。既定値は 13000 です。	既存のポート番号。
KLNAGENT_USESSL	使用しない	接続にトランスポート層セキュリティ（TLS）を使用するかどうかを定義します。	1（既定） - TLSが使用されます。 その他 - TLS は使用されません。
KLNAGENT_GW_MODE	使用しない	接続ゲートウェイを使用するかどうかを定義します。	1（既定） - 現在の設定は変更されません（最初の呼び出しで、接続ゲートウェイは指定されません）。 2 - 接続ゲートウェイは使用されません。 3 - 接続ゲートウェイが使用されます。 4 - ネットワークエージェントのインスタンスが、非武装地帯（DMZ）で接続ゲートウェイとして使用されます。
KLNAGENT_GW_ADDRESS	使用しない	接続ゲートウェイのアドレスを定義します。この値は、KLNAGENT_GW_MODE=3 の場合にのみ適用されます。	DNS 名または IP アドレス：
KLNAGENT_DEVICEOWNER_REGISTRATION_START	使用しない	ネットワークエージェントのインストール後に、デバイスの所有者としてのユーザー登録ユーティリティを実行できるようにします。オフにすると、ユーザーはデバイスの所有者として登録できなくなります。	1—デバイスの所有者としてのユーザー登録ユーティリティは、ネットワークエージェントのインストール後に実行されます。 その他—オフになっています。

6. ネットワークエージェントをインストールします：

- RPM パッケージから 32 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# rpm -i klnagent-<` ビルド番号 `>.i386.rpm`

- RPM パッケージから 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# rpm -i klnagent64-<` ビルド番号 `>.x86_64.rpm`

- RPM パッケージから ARM アーキテクチャの 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# rpm -i klnagent64-<` ビルド番号 `>.aarch64.rpm`

- DEB パッケージから 32 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# apt-get install ./klnagent_<` ビルド番号 `>_i386.deb`

- DEB パッケージから 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# apt-get install ./klnagent64_<ビルド番号>_amd64.deb`

- ARM アーキテクチャの 64 ビットオペレーティングシステムに DEB パッケージからネットワークエージェントをインストールするには、次のコマンドを実行します：
  `# apt-get install ./klnagent64_<ビルド番号>_arm64.deb`

Linux 用ネットワークエージェントのインストールはサイレントモードで開始されます。ユーザーが、プロセス中に操作を要求されることはありません。

ネットワークエージェントをインストールするために、閉鎖ソフトウェア環境モードで Astra Linux を実行しているデバイスを準備します

閉鎖ソフトウェア環境モードで Astra Linux を実行しているデバイスにネットワークエージェントをインストールする前に、2 つの準備手順を実行する必要があります。1つは以下の手順にある手順、もう 1つは Linux デバイスの一般的な準備手順です。

事前準備：

- Linux 用ネットワークエージェントをインストールするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。
- 必要なネットワークエージェントインストールファイルをカスペルスキーの Web サイトからダウンロードします。

ルート権限を持つアカウントを使用してこの手順にあるコマンドを実行します。

ネットワークエージェントをインストールするために、閉鎖ソフトウェア環境モードで Astra Linux を実行しているデバイスを準備するには：

1. ファイル `/etc/digsig/digsig_initramfs.conf` を開き、次の設定を指定します：

   ```
   DIGSIG_ELF_MODE=1
   ```

2. コマンドラインで次のコマンドを実行して、適合パッケージをインストールします：

   ```
   apt install astra-digsig-oldkeys
   ```

3. 製品のライセンスにディレクトリを作成します：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. 前の手順で作成したディレクトリに製品のライセンス /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg を配置します：

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Kaspersky Security Center 配布キットに kaspersky_astra_pub_key.gpg ライセンスが含まれていない場合は、以下のリンクをクリックしてダウンロードできます：
   https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg。

5. RAM ディスクをアップデートします：

   ```
   update-initramfs -u -k all
   ```

システムを再起動します。

6. すべての Linux デバイスに共通の準備手順を実行します。

デバイスが準備されました。これで、ネットワークエージェントのインストールに進むことができます。

対話モードでの Linux 用ネットワークエージェントのインストール

この記事では、インストールパラメータを段階的に指定して、対話モードで Linux デバイスにネットワークエージェントをインストールする方法について説明します。あるいは、アンサーファイル（インストールパラメータのカスタムセットである変数とそれぞれの値を含むテキストファイル）を使用することもできます。この応答ファイルを使用すると、インストールをサイレントモードで、つまりユーザーの参加なしで実行できます。

RED OS 7.3.4 以降のオペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントが正しく機能するために libxcrypt-compat パッケージをインストールしてください。

対話モードでネットワークエージェントをインストールするには：

1. ネットワークエージェントのインストールを実行します。Linux ディストリビューションに応じて、次のコマンドを実行します：

   - RPM パッケージから 32 ビットオペレーティングシステムにネットワークエージェントをインストールするには：

     ```
     # yum -i klnagent-<build number>.i386.rpm
     ```

   - RPM パッケージから 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには：

     ```
     # yum -i klnagent64-<build number>.x86_64.rpm
     ```

   - Arm アーキテクチャの 64 ビットオペレーティングシステムに RPM パッケージからネットワークエージェントをインストールするには：

     ```
     # yum -i klnagent64-<build number>.aarch64.rpm
     ```

   - DEB パッケージから 32 ビットオペレーティングシステムにネットワークエージェントをインストールするには：

     ```
     # apt install ./klnagent_<build number>_i386.deb
     ```

   - DEB パッケージから 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには：

     ```
     # apt install ./klnagent64_<build number>_amd64.deb
     ```

   - Arm アーキテクチャの 64 ビットオペレーティングシステムに DEB パッケージからネットワークエージェントをインストールするには：

     ```
     # apt install ./klnagent64_<build number>_arm64.deb
     ```

2. ネットワークエージェントの構成を実行します：

   ```
   # /opt/kaspersky/klnagent64/bin/setup/postinstall.pl
   ```

3. 使用許諾契約書（EULA）をお読みください。テキストはコマンドラインウィンドウに表示されます。次のテキストセグメントを表示するにはスペースキーを押します。次に、確認が表示されてから次の値を入力

します：

- EULA の内容を確認して同意する場合は「y」を入力します。
- EULA の内容に同意しない場合は「n」を入力します。ネットワークエージェントを使用するには、EULA の内容に同意する必要があります。
- EULA を再度表示するには、 r と入力します。

4. 管理サーバーの DNS 名または IP アドレスを入力します。
5. 管理サーバーのポート番号を入力します。既定では、ポート 14000 が使用されます。
6. 管理サーバーの SSL ポート番号を入力します。既定では、ポート 13000 が使用されます。
7. ネットワークエージェントと管理サーバー間のトラフィックに SSL 暗号化を使用する場合は、 y と入力します。それ以外の場合は n と入力します。
8. ネットワークエージェントを設定するには、次のオプションのいずれかを選択します：
   - [1] - 接続ゲートウェイを設定しないでください。
     デバイスは接続ゲートウェイとして機能せず、接続ゲートウェイを介して管理サーバーに接続しません。
   - [2] – 接続ゲートウェイを使用しません。
     デバイスは接続ゲートウェイを介して管理サーバーに接続しません。
   - [3] – 接続ゲートウェイを使用してサーバーに接続する
     デバイスは接続ゲートウェイを介して管理サーバーに接続します。
   - [4] – 接続ゲートウェイとして使用します。
     デバイスは接続ゲートウェイとして機能します。

ネットワークエージェントは Linux デバイスにインストールされます。

アプリケーション管理プラグインのローカルインストール

アプリケーション管理プラグインをインストールするには：

管理コンソールがインストールされているデバイスで、アプリケーション配布パッケージに含まれている klcfginst.exe 実行ファイルを実行します。

klcfginst.exe は、Kaspersky Security Center で管理できるすべてのアプリケーションに含まれます。このインストールはウィザードで行うため、面倒な設定は必要ありません。

サイレントモードでアプリケーションをインストールする

アプリケーションをサイレントモードでインストールするには：

1. Kaspersky Security Center のメインウィンドウを開きます。

2. コンソールツリーにある［**リモートインストール**］フォルダーの［**インストールパッケージ**］サブフォルダーを開き、該当するアプリケーションのインストールパッケージを選択するか、インストールパッケージを新規作成します。

インストールパッケージは、管理サーバーで指定された共有フォルダー内のサブフォルダー Packages 内にあります。各インストールパッケージは、個別のサブフォルダー内に格納されています。

3. 次のいずれかの方法で、必要なインストールパッケージを格納するためのフォルダーを開きます：

- 管理サーバーからクライアントデバイスに関連するインストールパッケージに対応するフォルダーをコピーします。コピーしたフォルダーをクライアントデバイスで開きます。
- クライアントデバイスから、管理サーバーの必須インストールパッケージに対応する共有フォルダーを開きます。

Microsoft Windows Vista がインストールされたデバイスに共有フォルダーがある場合は、［**ユーザーアカウント制御：管理者承認モードですべての管理者を実行する**］の値を「**無効**」にする必要があります（［**スタート**］→［**コントロールパネル**］→［**管理ツール**］→［**ローカルセキュリティポリシー**］→［**セキュリティオプション**］）。

4. 選択したアプリケーションに応じて次の手順を実行します：

- Kaspersky Anti-Virus for Windows Workstations、Kaspersky Anti-Virus for Windows Servers、Kaspersky Security Center の場合、サブフォルダー exec に移動し、/s キーを指定して実行ファイル（exe 拡張子のファイル）を実行します。
- その他のカスペルスキー製品の場合は、開かれたフォルダーから /s キーを指定して実行ファイル（exe 拡張子のファイル）を実行します。

`EULA=1` および `PRIVACYPOLICY=1` キーを指定して実行ファイルを実行すると、使用許諾契約書とプライバシーポリシーそれぞれの内容をすべて確認し、理解した上で条項に同意したことになります。また、プライバシーポリシーに記載されているように、データが処理されて送信されること（第三国への送信を含む）も理解したことになります。使用許諾契約書とプライバシーポリシーの本文は、Kaspersky Security Center の配布キットに含まれています。アプリケーションのインストールまたは以前のバージョンのアプリケーションをアップグレードするには、使用許諾契約書とプライバシーポリシーに同意する必要があります。

スタンドアロンパッケージを使用したアプリケーションのインストール

Kaspersky Security Center で、アプリケーションインストール用のスタンドアロンパッケージを作成できます。スタンドアロンパッケージは実行ファイル形式で、Web サーバーやメールなどを利用してクライアントデバイスに送信できます。この実行ファイルをクライアントデバイスにダウンロードすると、Kaspersky Security Center を使用せずにアプリケーションをインストールすることが可能となります。

スタンドアロンインストールパッケージを使用してアプリケーションをインストールするには：

1. 目的の管理サーバーに接続します。
2. コンソールツリーの［**リモートインストール**］フォルダーで、［**インストールパッケージ**］サブフォルダーを選択します。

3. 必要なアプリケーションのインストールパッケージを選択します。

4. 次のいずれかの方法でスタンドアロンインストールパッケージの作成プロセスを開始します：

   - インストールパッケージのコンテキストメニューの［**スタンドアロンインストールパッケージの作成**］を選択します。

   - インストールパッケージの作業領域の［**スタンドアロンインストールパッケージの作成**］をクリックします。

   スタンドアロンインストールパッケージ作成ウィザードが起動します。ウィザードの指示に従ってください。

   最終手順に到達したら、スタンドアロンインストールパッケージの送信方法を指定します。

5. スタンドアロンインストールパッケージをクライアントデバイスに送信します。

6. クライアントデバイスでスタンドアロンインストールパッケージを実行します。

   これにより、スタンドアロンパッケージに指定されている設定を用いてクライアントデバイスにアプリケーションをインストールできます。

スタンドアロンインストールパッケージは作成時に、Web サーバー上に自動的に公開されます。スタンドアロンパッケージをダウンロードするリンクは、作成済みスタンドアロンインストールパッケージのリストに表示されます。必要に応じて、特定のスタンドアロンパッケージの公開を取り消したり、Web サーバーに再度公開したりすることができます。スタンドアロンインストールパッケージのダウンロードに使用される既定のポートは 8060 です。

ネットワークエージェントのインストールパッケージ設定

ネットワークエージェントのインストールパッケージを設定するには：

1. コンソールツリーの［**リモートインストール**］フォルダーで、［**インストールパッケージ**］サブフォルダーを選択します。

   既定では［**リモートインストール**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。

2. ネットワークエージェントのインストールパッケージのコンテキストメニューで、［**プロパティ**］を選択します。

ネットワークエージェントのインストールパッケージのプロパティウィンドウが表示されます。

全般

［**全般**］セクションには、インストールパッケージに関する全般的な情報が表示されます：

- インストールパッケージ名
- インストールパッケージでインストールされるアプリケーションの名前とバージョン
- インストールパッケージのサイズ
- インストールパッケージの作成日
- インストールパッケージのフォルダーのパス

設定

このセクションには、ネットワークエージェントをインストール後すぐに正常に機能させるのに必要な設定が示されます。このセクションの設定は、Windows を実行しているデバイスでのみ使用できます。

［**インストール先フォルダー**］設定グループでは、ネットワークエージェントがインストールされるクライアントデバイスのフォルダーを選択できます。

- **既定のフォルダーにインストールする**

  このオプションをオンにすると、ネットワークエージェントは、フォルダー <ドライブ名>:\Program Files\Kaspersky Lab\NetworkAgent にインストールされます。このフォルダーがない場合は、フォルダーが自動的に作成されます。

  既定では、このオプションがオンです。

- **指定したフォルダーにインストールする**

  このオプションをオンにすると、ネットワークエージェントは、入力フィールドで指定したフォルダーにインストールされます。

次の設定グループでは、ネットワークエージェントのリモートアンインストールタスク用のパスワードを設定できます：

- **アンインストール用パスワードを使用する**

  このオプションをオンにすると、［**変更**］をクリックしてアンインストール用パスワード（Windows オペレーティングシステム実行中のデバイスのネットワークエージェントのみに使用可能）を入力できます。

  既定では、このオプションはオフです。

- **ステータス**

  パスワードのステータス：**パスワード設定あり**または**パスワード設定なし**です。

  既定では、パスワードは設定されていません。

- **ネットワークエージェントを不正な削除・停止から保護し、設定の変更を防止する**

  このオプションをオンにすると、管理対象デバイスにネットワークエージェントのインストールされた後、必要な権限がない場合はコンポーネントの削除や再設定が行えなくなります。また、ネットワークエージェントサービスを停止できなくなります。このオプションはドメインコントローラーに影響しません。

  ローカル管理者権限で操作されているワークステーション上のネットワークエージェントを保護するには、このオプションをオンにします。

  既定では、このオプションはオフです。

- **コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**

このオプションをオンにすると、管理サーバー、ネットワークエージェント、管理コンソール、および iOS MDM サーバー用にダウンロードされたすべてのアップデートとパッチが自動的にインストールされます。

このオプションをオフにすると、ダウンロードされたすべてのアップデートとパッチは、アップデートとパッチのステータスを［*承認*］に変更した後にインストールされます。［*未定義*］ステータスのアップデートとパッチはインストールされません。

既定では、このオプションはオンです。

接続

このセクションでは、ネットワークエージェントから管理サーバーへの接続を設定できます：接続を確立するために、SSL または UDP プロトコルを使用できます。接続を設定するには、次の設定を指定します：

- **管理サーバー**

  管理サーバーがインストールされたデバイスのアドレス。

- **ポート**

  接続に使用されるポート番号。

- **SSL ポート**

  SSL プロトコルによる接続に使用されるポート番号。

- **サーバー証明書を使用する**

  このオプションをオンにすると、［**参照**］をクリックして指定できる証明書ファイルが、ネットワークエージェントの管理サーバーへのアクセス認証に使用されます。

  このオプションをオフにすると、［**サーバーアドレス**］で指定したアドレスへのネットワークエージェントからかの初回接続時に、管理サーバーから証明書ファイルを受信します。

  管理サーバーへの接続時にネットワークエージェントで管理サーバー証明書を自動受信することはセキュアでないため、このオプションの無効化は推奨されません。

  既定では、このチェックボックスはオンです。

- **SSL を使用する**

  このオプションをオンにすると、SSL を使用してセキュアなポート経由で管理サーバーへの接続が確立されます。

  既定では、このオプションはオフです。セキュアな接続を保つために、このオプションを無効にしないことを推奨します。

- **UDP ポートを使用する**

このオプションをオンにすると、ネットワークエージェントは UDP ポート経由で管理サーバーに接続されます。これにより、クライアントデバイスを管理し、それらに関する情報を受け取ることができます。

ネットワークエージェントがインストールされている管理対象デバイスで,UDP ポートを開放する必要があります。したがって、このオプションを無効にしないことを推奨します。

既定では、このオプションはオンです。

- **UDP ポート番号**

  このフィールドでは、UDP プロトコル経由で管理サーバーがネットワークエージェントに接続するポートを指定できます。

  既定の UDP ポート番号は 15000 です。

- **Microsoft Windows ファイアウォールでネットワークエージェントのポートを開く**

  このオプションをオンにすると、ネットワークエージェントによって使用されるポートが Microsoft Windows ファイアウォールの除外リストに追加されます。

  既定では、このオプションはオンです。

- **プロキシサーバーを使用する**

  このオプションをオフにすると、デバイスを管理サーバーに接続するために直接接続が使用されます。

  このオプションをオンにする場合は、プロキシサーバーのパラメータを指定します：

  - **プロキシサーバーアドレス**
  - **プロキシサーバーのポート**

  プロキシサーバーで認証が必要な場合は、［**プロキシサーバー認証**］をオンにし、プロキシサーバーへの接続を確立するアカウントの**ユーザー名**と**パスワード**を指定します。プロキシサーバー認証に必要な最小限の権限が付与されているアカウントの資格情報を指定することを推奨します。

互換性のため、ネットワークエージェントのインストール パッケージ設定でプロキシ接続設定を指定することはお勧めしません。

詳細

［**詳細**］セクションでは、接続ゲートウェイの使用方法を設定できます。この目的のために、次の操作を実行できます：

- 非武装地帯（DMZ）の接続ゲートウェイとしてネットワークエージェントを使用して管理サーバーへの接続、管理サーバーとの通信を実行し、データ転送中にネットワークエージェント上のデータを安全に保ちます。
- 接続ゲートウェイを使用して管理サーバーに接続し、管理サーバーへの接続数を減らします。この場合、接続ゲートウェイとして機能するデバイスのアドレス［**接続ゲートウェイアドレス**］フィールドに入力します。
- ネットワークに仮想マシンが含まれている場合は、仮想デスクトップインフラストラクチャ（VDI）の接続を設定します。この目的のために、次を実行します：

- **VDI 向け動的モードを有効にする**

  このオプションをオンにすると、仮想マシンにインストールされたネットワークエージェントで仮想デスクトップインフラストラクチャ（VDI）向け動的モードが有効になります。

  既定では、このオプションはオフです。

- **VDI 向けに設定を最適化する**

  このオプションをオンにすると、ネットワークエージェントの設定で次の機能が無効にされます：

  - インストールされたソフトウェアに関する情報の取得
  - ハードウェアに関する情報の取得
  - 検知された脆弱性に関する情報の取得
  - 必要なアップデートに関する情報の取得

  既定では、このオプションはオフです。

追加コンポーネント

このセクションでは、ネットワークエージェントと同時にインストールする追加コンポーネントを選択できます。

タグ

［**タグ**］セクションには、ネットワークエージェントのインストール後にクライアントデバイスに追加できるキーワード（タグ）のリストが表示されます。リストへのタグの追加、リストからのタグの削除、タグの名前の変更を行うことができます。

タグの横のチェックボックスがオンの場合、そのタグは、ネットワークエージェントのインストール時に、管理対象デバイスに自動的に追加されます。

タグに隣接するチェックボックスをオフにすると、ネットワークエージェントのインストール時に、管理対象デバイスに自動的には追加されません。タグは手動でデバイスに追加できます。

リストからタグを削除すると、そのタグは、そのタグが追加されたすべてのデバイスから自動的に削除されます。

変更履歴

このセクションでは、インストールパッケージのリビジョンの履歴を確認できます。リビジョンの比較、リビジョンの表示、リビジョンのファイル保存、リビジョンの説明の追加と編集ができます。

次の表に、各オペレーティングシステムで利用できるネットワークエージェントのインストールパッケージ設定を示します。

ネットワークエージェントのインストールパッケージ設定

プロパティセクション	Windows	Mac	Linux
全般	✓	✓	✓

設定	✓	—	—
接続	✓	✓ （ただし、［**Microsoft Windows ファイアウォールでネットワークエージェントのポートを開く**］および［**プロキシサーバーの自動検出のみを使用する**］を除く）	✓ （ただし、［**Microsoft Windows ファイアウォールでネットワークエージェントのポートを開く**］および［**プロキシサーバーの自動検出のみを使用する**］を除く）
詳細	✓	✓	✓
追加コンポーネント	✓	✓	✓
タグ	✓	✓ （ただし、自動タグルールを除く）	✓ （ただし、自動タグルールを除く）
変更履歴	✓	✓	✓

プライバシーポリシーの表示

プライバシーポリシーは、https://www.kaspersky.co.jp/products-and-services-privacy-policy からオンラインで入手でき、オフラインでも利用できます。たとえば、ネットワークエージェントをインストールする前にプライバシーポリシーを読むことができます。

プライバシーポリシーをオフラインで読むには：

1. Kaspersky Security Center のインストーラーを起動します。
2. インストーラーウィンドウで、［**インストールパッケージの解凍**］リンクに進みます。
3. 開いたリストで、［Kaspersky Security Center ネットワークエージェント］を選択し、［**次へ**］をクリックします。

ファイル Privacy_policy.txt がデバイスの指定したフォルダーのサブフォルダー NetAgent に表示されます。

モバイルデバイス管理システムの導入

このセクションでは、iOS MDM および Kaspersky Endpoint Security のプロトコルを使用して、モバイルデバイス管理システムを導入する方法について説明します。

iOS MDM プロトコルを使用した管理システムの導入

Kaspersky Security Center では、iOS を動作させているモバイルデバイスを管理できます。iOS MDM デバイスとは、iOS MDM サーバーに接続され、管理サーバーによって管理される iOS モバイルデバイスのことです。

モバイルデバイスは、次の手順で iOS MDM サーバーに接続されます：

1. 管理者はiOS MDM サーバーをインストールします。
2. 管理者は、APNs（Apple Push Notification Service）証明書を取得します。

   APNs 証明書により、管理サーバーが APNs サーバーに接続し、iOS MDM デバイスにプッシュ通知を送信できます。

3. iOS MDM サーバーに APNs 証明書をインストールします。

4. iOS モバイルデバイスのユーザー用に iOS MDM プロファイルを作成します。

   iOS MDM プロファイルには、iOS モバイルデバイスが管理サーバーに接続するための設定が含まれます。

iOS MDM プロファイルのインストールがされて、iOS MDM デバイスが管理サーバーと同期されると、そのデバイスが、コンソールツリーの［**モバイルデバイス管理**］サブフォルダーにある［**モバイルデバイス**］フォルダーに表示されます。

iOS MDM サーバーのインストール

iOS MDM サーバーをローカルデバイスにインストールするには：

1. 実行ファイル setup.exe を実行します。

   ウィンドウが開き、インストールするカスペルスキー製品の選択を要求されます。

   製品を選択するウィンドウで、［**iOS MDM サーバーのインストール**］をクリックし、iOS MDM サーバーのセットアップウィザードを開始します。

2. インストール先フォルダーを選択します。

   既定のインストール先フォルダーは、<ドライブ名>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS です。このフォルダーがない場合は、インストール中に自動的に作成されます。インストール先フォルダーは、［**参照**］を使用して変更できます。

3. ウィザードの［**iOS MDM サーバーへの接続を設定します**］ウィンドウの［**iOS MDM サービスへの外部アクセスポート**］で、モバイルデバイスが iOS MDM サービスに接続するための外部ポートを指定します。

   外部ポート 5223 が、モバイルデバイスによって APNs サーバーとの通信のために使用されます。ファイアウォールで、ポート 5223 がアドレス範囲 17.0.0.0/8 に対して開いていることを確認してください。

   既定では、ポート 443 が iOS MDM サーバーとの接続のために使用されます。ポート 443 が別のサービスやアプリケーションによって使用されている場合、ポート 9443 などに変更できます。

   iOS MDM サーバーは、外部ポート 2197 を APNs サーバーへの送信通知に使用します。

   APNs サーバーは、ロードバランシングモードで実行されます。モバイルデバイスが通知を受け取る IP アドレスは、常に同じではありません。アドレス範囲 17.0.0.0/8 が Apple によって予約されています。そのため、ファイアウォールの設定では、この範囲の全体を許可するよう指定してください。

4. アプリケーションコンポーネント用の対話ポートを手動で構成する場合、［**手動でローカルポートを設定する**］をオンにし、次の設定値を指定します：

   - **ネットワークエージェント接続用ポート**：このフィールドでは、iOS MDM サービスをネットワークエージェントに接続するためのポートを指定します。既定のポート番号は 9799 です。

   - **iOS MDM サービスへの接続用ローカルポート**：このフィールドでは、ネットワークエージェントを iOS MDM サービスに接続するためのローカルポートを指定します。既定のポート番号は 9899 です。

   既定値を使用してください。

5. ウィザードの［**モバイルデバイスサーバーの外部アドレスです**］ウィンドウの［**モバイルデバイスサーバーへのリモート接続用 URL**］に、iOS MDM サーバーをインストールするクライアントデバイスのアドレスを入力します。

   このアドレスは、管理対象のモバイルデバイスを iOS MDM サービスに接続するために使用されます。iOS MDM デバイスが接続するためには、このクライアントデバイスが使用可能になっている必要があります。

クライアントデバイスのアドレスは、次のいずれかのフォーマットで指定します：

- デバイスの FQDN（mdm.example.com など）
- デバイスの NetBIOS 名

URL スキームおよびポート番号をアドレスに追加しないでください。これらの値は自動的に追加されます。

ウィザードが終了すると、iOS MDM サーバーがローカルデバイスにインストールされます。iOS MDM サーバーが、コンソールツリーの［**モバイルデバイス管理**］フォルダーに表示されます。

サイレントモードでの iOS MDM サーバーのインストール

Kaspersky Security Center では、iOS MDM サーバーをローカルデバイスにサイレントモードでインストール設定を対話的に入力することなくインストールできます。

iOS MDM サーバーをローカルデバイスにサイレントモードでインストールするには：

1. 使用許諾契約書をお読みください。以下のコマンドは、使用許諾契約書の内容を理解して条項に同意する場合にのみ使用してください。
2. 次のコマンドを実行します：
   `.\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 <セットアップパラメータ>"`
   ここで、<セットアップパラメータ>には、設定と対応する値のペアをスペースで区切って並べます（例：`PROP1=PROP1VAL PROP2=PROP2VAL`）。Setup.exe ファイルは Server フォルダーにあり、これは Kaspersky Security Center 配布キットに含まれています。

iOS MDM サーバーをサイレントモードでインストールする時に使用できるパラメータの名前と可能な値は、以下の表の通りです。パラメータは任意の順序で指定できます。

サイレントモードでの iOS MDM サーバーのインストールパラメータ

パラメータ名	パラメータの説明	設定可能な値
EULA	使用許諾契約書の条項への同意。このパラメータは必須です。	• 1 – 使用許諾契約書の内容をすべて確認し、理解した上で条項に同意します。 • その他の値または値なし – 使用許諾契約書に同意しません（インストールは実行されません）。
DONT_USE_ANSWER_FILE	iOS MDM サーバーのインストール設定が記述された XML ファイルを使用するかどうか。 XML ファイルは、インストールパッケージに含まれているか、管理サーバーに保存されています。ファイルのパスを指定する必要はありません。 このパラメータは必須です。	• 1 - パラメータを含む XML ファイルを使用しない。 • その他の値、または値なし - パラメータを含む XML ファイルを使用する。
INSTALLDIR	iOS MDM サーバーをインストールするフォルダー。 このパラメータの指定は任意です。	文字列。例： `INSTALLDIR=\"C:\install\"`
CONNECTORPORT	iOS MDM サービスをネットワークエージェントに接続するローカルポート。 既定のポート番号は 9799 です。 このパラメータの指定は任意です。	数値

LOCALSERVERPORT	ネットワークエージェントを iOS MDM サービスに接続するローカルポート。 既定のポート番号は 9899 です。 このパラメータの指定は任意です。	数値
EXTERNALSERVERPORT	デバイスを iOS MDM サーバーに接続するポート。 既定のポート番号は 443 です。 このパラメータの指定は任意です。	数値
EXTERNAL_SERVER_URL	iOS MDM サーバーをインストールするクライアントデバイスの外部アドレス。このアドレスは、管理対象のモバイルデバイスを iOS MDM サービスに接続するために使用されます。iOS MDM で接続するためには、このクライアントデバイスが使用可能になっている必要があります。 アドレスには URL スキームやポート番号を含めないでください。これらの値は自動的に追加されます。 このパラメータの指定は任意です。	• デバイスの FQDN（mdm.example.com など） • デバイスの NetBIOS 名 • デバイスの IP アドレス
WORKFOLDER	iOS MDM サーバーの作業フォルダー 作業フォルダーを指定しない場合、データは既定のフォルダーに書き込まれます。 このパラメータの指定は任意です。	文字列。例： `WORKFOLDER=\"C:\work\"`
MTNCY	複数の仮想サーバーで iOS MDM サーバーを使用する。 このパラメータの指定は任意です。	• 1 - 複数の仮想管理サーバーで iOS MDM サーバーを使用する • その他の値、または値なし - 複数の仮想管理サーバーで iOS MDM サーバーを使用しない

例：

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

iOS MDM サーバーのインストールパラメータについては、「iOS MDM サーバーのインストール」セクションで詳しく説明しています。

iOS MDM サーバーの導入シナリオ

インストールする iOS MDM サーバーのコピー数は、使用可能なハードウェア、または対象となるモバイルデバイスの合計数に基づき選択できます。

1つの Kaspersky Device Management for iOS で管理するモバイルデバイスは、できるだけ 50,000 台以下にしてください。負荷を削減するために、iOS MDM サーバーがインストールされた複数のサーバー間にデバイスのプール全体を分散させることができます。

iOS MDM デバイスの認証は、ユーザー証明書を使用して実施されます（デバイスにインストールされた任意のプロファイルには、デバイス所有者の証明書が含まれます）。そのため、1つの iOS MDM サーバーに対して次の 2 つの導入スキームが可能です：

- 簡易スキーム
- Kerberos の制約付き委任（KCD）を使用した導入スキーム

簡易導入スキーム

簡易スキームに基づき iOS MDM サーバーを導入する場合、モバイルデバイスは iOS MDM Web サービスに直接接続されます。この場合、管理サーバーで発行されたユーザー証明書は、デバイス認証にのみ利用されます。公開鍵基盤（PKI）との統合は、ユーザー証明書の場合は不可能です。

Kerberos の制約付き委任（KCD）を使用した導入スキーム

Kerberos 制約付き委任 (KCD) で導入スキームを使用するには、次の要件を満たす必要があります：

- 管理サーバーと iOS MDM サーバーは、組織の内部ネットワーク上に配置されます。
- KCD をサポートするリバースプロキシが使用されています。

この導入スキームでは以下が実現されます：

- KCD をサポートするリバースプロキシとの統合
- KCD を使用したモバイルデバイスの認証
- PKI との統合によるユーザー証明書の適用

この導入スキームを使用する場合、以下を実行する必要があります：

- 管理コンソールの iOS MDM Web サービスの設定で［**Kerberos の制約付き委任との互換性を確保する**］をオンにします。
- iOS MDM Web サービスがリバースプロキシで公開された際に定義されたカスタマイズ済みの証明書を、iOS MDM Web サービスの証明書として指定します。
- iOS デバイスのユーザー証明書は、ドメインの Certificate Authority（CA）によって発行される必要があります。ドメインに複数のルート CA がある場合、ユーザー証明書は、iOS MDM Web サービスがリバースプロキシで公開された時に指定された CA によって発行される必要があります。

  以下の方法のいずれかを使用して、ユーザー証明書が、この CA の発行要件を満たしていることを確認できます：

  - 新しい iOS MDM プロファイルウィザードと証明書インストールウィザードでユーザー証明書を指定します。
  - 管理サーバーとドメインの PKI を統合し、証明書発行ルールの該当する設定を定義します：

    1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを展開し、［**証明書**］サブフォルダーを選択します。
    2. ［**証明書**］フォルダーの作業領域で［**証明書の発行ルールを指定する**］をクリックして［**証明書発行ルール**］ウィンドウを表示します。
    3. ［**PKI（公開鍵基盤）の統合**］セクションで、公開鍵基盤との統合を設定します。
    4. ［**モバイル証明書の発行**］セクションで、証明書のソースを指定します。

以下を前提とした Kerberos の制約付き委任（KCD）の設定例を次に示します：

- iOS MDM Web サービスがポート 443 で実行されている。
- リバースプロキシを備えたデバイスの名前は、firewall.mydom.local です。

- iOS MDM Web サービスがインストールされたデバイスの名前が iosmdm.mydom.local である。
- iOS MDM Web サービスの外部公開名が iosmdm.mydom.global である。

http/iosmdm.mydom.local のサービスプリンシパル名

ドメインで、iOS MDM Web サービスがインストールされたデバイス（iosmdm.mydom.local）のサービスプリンシパル名（SPN）を次のように登録する必要があります：

```
setspn -a http/iosmdm.mydom.local iosmdm
```

リバースプロキシ（firewall.mydom.local）を持つデバイスのドメインプロパティを設定します

トラフィックを委任するには、SPN によって定義されたサービス（http/iosmdm.mydom.local）に対してリバースプロキシ（firewall.mydom.local）を備えたデバイスを信頼します。

SPN によって定義されたサービス（http/iosmdm.mydom.local）に対してリバースプロキシを持つデバイスを信頼させるには、管理者は以下の操作を実行する必要があります：

1. 「Active Directory Users and Computers」という名前の Microsoft 管理コンソールスナップインで、リバースプロキシがインストールされているデバイス（firewall.mydom.local）を選択します。
2. デバイスのプロパティの［**委任**］タブで、［**このコンピューターを、指定されたサービスの委任に限って信頼する**］トグルを［**任意の認証プロトコルを使用する**］に設定します。
3. SPN（http/iosmdm.mydom.local）を［**このアカウントが委任された資格情報を提供できるサービス**］リストに追加します。

公開された Web サービス（iosmdm.mydom.global）向けの専用（カスタマイズ済み）の証明書

FQDN iosmdm.mydom.global の iOS MDM Web サービス向けの専用（カスタマイズ済み）の証明書を発行し、管理コンソールの iOS MDM Web サービスの設定で、既定の証明書に置き換えるように指定する必要があります。

証明書のコンテナー（拡張子が p12 または pfx のファイル）には、ルート証明書（公開鍵）のチェーンも含まれる必要があることに留意してください。

リバースプロキシでの iOS MDM Web サービスの公開

リバースプロキシでは、モバイルデバイスから iosmdm.mydom.global のポート 443 に向かうトラフィックについては、FQDN（iosmdm.mydom.global）に対して発行された証明書を使用して、
SPN（http/iosmdm.mydom.local）上で KCD を設定する必要があります。公開中、および公開済みの Web サービスは、同じサーバー証明書を共有しなければならないことに留意してください。

APNs 証明書の取得

既に APNs 証明書をお持ちの場合は、新しく作成する代わりに更新を検討してください。既存の APNs 証明書を新しく作成した証明書に置換すると、管理サーバーは現在接続されている iOS モバイルデバイスの管理ができなくなります。

APNs 証明書ウィザードの最初のステップで証明書署名リクエスト（CSR）が作成される時に、その秘密鍵がデバイスの RAM に保存されます。したがって、ウィザードのすべてのステップを中断することなく最後まで実行する必要があります。

APNs 証明書を取得するには：

1. コンソールツリーの［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイスサーバー**］サブフォルダーを選択します。
2. ［**モバイルデバイスサーバー**］フォルダーの作業領域で、iOS MDM サーバーを選択します。
3. iOS MDM サーバーのコンテキストメニューで、［**プロパティ**］を選択します。
   iOS MDM サーバーのプロパティウィンドウが表示されます。
4. iOS MDM サーバーのプロパティウィンドウで［**証明書**］セクションを選択します。
5. ［**証明書**］セクションの［**Apple Push Notification 証明書**］で［**新規リクエスト**］をクリックします。
   APNs 証明書の取得ウィザードが開始され、［**新規リクエスト**］ウィンドウが表示されます。
6. 証明書署名リクエスト（以降「CSR」と表記）を作成します。それには、次の操作を実行します：
   a. ［**CSR の作成**］をクリックします。
   b. 表示される［**CSR の作成**］ウィンドウで、リクエストの名前、会社名と部門、所在地を指定します。
   c. ［**保存**］をクリックし、CSR を保存するファイルの名前を指定します。

   証明書の秘密鍵がデバイスのメモリに保存されます。
7. 作成した CSR ファイルを、カンパニーアカウントを使用してカスペルスキーに送信し、署名を要求します。

   CSR への署名は、モバイルデバイス管理の使用を許可する鍵をカスペルスキーカンパニーアカウントポータルにアップロードするまで受けられません。

   オンラインリクエストの処理の後、カスペルスキーによって署名された CSR ファイルが送られてきます。
8. 任意の Apple ID を使用して、署名済み CSR ファイルを Apple Inc. の Web サイトに送信します。

   個人の Apple ID の使用は避けてください。法人用に専用の Apple ID を作成してください。Apple ID を作成した後、それを組織のメールボックスにリンクします。従業員のメールボックスにはリンクしないでください。

   Apple Inc. で CSR の処理が終わると、APNs 証明書の公開鍵が送られてきます。そのファイルをディスクに保存します。

9. CSR の生成時に作成された秘密鍵とともに、APNs 証明書を PFX ファイル形式でエクスポートします。次の操作を行います：

   a. ［**新規 APNs 証明書のリクエスト**］ウィンドウで、［**CSR の完了**］をクリックします。

   b. ［**開く**］ウィンドウで、CSR 処理の結果として Apple Inc. から受け取った証明書の公開鍵が入ったファイルを選択し、［**開く**］をクリックします。

      証明書のエクスポートが開始されます。

   c. 次のウィンドウで、秘密鍵のパスワードを入力し、［**OK**］をクリックします。

      このパスワードは、iOS MDM サーバーに APNs 証明書をインストールするために使用されます。

   d. ［**APNs 証明書の保存**］ウィンドウで、APNs 証明書のファイル名を指定し、フォルダーを選択し、［**保存**］をクリックします。

証明書の秘密鍵と公開鍵が組み合わされ、APNs 証明書が PFX フォーマットで保存されます。その後、iOS MDM サーバーにこの APNs 証明書をインストールできます。

APNs 証明書の更新

APNs 証明書を更新するには：

1. コンソールツリーの［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイスサーバー**］サブフォルダーを選択します。
2. ［**モバイルデバイスサーバー**］フォルダーの作業領域で、iOS MDM サーバーを選択します。
3. iOS MDM サーバーのコンテキストメニューで、［**プロパティ**］を選択します。

   iOS MDM サーバーのプロパティウィンドウが表示されます。
4. iOS MDM サーバーのプロパティウィンドウで［**証明書**］セクションを選択します。
5. ［**証明書**］セクションの［**Apple Push Notification 証明書**］で［**更新**］をクリックします。

   APNs 証明書の更新ウィザードが開始され、［**APNs 証明書を更新する**］ウィンドウが表示されます。
6. 証明書署名要求（以降「CSR」と表記）を作成します。それには、次の操作を実行します：

   a. ［**CSR の作成**］をクリックします。

   b. 表示される［**CSR の作成**］ウィンドウで、リクエストの名前、会社名と部門、所在地を指定します。

   c. ［**保存**］をクリックし、CSR を保存するファイルの名前を指定します。

   証明書の秘密鍵がデバイスのメモリに保存されます。
7. 作成した CSR ファイルを、カンパニーアカウントを使用してカスペルスキーに送信し、署名を要求します。

   CSR への署名は、モバイルデバイス管理の使用を許可する鍵をカスペルスキーカンパニーアカウントポータルにアップロードするまで受けられません。

オンラインリクエストの処理の後、カスペルスキーによって署名された CSR ファイルが送られてきます。

8. 任意の Apple ID を使用して、署名済み CSR ファイルを Apple Inc. の Web サイト に送信します。

   個人の Apple ID の使用は避けてください。法人用に専用の Apple ID を作成してください。Apple ID を作成した後、それを組織のメールボックスにリンクします。従業員のメールボックスにはリンクしないでください。

   Apple Inc. で CSR の処理が終わると、APNs 証明書の公開鍵が送られてきます。そのファイルをディスクに保存します。

9. 証明書の公開鍵をリクエストします。それには、次の操作を実行します：

   a. Apple Push Certificates ポータル を開きます。証明書の最初のリクエスト時に受け取った Apple ID を使用してポータルにログインします。

   b. 証明書のリストで、APSP 名（「APSP: <番号>」の形式）が iOS MDM サーバーで使用している証明書の APSP 名と一致する証明書を選択し、［**更新**］をクリックします。

      APNs 証明書が更新されます。

   c. ポータルで作成された証明書を保存します。

10. CSR の生成時に作成された秘密鍵とともに、APNs 証明書を PFX ファイル形式でエクスポートします。それには、次の操作を実行します：

    a. ［**APNs 証明書を更新する**］ウィンドウで、［**CSR の完了**］をクリックします。

    b. ［**開く**］ウィンドウで、CSR 処理の結果として Apple Inc. から受け取った、証明書の公開鍵が入ったファイルを選択し、［**開く**］をクリックします。

       証明書のエクスポートが開始されます。

    c. 次のウィンドウで、秘密鍵のパスワードを入力し、［**OK**］をクリックします。

       このパスワードは、iOS MDM サーバーに APNs 証明書をインストールするために使用されます。

    d. ［**APNs 証明書を更新する**］ウィンドウが開いたら、APNs 証明書のファイル名前を指定し、フォルダーを選択し、［**保存**］をクリックします。

証明書の秘密鍵と公開鍵が組み合わされ、APNs 証明書が PFX フォーマットで保存されます。

予備の iOS MDM サーバー証明書の設定

iOS MDM サーバーの機能を使用すると、予備証明書を発行できます。予備証明書は、iOS MDM サーバー証明書の有効期限が切れた後、管理対象 iOS デバイスの切り替えがシームレスに行われるように、iOS MDM プロファイルで使用することを目的としています。

iOS MDM サーバーがカスペルスキーによって発行された既定の証明書を使用している場合、iOS MDM サーバー証明書の有効期限が切れる前に、予備証明書を発行できます（または独自のカスタム証明書を予備として指定できます）。既定では、予備証明書は iOS MDM サーバー証明書の有効期限が切れる 60 日前に自動的に発行されます。予備の iOS MDM サーバー証明書は、iOS MDM サーバー証明書の有効期限が切れるとすぐに、メインの証明書になります。公開鍵は設定プロファイルを介してすべての管理対象デバイスに配布されるため、手動で送信する必要はありません。

予備の iOS MDM サーバー証明書の発行、またはカスタムの予備証明書の指定を行うには：

1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーにある［**モバイルデバイスサーバー**］サブフォルダーを選択します。

2. モバイルデバイスサーバーのリストで、目的の iOS MDM サーバーを選択し、右側のペインで［**iOS MDM サーバーを設定**］をクリックします。

3. 表示される iOS MDM サーバーの設定ウィンドウで、［**証明書**］セクションを選択します。

4. 設定の［**予備の証明書**］ブロックで、次のいずれかを実行します：

   - 自己署名証明書（つまり、カスペルスキーによって発行された証明書）を引き続き使用する場合：

     a. ［**発行**］をクリックします。

     b. 表示される［**アクティベーション日時**］ウィンドウで、予備証明書を適用する日付について 2 つのオプションのいずれかをオンにします：

        - 現在の証明書の有効期限が切れた時に予備証明書を適用する場合は、［**現在の証明書の有効期限が切れた時**］をオンにします。

        - 現在の証明書の有効期限が切れる前に予備証明書を適用する場合は、［**指定した期間の経過後（日）**］をオンにします。このオプションの横の入力フィールドで、現在の証明書を予備証明書に置き換えるまでの期間を指定します。

        > 指定する予備証明書の有効期間は、現在の iOS MDM サーバー証明書の有効期間を超えることはできません。

     c. ［**OK**］をクリックします。

     予備の iOS MDM サーバー証明書が発行されます。

   - 認証局によって発行されたカスタム証明書を使用する場合：

     a. ［**追加**］をクリックします。

     b. 表示されるファイルエクスプローラーのウィンドウで、デバイスに保存されている PEM、PFX、P12 形式の証明書ファイルを指定し、［**開く**］をクリックします。

     カスタム証明書が予備の iOS MDM サーバー証明書として指定されます。

これで、予備の iOS MDM サーバー証明書が指定されました。予備証明書の詳細は、設定の［**予備の証明書**］ブロックに表示されます（証明書名、発行者名、有効期限、予備証明書を適用する日付（存在する場合））。

iOS MDM サーバーへの APNs 証明書のインストール

APNs 証明書を取得した後、それを iOS MDM サーバーにインストールする必要があります。

iOS MDM サーバーに APNs 証明書をインストールするには：

1. コンソールツリーの［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイスサーバー**］サブフォルダーを選択します。

2. ［**モバイルデバイスサーバー**］フォルダーの作業領域で、iOS MDM サーバーを選択します。

3. iOS MDM サーバーのコンテキストメニューで、［**プロパティ**］を選択します。
   iOS MDM サーバーのプロパティウィンドウが表示されます。

4. iOS MDM サーバーのプロパティウィンドウで［**証明書**］セクションを選択します。

5. ［**証明書**］セクションの［**Apple Push Notification 証明書**］で［**インストール**］をクリックします。

6. APNs 証明書が含まれる PFX ファイルを選択します。

7. APNs 証明書のエクスポート時に指定した秘密鍵のパスワードを入力します。

APNs 証明書が iOS MDM サーバーにインストールされます。証明書の詳細は、iOS MDM サーバーのプロパティウィンドウの［**証明書**］セクションに表示されます。

Apple Push Notification サービスへのアクセスの設定

iOS MDM Web サービスが適切に機能し、モバイルデバイスが管理者のコマンドに適時に応答するようにするには、iOS MDM サーバー設定で、Apple Push Notification サービス証明書（以下、「APNs 証明書」）を指定する必要があります。

Apple Push Notification（以降、「APNs」と表記）と通信する iOS MDM Web サービスは、ポート 2197（送信）経由で外部アドレスの api.push.apple.com に接続されます。そのため、iOS MDM Web サービスは、アドレス範囲 17.0.0.0/8 でポート TCP 2197 にアクセスする必要があります。iOS デバイス側からは、アドレス範囲 17.0.0.0/8 でポート TCP 5223 にアクセスします。

iOS MDM Web サービス側からプロキシサーバー経由で APNs にアクセスする場合は、iOS MDM Web サービスがインストールされたデバイスで以下の操作を実行する必要があります：

1. 次の文字列をレジストリに追加します：

   - 32 ビットオペレーティングシステム：

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<プロキシのホスト名>"
"ApnProxyPort"="<プロキシのポート>"
"ApnProxyLogin"="<プロキシのログイン>"
"ApnProxyPwd"="<プロキシのパスワード>"
```

   - 64 ビットオペレーティングシステム：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<プロキシのホスト名>"
"ApnProxyPort"="<プロキシのポート>"
"ApnProxyLogin"="<プロキシのログイン>"
"ApnProxyPwd"="<プロキシのパスワード>"
```

2. iOS MDM ウェブサービスを再起動します。

モバイルデバイスの共有証明書の発行とインストール

共有証明書をユーザーに発行するには：

1. コンソールツリーで、［**ユーザーアカウント**］フォルダーからユーザーアカウントを選択します。
2. ユーザーアカウントのコンテキストメニューで、［**証明書のインストール**］を選択します。

   証明書インストールウィザードが起動します。ウィザードの指示に従ってください。

ウィザードが終了すると、証明書が作成され、ユーザーの証明書のリストに追加されます。

発行された証明書は、iOS MDM プロファイルを含むインストールパッケージと一緒にユーザーによってダウンロードされます。

モバイルデバイスが iOS MDM サーバーに接続されると、iOS MDM プロファイルの設定がデバイスに適用されます。管理者は、接続後にデバイスを管理できます。

iOS MDM サーバーに接続されたモバイルデバイスは、コンソールツリーの［**モバイルデバイス管理**］フォルダーにある［**モバイルデバイス**］サブフォルダーに表示されます。

管理対象デバイスのリストへの KES デバイスの追加

Google Play™ へのリンクを使用して、ユーザーの KES デバイスを管理対象デバイスのリストに追加するには：

1. コンソールツリーで、［**ユーザーアカウント**］フォルダーを選択します。

   既定では、［**ユーザーアカウント**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。
2. 管理対象デバイスのリストに追加するモバイルデバイスのユーザーのアカウントを選択します。
3. ユーザーアカウントを右クリックし、コンテキストメニューで［**モバイルデバイスの追加**］を選択します。

   モバイルデバイスの接続ウィザードが起動します。ウィザードの［**証明書ソース**］ウィンドウで、管理サーバーがモバイルデバイスの識別に使用する共有証明書の作成方法を指定します。次のいずれかの方法で、共有証明書を指定できます：

   - 管理サーバーツールを使用して自動で共有証明書を作成した後、デバイスに配信する。
   - 共有証明書ファイルを指定する。
4. ウィザードの［**デバイス種別**］ウィンドウで、［**Google Play へのリンク**］を選択します。
5. ウィザードの［**ユーザー通知方法**］ウィンドウで、証明書の作成についてのモバイルデバイスユーザーへの通知設定を定義します（SMS メッセージ、メール、またはウィザード終了時の情報の表示）。
6. ウィザードの［証明書情報］ウィンドウで、［**終了**］をクリックして、ウィザードを閉じます。

ウィザードの処理が完了すると、Google Play から Kaspersky Endpoint Security をダウンロードするためのリンクと QR コードがユーザーのモバイルデバイスに送信されます。ユーザーがリンクをクリックするか QR コードをスキャンして Google Play に移動します。デバイスのオペレーティングシステムが、Kaspersky Endpoint Security for Android のインストールの同意を要求します。Kaspersky Endpoint Security for Android がダウンロードされてインストールされると、モバイルデバイスが管理サーバーに接続して、共有証明書をダウンロードします。証明書がモバイルデバイスにインストールされると、そのモバイルデバイスが、コンソールツリーの［**モバイルデバイス**］フォルダーにある［**モバイルデバイス管理**］フォルダーに表示されます。

既に Kaspersky Endpoint Security for Android がデバイスにインストールされている場合、管理サーバーへの接続設定をユーザーが管理者から取得して入力する必要があります。接続設定が定義されると、モバイルデバイスが管理サーバーに接続されます。管理者が、そのデバイス用の共有証明書を発行し、証明書をダウンロードするためのログインとパスワードをユーザーにメールまたは SMS メッセージで送信します。ユーザーが共有証明書をダウンロードしインストールします。証明書がモバイルデバイスにインストールされると、そのモバイルデバイスが、コンソールツリーの［**モバイルデバイス**］フォルダーにある［**モバイルデバイス管理**］フォルダーに表示されます。この場合は、Kaspersky Endpoint Security for Android が再びダウンロードおよびインストールされることはありません。

KES デバイスの管理サーバーへの接続

KES デバイスに対する Kaspersky Device Management for iOS では、デバイスを管理サーバーに接続する方法に応じて、次の 2 つの導入スキームが可能です：

- デバイスを管理サーバーに直接接続する導入スキーム
- Kerberos の制約付き委任をサポートするリバースプロキシを含む導入スキーム

デバイスと管理サーバーの直接接続

KES デバイスは、管理サーバーのポート 13292 に直接接続できます。

KES デバイスと管理サーバーの接続では、使用する認証方法に応じて次の 2 つの選択肢が用意されています：

- ユーザー証明書を使用してデバイスを接続する
- ユーザー証明書を使用せずにデバイスを接続する

ユーザー証明書を使用してデバイスを接続する

ユーザー証明書を使用してデバイスを接続する場合、そのデバイスは、管理サーバーツールで該当の証明書が割り当てられているユーザーアカウントと関連付けられます。

この場合、双方向 SSL 認証（相互認証）が採用されます。管理サーバーとデバイスの双方が、証明書を使用して認証されます。

ユーザー証明書を使用せずにデバイスを接続する

ユーザー証明書を使用せずにデバイスを接続する場合、そのデバイスは、管理サーバーのいかなるユーザーアカウントとも関連付けられません。ただし、デバイスが証明書を受信すると、デバイスは、管理サーバーツールで該当の証明書が割り当てられているユーザーと関連付けられます。

そのデバイスを管理サーバーに接続する場合、片方向 SSL 認証が採用されるため、管理サーバーのみがその証明書を使用して認証されます。デバイスがユーザー証明書を取得した後、認証の種類は双方向 SSL 認証（双方向 SSL 認証、相互認証）に変更されます。

Kerberos の制約付き委任（KCD）を使用して KES デバイスをサーバーに接続するスキーム

Kerberos の制約付き委任（KCD）を使用して KES デバイスをサーバーに接続するスキームでは、以下を実現します：

- KCD をサポートするリバースプロキシとの統合
- Kerberos の制約付き委任（以下、「KCD」）を使用したモバイルデバイスの認証
- 公開鍵基盤（以下、「PKI」）との統合によるユーザー証明書の適用

この接続スキームを使用する場合は、以下に留意してください：

- KES デバイスのリバースプロキシへの接続タイプは「双方向 SSL 認証」でなければなりません。つまり、デバイスは専用のクライアント証明書（ユーザー証明書）を介してリバースプロキシに接続される必要があります。これを行うには、デバイスにインストールされている Kaspersky Endpoint Security for Android のインストールパッケージに、ユーザー証明書を統合する必要があります。この KES パッケージは、このデバイス（ユーザー）専用の管理サーバーによって作成される必要があります。
- 次のように、モバイルプロトコルの既定のサーバー証明書ではなく、専用（カスタマイズ済み）の証明書を指定する必要があります：

  1. 管理サーバーのプロパティウィンドウの［**管理サーバー接続設定**］セクションの［追加のポート］で、［**モバイルデバイス用ポートを開く**］をオンにし、ドロップダウンリストで［**証明書の追加**］を選択します。
  2. 表示されたウィンドウで、モバイルプロトコルへのアクセスポイントが管理サーバーで公開された際にリバースプロキシに設定されたものと同じ証明書を指定します。

- KES デバイスのユーザー証明書は、ドメインの Certificate Authority（CA）によって発行される必要があります。ドメインに複数のルート CA が含まれる場合、クライアント証明書（ユーザー証明書）は、リバースプロキシの公開に設定されている CA によって発行される必要があることに注意してください。

  以下の方法のいずれかを使用して、ユーザー証明書が、上述の要件を満たしていることを確認できます：

  - 新規パッケージウィザードと証明書インストールウィザードで、専用のユーザー証明書を指定します。
  - 管理サーバーとドメインの PKI を統合し、証明書発行ルールの該当する設定を定義します：

    1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを展開し、［**証明書**］サブフォルダーを選択します。
    2. ［**証明書**］フォルダーの作業領域で［**証明書の発行ルールを指定する**］をクリックし、［**証明書発行ルール**］を開きます。
    3. ［**PKI（公開鍵基盤）の統合**］セクションで、公開鍵基盤との統合を設定します。
    4. ［**モバイル証明書の発行**］セクションで、証明書のソースを指定します。

以下を前提とした Kerberos の制約付き委任（KCD）の設定例を次に示します：

- 管理サーバーのモバイルプロトコルへのアクセスポイントがポート 13292 に設定されている。
- リバースプロキシを備えたデバイスの名前は、firewall.mydom.local です。

- 管理サーバーがインストールされたデバイスの名前が ksc.mydom.local である。
- モバイルプロトコルへのアクセスポイントの外部公開名が kes4mob.mydom.global である。

管理サーバーのドメインアカウント

管理サーバーサービスが実行されるドメインアカウント（例：KSCMobileSrvcUsr）を作成する必要があります。管理サーバーサービスのアカウントは、管理サーバーのインストール時に、または klsrvswch ユーティリティを使用して指定できます。klsrvswch ユーティリティは、管理サーバーのインストールフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

ドメインアカウントを指定しなければならない理由は次の通りです：

- KES デバイスの管理機能は、管理サーバーにおいて不可欠であるため。
- Kerberos の制約付き委任（KCD）が適切に機能するには、受信側（すなわち管理サーバー）がドメインアカウントで実行される必要があるため。

http/kes4mob.mydom.local のサービスプリンシパル名

ドメインの KSCMobileSrvcUsr アカウントの下で、管理サーバーがインストールされたデバイスのポート 13292 にモバイルプロトコルサービスを発行する SPN を追加します。管理サーバーがインストールされた kes4mob.mydom.local デバイスでは、次のようになります：

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

リバースプロキシ（firewall.mydom.local）を持つデバイスのドメインプロパティを設定します

トラフィックを委任するには、SPN で定義されたサービス（http/kes4mob.mydom.local:13292）に対してリバースプロキシ（firewall.mydom.local）を備えたデバイスを信頼する必要があります。

SPN で定義されたサービス（http/kes4mob.mydom.local:13292）に対してリバースプロキシを備えたデバイスに信頼するには、管理者は以下の操作を実行する必要があります：

1. 「Active Directory Users and Computers」という名前の Microsoft 管理コンソールスナップインで、リバースプロキシがインストールされているデバイス（firewall.mydom.local）を選択します。
2. デバイスのプロパティの［**委任**］タブで、［**このコンピューターを、指定されたサービスの委任に限って信頼する**］トグルを［**任意の認証プロトコルを使用する**］に設定します。
3. ［**このアカウントが委任された資格情報を提供できるサービス**］リストに、SPN（http/kes4mob.mydom.local:13292）を追加します。

公開専用（カスタマイズ済み）の証明書（kes4mob.mydom.global）

管理サーバーのモバイルプロトコルを公開するには、FQDN kes4mob.mydom.global 専用（カスタマイズ済み）の証明書を発行し、管理コンソールにおいて、管理サーバーのモバイルプロトコル設定で、この証明書を既定のサーバー証明書の代わりに指定する必要があります。これを行うには、管理サーバーのプロパティウィンドウの［**管理サーバー接続設定**］セクションの［追加のポート］で、［**モバイルデバイス用ポートを開く**］をオンにし、次にドロップダウンリストで［**証明書の追加**］を選択します。

サーバー証明書のコンテナー（拡張子が p12 または pfx のファイル）には、ルート証明書（公開鍵）のチェーンも含まれる必要があることに留意してください。

リバースプロキシでの公開の設定

リバースプロキシ上で、モバイルデバイス側から kes4mob.mydom.global の 13292 番ポートに向かうトラフィックについては、FQND の kes4mob.mydom.global に対して発行されたサーバー証明書を使用して、SPN（http/kes4mob.mydom.local:13292）に KCD を設定する必要があります。公開中、および公開済みのアクセスポイント（管理サーバーのポート 13292）は、同じサーバー証明書を共有する必要があることに留意してください。

Firebase Cloud Messaging の使用

Android オペレーティングシステムが管理する KES デバイスにコマンドがタイミングよく確実に配信されるようにするため、Kaspersky Security Center ではプッシュ通知のメカニズムが使用されます。プッシュ通知は、Firebase Cloud Messaging（以下、FCM）を介して KES デバイスと管理サーバー間で交換されます。Kaspersky Security Center 管理コンソールで、Firebase Cloud Messaging サービスの設定を指定することで、サービスに KES デバイスを接続できます。

Firebase Cloud Messaging の設定を取得するには、Google アカウントが必要です。

FCM の使用を有効化するには：

1. 管理コンソールで、［**モバイルデバイス管理**］フォルダー、および［**モバイルデバイス**］フォルダーを選択します。
2. ［**モバイルデバイス**］フォルダーのコンテキストメニューで、［**プロパティ**］を選択します。
3. フォルダーのプロパティで、［**Firebase Cloud Messaging の設定**］セクションを選択します。
4. ［**Firebase プロジェクト番号**］フィールドに、FCM 送信者 ID を指定します。
5. ［**秘密鍵ファイル（JSON 形式）**］フィールドで、秘密鍵ファイルを選択します。

   管理サーバーとの次回の同期時に、Android オペレーティングシステムが管理する KES デバイスが、Firebase Cloud Messaging に接続されます。

Firebase Cloud Messaging の設定は、［**設定をリセット**］をクリックして編集できます。

別の Firebase プロジェクトに切り替える場合は、FCM が再開されるまで 10 分間待つ必要があります。

FCM サービスは、以下のアドレス範囲で実行されます：

- KES デバイス側では、以下のアドレスのポート 443（HTTPS）、5228（HTTPS）、5229（HTTPS）、および 5230（HTTPS）に対するアクセスが必要です：
  - google.com
  - fcm.googleapis.com

- android.apis.google.com
- Google の ASN 15169 に一覧表示されたすべての IP アドレス

- 管理サーバー側では、以下のアドレスのポート 443（HTTPS）に対するアクセスが必要です：
  - fcm.googleapis.com
  - Google の ASN 15169 に一覧表示されたすべての IP アドレス

管理コンソールの管理サーバーのプロパティで、プロキシサーバー設定（［**詳細**］→［**インターネットアクセスの設定**］）が指定されている場合、その設定が FCM とのやり取りに使用されます。

FCM の設定：送信者 ID と秘密鍵ファイルの取得

FCM を設定するには：

1. Google ポータル で登録します。
2. Firebase コンソール へ移動します。
3. 次のいずれかの手順を実行します：
   - 新しいプロジェクトを作成するには、［**プロジェクトの作成**］をクリックし、画面の指示に従います。
   - 既存のプロジェクトを開きます。
4. 歯車アイコンをクリックし、［**プロジェクト設定**］を選択します。
   ［**プロジェクト設定**］ウィンドウが開きます。
5. ［**クラウドメッセージング**］タブを選択します。
6. ［**Firebase Cloud Messaging API (V1)**］セクションの［**送信者 ID**］フィールドから関連する送信者 ID を取得します。
7. ［**サービスアカウント**］タブを選択し、［**新しい秘密鍵の生成**］をクリックします。
8. 開いたウィンドウで、［**鍵の生成**］をクリックして秘密鍵ファイルを生成し、ダウンロードします。

Firebase Cloud Messaging が設定されました。

公開鍵基盤との統合

公開鍵基盤（以下、「PKI」）との統合は、管理サーバーによるドメインユーザー証明書の発行を簡略化することが主な目的です。

管理者は、管理コンソールでユーザーのドメイン証明書を割り当てることができます。この作業は、以下の方法のいずれかを使用して行うことができます：

- 証明書インストールウィザードで、ファイルから専用（カスタマイズ済み）の証明書を割り当てます。
- PKI との統合を実施し、PKI が、特定の種別の証明書、またはすべての種別の証明書のソースとして機能するようにします。

PKI との統合は、［**モバイルデバイス管理**］ - ［**証明書**］フォルダーの作業領域で、［**公開鍵基盤と統合する**］をクリックして設定できます。

ドメインユーザー証明書の発行における PKI との統合の一般原則

管理コンソールで、［**モバイルデバイス管理**］ - ［**証明書**］フォルダーの作業領域の［**公開鍵基盤と統合する**］をクリックし、管理サーバーがドメインの CA（以下、「PKI との統合が実施されるアカウント」）経由でドメインユーザー証明書を発行するために使用するドメインアカウントを指定します。

以下に留意してください：

- PKI との統合の設定では、すべての種別の証明書に対して既定のテンプレートを指定できます。証明書の発行ルール（［**モバイルデバイス管理**］ - ［**証明書**］フォルダーの作業領域で、［**証明書の発行ルールを指定する**］をクリック）では、すべての種別の証明書に対して個別のテンプレートを指定できることに留意してください。

- PKI との統合が実施されるアカウントの証明書リポジトリで、専用の Enrollment Agent（EA）証明書が、管理サーバーがインストールされたデバイスにインストールされる必要があります。Enrollment Agent（EA）証明書は、ドメインの CA（Certificate Authority）の管理者によって発行されます。

PKI との統合が実施されるアカウントは、以下の基準を満たす必要があります：

- ドメインユーザーである。

- PKI との統合を開始した管理サーバーがインストールされたデバイスのローカル管理者である。

- *サービスとしてログオン*する権限がある。

- 管理サーバーがインストールされたデバイスは、永続的なユーザープロファイルを作成するために、少なくとも 1 度はこのアカウントで実行される必要がある。

Kaspersky Security Center Web サーバー

Kaspersky Security Center Web サーバー（「Web サーバー」とも表記）は、Kaspersky Security Center のコンポーネントです。Web サーバーは、スタンドアロンインストールパッケージ、モバイルデバイス用スタンドアロンインストールパッケージ、iOS MDM プロファイル、および共有フォルダーのファイルを公開することを目的に設計されています。

作成された iOS MDM プロファイルとインストールパッケージは、Web サーバーで自動的に公開され、初回のダウンロード後に削除されます。管理者は、メールなど便利な方法を利用して、ユーザーに新しいリンクを送信します。

ユーザーはそのリンクをクリックして、必要な情報をモバイルデバイスにダウンロードできます。

Web サーバーの設定

Web サーバーの微調整が必要な場合は、管理コンソール Web サーバーのプロパティで、HTTP（8060）および HTTPS（8061）のポートを変更できます。ポートの変更に加えて、HTTPS のサーバー証明書を置き換えることや、HTTP の Web サーバーの FQDN を変更することが可能です。

Kaspersky Security Center のインストール

このセクションでは、Kaspersky Security Center のインストールについて説明します。本製品を 1 つのデバイスにのみローカルでインストールする場合は、2 つのインストールオプションを使用できます：

- **標準**：企業ネットワーク内の小規模エリアで動作をテストするなど、Kaspersky Security Center を試したい場合は、このオプションを推奨します。標準インストール中は、データベースのみを設定します。また、カスペルスキー製品の既定の管理プラグインセットのみをさらにインストールできます。Kaspersky Security Center の使用経験があり、標準インストール後にすべての設定を適切に指定する方法を把握している場合は、標準インストールを使用することもできます。

- **カスタム**：共有フォルダーのパス、管理サーバーへの接続用アカウントおよびポート、データベース設定などの Kaspersky Security Center の設定を編集する場合は、このオプションを推奨します。カスタムインストールでは、インストールするカスペルスキー製品の管理プラグインの指定ができます。必要に応じて、サイレントモードでカスタムインストールを開始できます。

ネットワーク内に管理サーバーが 1 つでもインストールされていれば、強制インストールを使用したリモートインストールタスクによって、他のデバイスにサーバーをリモートインストールできます。リモートインストールタスクを作成する際、管理サーバーのインストールパッケージを使用する必要があります：ksc_<バージョン番号>.<ビルド番号>_full_<ローカリゼーション言語>.exe。

このパッケージを使用して、Kaspersky Security Center のフル機能のために必要なすべてのコンポーネントをインストールするか、現在のバージョンのこれらのコンポーネントをアップグレードすることができます。

Kaspersky Security Center のフェールオーバークラスターを導入する場合は、クラスターのすべてのノードに Kaspersky Security Center をインストールする必要があります。

インストールの準備

インストールを開始する前に、次のアクションを実行します。

- **ハードウェアとソフトウェアの要件を確認する**

  デバイスのハードウェアおよびソフトウェアが「管理サーバーと管理コンソールの要件」を満たしていることを確認してください。

- **データベース管理システム（DBMS）を選択してインストールする**

  Kaspersky Security Center は、その情報を DBMS によって管理されるデータベースに保存します。Kaspersky Security Center の前に DBMS をネットワークにインストールします（DBMS の選択方法の詳細を参照してください）。PostgreSQL または Postgres Pro DBMS をインストールする場合は、スーパーユーザーのパスワードを指定してください。パスワードが指定されていない場合、管理サーバーがデータベースに接続できない可能性があります。

  管理サーバーは、ドメインコントローラーではなく専用サーバーにインストールすることを推奨します。ただし、読み取り専用ドメインコントローラー（RODC）として動作するサーバーに Kaspersky Security Center をインストールする場合は、Microsoft SQL Server（SQL Express）をローカル（同じデバイス）にインストールしないでください。この場合、Microsoft SQL Server（SQL Express）と Kaspersky Security Center とは別のデバイスにインストールするか、Kaspersky Security Center と同じデバイスに DBMS をインストールする必要がある場合には MySQL、MariaDB、または PostgreSQL を使用することを推奨します。

- **管理サーバー、ネットワークエージェント、管理コンソール用のフォルダを準備する**

管理サーバー、ネットワークエージェント、管理コンソールは、大文字と小文字の区別が無効になっているフォルダーにインストールする必要があります。また、管理サーバーの共有フォルダーおよびKaspersky Security Centerの非表示フォルダー（%ALLUSERSPROFILE%\KasperskyLab\adminkit）でも、大文字と小文字の区別は無効にしておく必要があります。

- **古いネットワークエージェントを削除する**

  サーバー向けネットワークエージェントが、管理サーバーとともにデバイスにインストールされます。標準バージョンのネットワークエージェントは、管理サーバーと共存できません。サーバー向けネットワークエージェントが既にインストールされている場合は、そのエージェントを削除してから管理サーバーのインストールを開始します。ネットワークエージェントのサーバーバージョンの詳細は、「Kaspersky Security Center インストール後のシステムの変更」を参照してください。

- **アカウントの確認**

  Kaspersky Security Centerのインストールには、インストールを実行するデバイスでの管理者権限が必要となります。

  Kaspersky Security Centerは、管理対象サービスアカウントとグループ管理対象サービスアカウントをサポートしています。これらのタイプのアカウントがドメインで使用されており、そのうちの1つを管理サーバーサービスのアカウントとして指定する場合は、最初に管理サーバーをインストールするのと同じデバイスにアカウントをインストールします。ローカルデバイスへの管理対象サービスアカウントのインストールの詳細は、Microsoft公式ドキュメントを参照してください。

DBMSに使用するアカウント

管理サーバーをインストールして使用するには、管理サーバーのインストーラー（以降、インストーラーとも表記）を実行するWindowsアカウント、管理サーバーサービスを開始するWindowsアカウント、およびDBMSにアクセスするための内部DBMSアカウントが必要です。新しいアカウントを作成するか、既存のアカウントを使用できます。これらすべてのアカウントには、特定の権利が必要です。必要なアカウントとその権限のセットは、次の基準に応じて異なります：

- DBMSタイプ：
  - （Windows認証またはSQL Server認証を備えた）Microsoft SQL Server
  - MySQLまたはMariaDB
  - PostgreSQLまたはPostgres Pro
- DBMSの場所：
  - **ローカルDBMS**：*ローカルDBMS*とは、管理サーバーと同じデバイスにインストールされているDBMSを意味します。
  - **リモートDBMS**：*リモートDBMS*は、別のデバイスにインストールされたDBMSです。
- 管理サーバーデータベースの作成方法：
  - **自動**管理サーバーのインストール中に、インストーラーを使用して、管理サーバーデータベース（以降、サーバーデータベースと表記）を自動的に作成できます。
  - **手動**サードパーティ製品（SQL Server Management Studioなど）またはスクリプトを使用して、空のデータベースを作成できます。その後、管理サーバーのインストール時に、このデータベースをサーバーデータベースとして指定できます。

アカウントに権限とアクセス許可を付与するときは、最小特権の原則に従います。つまり、付与する権限は、必要なアクションを実行するのに必要最低限にすべきです。

以下の表は、管理サーバーをインストールして起動する前にアカウントに付与する必要があるシステム権限とDBMS権限に関する情報を示しています。

Windows認証を使用するMicrosoft SQL Server

DBMSとしてSQL Serverを選択すると、Windows認証を使用してSQL Serverにアクセスできます。インストーラーの実行に使用するWindowsアカウントと、管理サーバーサービスの開始に使用するWindowsアカウントのシステム権限を設定します。SQL Serverで、これら両方のWindowsアカウントのログインを作成します。サーバーデータベースの作成方法に応じて、次の表の説明に従って必要なSQL Server権限をこれらのアカウントに付与します。アカウントの権限を設定する方法の詳細は、「PostgreSQLおよびPostgres Proを使用するためのアカウントの設定」を参照してください。

DBMS：Windows認証を備えたMicrosoft SQL Server（Express Editionを含む）

	自動データベース作成（インストーラーによる）	手動データベース作成（管理者による）
インストーラーを実行しているアカウント	• リモートDBMS：DBMSがインストールされているリモートデバイスのドメインアカウントのみ。 • ローカルDBMS：ローカル管理者アカウントまたはドメインアカウント。	• リモートDBMS：DBMSがインストールされているリモートデバイスのドメインアカウントのみ。 • ローカルDBMS：ローカル管理者アカウントまたはドメインアカウント。
インストーラーを実行しているアカウントの権限	• システム権限：ローカル管理者権限 • SQL Serverの権限： • サーバーレベルロール：sysadmin	• システム権限：ローカル管理者権限 • SQL Serverの権限： • サーバーレベルでのロール：public • サーバーデータベースのデータベースロールメンバーシップ：db_owner、public • サーバーデータベースの既定スキーマ：dbo
管理サーバーのサービスアカウント	• リモートDBMS：DBMSがインストールされているリモートデバイスのドメインアカウントのみ。 • ローカルDBMS： • 管理者が選択したWindowsアカウント • インストーラーが自動的に作成するKL-AK-*形式のアカウント	• リモートDBMS：DBMSがインストールされているリモートデバイスのドメインアカウントのみ。 • ローカルDBMS： • 管理者が選択したWindowsアカウント • インストーラーが自動的に作成するKL-AK-*形式のアカウント（この場合、KL-AK-*アカウントの自動生成は推奨しません）
管理サーバーのサービスアカウント権限	• システム権限：必要な権限がインストーラーによって付与されます • SQL Server権限：必要な権限がインストーラーによって付与されます	• システム権限：必要な権限がインストーラーによって付与されます • SQL Serverの権限： • サーバーレベルでのロール：public • サーバーデータベースのデータベースロールメンバーシップ：db_owner、public • サーバーデータベースの既定スキーマ：dbo

SQL Server認証を使用するMicrosoft SQL Server

DBMS として SQL Server を選択すると、SQL Server 認証を使用して SQL Server にアクセスできます。インストーラーの実行に使用する Windows アカウントと、管理サーバーサービスの開始に使用する Windows アカウントのシステム権限を設定します。SQL Server で、パスワードを使用してログインを作成し、認証に使用します。次に、この SQL Server アカウントに、次の表に示す必要な権限を付与します。アカウントの権限を設定する方法の詳細は、「SQL Server を使用するためのアカウントの設定（SQL Server 認証）」を参照してください。

DBMS：SQL Server 認証を備えた Microsoft SQL Server（Express Edition を含む）

	自動データベース作成（インストーラーによる）	手動データベース作成（管理者による）
インストーラーを実行しているアカウント	• リモート DBMS：DBMS がインストールされているリモートデバイスのドメインアカウントのみ。 • ローカル DBMS：ローカル管理者アカウントまたはドメインアカウント。	• リモート DBMS：DBMS がインストールされているリモートデバイスのドメインアカウントのみ。 • ローカル DBMS：ローカル管理者アカウントまたはドメインアカウント。
インストーラーを実行しているアカウントの権限	システム権限：ローカル管理者権限	システム権限：ローカル管理者権限
管理サーバーのサービスアカウント	• リモート DBMS：DBMS がインストールされているリモートデバイスのドメインアカウントのみ。 • ローカル DBMS： • 管理者が選択した Windows アカウント • インストーラーが自動的に作成する KL-AK-* 形式のアカウント	• リモート DBMS：DBMS がインストールされているリモートデバイスのドメインアカウントのみ。 • ローカル DBMS： • 管理者が選択した Windows ユーザーアカウント • インストーラーが自動的に作成する KL-AK-* 形式のアカウント
管理サーバーのサービスアカウント権限	システム権限：必要な権限がインストーラーによって付与されます	システム権限：必要な権限がインストーラーによって付与されます
SQL Server 認証に使用されるログインの権限	データベースの作成と管理サーバーのインストールに必要な SQL Server 権限： • サーバーレベルでのロール：public • マスターデータベースのデータベースロールメンバーシップ：db_owner • マスターデータベースの既定スキーマ：dbo • アクセス権限： • CONNECT ANY DATABASE • CONNECT SQL • CREATE ANY DATABASE • VIEW ANY DATABASE • VIEW SERVER STATE（**Always On** オプションが有効な場合） 管理サーバーを使用するために必要な SQL Server 権限： • サーバーレベルでのロール：public • サーバーデータベースのデータベースロールメンバーシップ：db_owner • サーバーデータベースの既定スキーマ：dbo • アクセス権限： • CONNECT SQL • VIEW ANY DATABASE	SQL Server の権限： • サーバーレベルでのロール：public • サーバーデータベースのデータベースロールメンバーシップ：db_owner • サーバーデータベースの既定スキーマ：dbo • アクセス権限： • CONNECT SQL • VIEW ANY DATABASE • VIEW ANY DEFINITION

	• VIEW SERVER STATE（**Always On** オプションが有効な場合） • VIEW ANY DEFINITION	

管理サーバーのデータ復旧のための SQL Server 権限の設定

バックアップから管理サーバーデータを復元するには、管理サーバーのインストールに使用した Windows アカウントで klbackup ユーティリティを実行します。SQL Server で klbackup ユーティリティを起動する前に、この Windows アカウントに関連付けられた SQL Server ログインに権限を付与します。SQL Server の権限は、管理サーバーのバージョンによって異なります。バージョン 14.2 以降の管理サーバーの場合、sysadmin サーバーレベルロールまたは dbcreator サーバーレベルロールを付与できます。

管理サーバーデータベースの回復のための SQL Server 権限

バージョン 14.2 以降の管理サーバー	管理サーバーのその他のバージョン
• SQL Server の権限： • サーバーレベルロール：sysadmin	• SQL Server の権限： • サーバーレベルロール：sysadmin
• SQL Server の権限： • サーバーレベルロール：dbcreator • アクセス権限： • VIEW ANY DEFINITION klbackup ユーティリティを起動する前に、KLSRV_SKIP_ADJUSTING_DBMS_ACCESS サーバーフラグを指定します。Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。その後、コマンドラインで次のコマンドを実行します： `klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1`	

MySQL および MariaDB

DBMS として MySQL または MariaDB を選択した場合は、DBMS 内部アカウントを作成し、次の表に示す必要な権限をこのアカウントに付与します。インストーラーと管理サーバーサービスは、この内部 DBMS アカウントを使用して DBMS にアクセスします。データベースの作成方法によって、必要な権限のセットに影響はありません。アカウント権限を設定する方法の詳細は、「MySQL および MariaDB を使用するためのアカウントの設定」を参照してください。

DBMS：MySQL および MariaDB

	自動または手動のデータベース作成
インストーラーを実行しているアカウント	• リモート DBMS：DBMS がインストールされているリモートデバイスのドメインアカウントのみ。 • ローカル DBMS：ローカル管理者アカウントまたはドメインアカウント。
インストーラーを実行しているアカウントの権限	システム権限：ローカル管理者権限
管理サーバーのサービスアカウント	• リモート DBMS：DBMS がインストールされているリモートデバイスのドメインアカウントのみ。 • ローカル DBMS：

	• 管理者が選択した Windows アカウント • インストーラーが自動的に作成する KL-AK-* 形式のアカウント
管理サーバーのサービスアカウント権限	システム権限：必要な権限がインストーラーによって付与されます
DBMS 内部アカウントの権限	スキーマ権限： • 管理サーバーデータベース：ALL（GRANT OPTION を除く）。 • システムスキーム（mysql および sys）：SELECT、SHOW VIEW。 • sys.table_exists ストアドプロシージャ：EXECUTE（MariaDB 10.5 以前を DBMS として使用する場合、EXECUTE 権限を付与する必要はありません）。 すべてのスキームに対するグローバル権限：PROCESS、SUPER。

管理サーバーのデータ復旧のための権限の設定

内部 DBMS アカウントに付与した権限は、管理サーバーのデータをバックアップから復元するのに十分です。復元を開始するには、管理サーバーのインストールに使用した Windows アカウントで klbackup ユーティリティを実行します。

PostgreSQL または Postgres Pro

PostgreSQL または Postgres Pro を DBMS として選択した場合、ユーザー *Postgres*（Postgres の既定のロール）を使用するか、新しい Postgres ロール（以降、ロールとも表記）を作成して DBMS にアクセスできます。サーバーデータベースの作成方法に応じて、次の表の説明に従って必要な権限をロールに付与します。ロールの権限を設定する方法の詳細は、「PostgreSQL および Postgres Pro を使用するためのアカウントの設定」を参照してください。

DBMS：PostgreSQL または Postgres Pro

	自動のデータベース作成		手動のデータベース作成
インストーラーを実行しているアカウント	• リモート DBMS：DBMS がインストールされているリモートデバイスのドメインアカウントのみ。 • ローカル DBMS：ローカル管理者アカウントまたはドメインアカウント。		• リモート DBMS：DBMS がインストールされているリモートデバイスのドメインアカウントのみ。 • ローカル DBMS：ローカル管理者アカウントまたはドメインアカウント。
インストーラーを実行しているアカウントの権限	システム権限：ローカル管理者権限		システム権限：ローカル管理者権限
管理サーバーのサービスアカウント	• リモート DBMS：DBMS がインストールされているリモートデバイスのドメインアカウントのみ。 • ローカル DBMS： • 管理者が選択した Windows アカウント • インストーラーが自動的に作成する KL-AK-* 形式のアカウント		• リモート DBMS：DBMS がインストールされているリモートデバイスのドメインアカウントのみ。 • ローカル DBMS： • 管理者が選択した Windows アカウント • インストーラーが自動的に作成する KL-AK-* 形式のアカウント
管理サーバーのサービスアカウント権限	システム権限：必要な権限がインストーラーによって付与されます		システム権限：必要な権限がインストーラーによって付与されます
Postgres ロールの権限	ユーザー *Postgres* には、追加の権限は必要ありません。	新しいロールの権限：`CREATEDB`。	新しいロールの場合： • 管理サーバーデータベースに対する権限：`ALL`。 • パブリックスキーマ内のすべてのテーブルに対する権限：`ALL`。

		• パブリックスキーマ内のすべてのシーケンスに対する権限：ALL。

管理サーバーのデータ復旧のための権限の設定

バックアップから管理サーバーデータを復元するには、管理サーバーのインストールに使用した Windows アカウントで klbackup ユーティリティを実行します。DBMS へのアクセスに使用される Postgres ロールには、管理サーバーデータベースに対する所有者権限が必要です。

SQL Server を使用するためのアカウントの設定（Windows 認証）

必須条件

アカウントに権限を割り当てる前に、次のアクションを実行します：

1. ローカル管理者アカウントでシステムにログインしていることを確認します。
2. SQL Server を使用するための環境をインストールします。
3. 管理サーバーのインストールに使用する Windows アカウントがあることを確認します。
4. 管理サーバーサービスの開始に使用する Windows アカウントがあることを確認します。
5. SQL Server で、管理サーバーインストーラー（以降、インストーラーとも表記）の実行に使用される Windows アカウントのログインを作成します。また、管理サーバーサービスの開始に使用する Windows アカウントのログイン情報を作成します。

SQL Server Management Studio を使用する場合、ログインプロパティウィンドウの［**全般**］ページで、［**Windows 認証**］をオンにします。

別の Windows ドメインにあるデバイスに管理サーバーと SQL Server をインストールする場合は、タスクの実行やポリシーの適用など、管理サーバーが正しく動作するように、これらのドメインに双方向の信頼関係が必要であることに注意してください。さまざまな DBMS を操作するために必要なアカウントとアカウントの権限については、「DBMS に使用するアカウント」を参照してください。

管理サーバーをインストールするためのアカウントの設定（管理サーバーデータベースの自動作成）

管理サーバーのインストール用にアカウントを設定するには：

1. SQL Server で、sysadmin サーバーレベルロールを、インストーラーの実行に使用した Windows アカウントのログインに割り当てます。
2. インストーラーの実行に使用した Windows アカウントでシステムにログインします。
3. 管理サーバーのインストーラーを実行します。
   管理サーバーのセットアップウィザードが起動します。ウィザードの指示に従ってください。

4. ［管理サーバーのカスタムインストール］を選択します。

5. 管理サーバーデータベースを格納する DBMS として Microsoft SQL Server を選択します。

6. Windows アカウントを介して管理サーバーと SQL Server との間の接続を確立するには、Microsoft Windows 認証モードを選択します。

7. 管理サーバーサービスを開始する Windows アカウントを指定します。

   以前に SQL Server ログイン情報を作成した Windows ユーザーアカウントを選択できます。または、インストーラーを使用して、KL-AK-* 形式で新しい Windows アカウントを自動的に作成することもできます。この場合、インストーラーはこのアカウント用の SQL Server ログインを自動的に作成します。アカウントの選択にかかわらず、インストーラーは必要なシステム権限と SQL Server 権限を管理サーバーサービスアカウントに割り当てます。

インストールが完了すると、サーバーデータベースが作成され、必要なすべてのシステム権限と SQL Server 権限が管理サーバーサービスアカウントに割り当てられます。管理サーバーが使用できるようになります。

管理サーバーをインストールするためのアカウントの設定（管理サーバーデータベースの手動作成）

管理サーバーのインストール用にアカウントを設定するには：

1. SQL Server で、空のデータベースを作成します。このデータベースは、管理サーバーデータベース（以降、サーバーデータベースとも表記）として使用されます。

2. Windows アカウント用に作成された両方の SQL Server ログイン情報にパブリックサーバーレベルロールを指定し、作成されたデータベースへのマッピングを設定します：

   - サーバーレベルでのロール：public
   - データベースロールメンバーシップ：db_owner、public
   - 既定のスキーマ：dbo

3. インストーラーの実行に使用した Windows アカウントでシステムにログインします。

4. 管理サーバーのインストーラーを実行します。

   管理サーバーのセットアップウィザードが起動します。ウィザードの指示に従ってください。

5. ［管理サーバーのカスタムインストール］を選択します。

6. 管理サーバーデータベースを格納する DBMS として Microsoft SQL Server を選択します。

7. 作成したデータベースの名前を管理サーバーのデータベース名として指定します。

8. Windows アカウントを介して管理サーバーと SQL Server との間の接続を確立するには、Microsoft Windows 認証モードを選択します。

9. 管理サーバーサービスを開始する Windows アカウントを指定します。

   以前に SQL Server ログイン情報を作成してログイン権限を設定した Windows ユーザーアカウントを選択できます。

新しい Windows アカウントを KL-AK-* 形式で自動的に作成することは推奨しません。この場合、インストーラーにより、SQL Server アカウントを作成して設定していない新しい Windows アカウントが作成されます。管理サーバーがこのアカウントを使用して管理サーバーサービスを開始することはできません。KL-AK-* 形式の Windows アカウントを作成する必要がある場合は、インストール後に管理コンソールを起動しないでください。代わりに、次の手順に従います：

1. kladminserver サービスを停止します。
2. SQL Server で、作成した KL-AK-* 形式の Windows アカウント用に SQL Server ログインを作成します。
3. この SQL Server ログインに権限を付与し、作成されたデータベースへのマッピングを設定します：
   - サーバーレベルでのロール：public
   - データベースロールメンバーシップ：db_owner、public
   - 既定のスキーマ：dbo
4. kladminserver サービスを再起動してから、管理コンソールを実行します。

インストールが完了すると、管理サーバーは作成されたデータベースをサーバーデータの保存に使用するようになります。管理サーバーが使用できるようになります。

SQL Server を使用するためのアカウントの設定（SQL Server 認証）

必須条件

アカウントに権限を割り当てる前に、次のアクションを実行します：

1. ローカル管理者アカウントでシステムにログインしていることを確認します。
2. SQL Server を使用するための環境をインストールします。
3. 管理サーバーのインストールに使用する Windows アカウントがあることを確認します。
4. 管理サーバーサービスの開始に使用する Windows アカウントがあることを確認します。
5. SQL Server で、SQL Server 認証モードを有効にします。

   SQL Server Management Studio を使用する場合、SQL Server のプロパティウィンドウの［**セキュリティ**］ページで、［**SQL Server 認証モードと Windows 認証モード**］をオンにします。
6. SQL Server で、パスワードを使用してログインを作成します。管理サーバーインストーラー（以降、インストーラーとも表記）と管理サーバーサービスは、この SQL Server アカウントを使用して SQL Server にアクセスします。

   SQL Server Management Studio を使用する場合、ログインプロパティウィンドウの［**全般**］ページで、［**SQL Server 認証**］をオンにします。

別の Windows ドメインにあるデバイスに管理サーバーと SQL Server をインストールする場合は、タスクの実行やポリシーの適用など、管理サーバーが正しく動作するように、これらのドメインに双方向の信頼関係が必要であることに注意してください。さまざまな DBMS を操作するために必要なアカウントとアカウントの権限については、「DBMS に使用するアカウント」を参照してください。

管理サーバーをインストールするためのアカウントの設定（管理サーバーデータベースの自動作成）

管理サーバーのインストール用にアカウントを設定するには：

1. SQL Server で、SQL Server アカウントを既定の *マスター*データベースにマッピングします。 *マスター*データベースは、管理サーバーデータベース（以降、サーバーデータベースとも表記）のテンプレートです。 *マスター*データベースは、インストーラーがサーバーデータベースを作成するまで、マッピングに使用されます。次の権限とアクセス許可を SQL Server アカウントに付与します：
   - サーバーレベルでのロール：public
   - *マスター*データベースのデータベースロールメンバーシップ：db_owner
   - *マスター*データベースの既定スキーマ：dbo
   - アクセス権限：
     - CONNECT ANY DATABASE
     - CONNECT SQL
     - CREATE ANY DATABASE
     - VIEW ANY DATABASE
2. インストーラーの実行に使用した Windows アカウントでシステムにログインします。
3. インストーラーを実行します。
   管理サーバーのセットアップウィザードが起動します。ウィザードの指示に従ってください。
4. ［管理サーバーのカスタムインストール］を選択します。
5. 管理サーバーデータベースを格納する DBMS として Microsoft SQL Server を選択します。
6. 管理サーバーデータベース名を指定します。
7. 作成された SQL Server アカウントを介して管理サーバーと SQL Server との間の接続を確立するには、SQL Server 認証モードを選択します。次に、SQL Server アカウントの資格情報を指定します。
8. 管理サーバーサービスを開始する Windows アカウントを指定します。
   インストーラーを使用して、既存の Windows ユーザーアカウントを選択するか、KL-AK-* 形式で新しい Windows アカウントを作成することができます。アカウントの選択にかかわらず、インストーラーは必要なシステム権限を管理サーバーサービスアカウントに割り当てます。

インストールが完了すると、サーバーデータベースが作成され、必要なすべてのシステム権限が管理サーバーサービスアカウントに割り当てられます。管理サーバーが使用できるようになります。

インストーラーが管理サーバーのインストール中にサーバーデータベースを作成し、このデータベースへのマッピングを設定したため、 *マスター*データベースへのマッピングをキャンセルできます。

データベースの自動作成には、管理サーバーでの通常の作業よりも多くの権限が必要になるため、一部の権限を取り消すことができます。SQL Server で、SQL Server アカウントを選択し、管理サーバーを使用するために次の権限を付与します：

- サーバーレベルでのロール：public
- サーバーデータベースのデータベースロールメンバーシップ：db_owner
- サーバーデータベースの既定スキーマ：dbo
- アクセス権限：
  - CONNECT SQL
  - VIEW ANY DATABASE

管理サーバーをインストールするためのアカウントの設定（管理サーバーデータベースの手動作成）

管理サーバーのインストール用にアカウントを設定するには：

1. SQL Server で、空のデータベースを作成します。このデータベースは、管理サーバーデータベースとして使用されます。
2. SQL Server で、次の権限とアクセス許可を SQL Server アカウントに付与します：
   - サーバーレベルでのロール：public
   - 作成されたデータベースのデータベースロールメンバーシップ：db_owner
   - 作成されたデータベースの既定スキーマ：dbo
   - アクセス権限：
     - CONNECT SQL
     - VIEW ANY DATABASE
3. インストーラーの実行に使用した Windows アカウントでシステムにログインします。
4. インストーラーを実行します。
   管理サーバーのセットアップウィザードが起動します。ウィザードの指示に従ってください。
5. ［管理サーバーのカスタムインストール］を選択します。
6. 管理サーバーデータベースを格納する DBMS として Microsoft SQL Server を選択します。
7. 作成したデータベースの名前を管理サーバーのデータベース名として指定します。
8. 作成された SQL Server アカウントを介して管理サーバーと SQL Server との間の接続を確立するには、SQL Server 認証モードを選択します。次に、SQL Server アカウントの資格情報を指定します。
9. 管理サーバーサービスを開始する Windows アカウントを指定します。
   インストーラーを使用して、既存の Windows ユーザーアカウントを選択するか、KL-AK-* 形式で新しい Windows アカウントを作成することができます。アカウントの選択にかかわらず、インストーラーは必要なシステム権限を管理サーバーサービスアカウントに割り当てます。

インストールが完了すると、管理サーバーは作成されたデータベースを管理サーバーデータの保存に使用するようになります。必要なすべてのシステム権限が管理サーバーサービスアカウントに割り当てられます。管理サーバーが使用できるようになります。

MySQL および MariaDB を使用するためのアカウントの設定

必須条件

アカウントに権限を割り当てる前に、次のアクションを実行します：

1. ローカル管理者アカウントでシステムにログインしていることを確認します。
2. MySQL または MariaDB を使用するための環境をインストールします。
3. 管理サーバーのインストールに使用する Windows アカウントがあることを確認します。
4. 管理サーバーサービスの開始に使用する Windows アカウントがあることを確認します。

管理サーバーをインストールするためのアカウントの設定

管理サーバーのインストール用にアカウントを設定するには：

1. DBMS のインストール時に作成した root アカウントで、MySQL または MariaDB を使用するための環境を実行します。
2. パスワード付きの内部 DBMS アカウントを作成します。管理サーバーインストーラー（以降、インストーラーとも表記）と管理サーバーサービスは、この内部 DBMS アカウントを使用して DBMS にアクセスします。このアカウントに次の権限を付与します：
   - スキーマ権限：
     - 管理サーバーデータベース：ALL（`GRANT OPTION` を除く）
     - システムスキーム（mysql および sys）：`SELECT`、`SHOW VIEW`
     - sys.table_exists ストアドプロシージャ：`EXECUTE`
   - すべてのスキームに対するグローバル権限：`PROCESS`、`SUPER`

   内部 DBMS アカウントを作成し、このアカウントに必要な権限を付与するには、次のスクリプトを実行します（このスクリプトでは、DBMS ログインは *KSCAdmin*、管理サーバーのデータベース名は *kav* です）：

   ```
   /* KSCAdmin という名前のユーザーを作成します */
   CREATE USER 'KSCAdmin'
   /* KSCAdmin のパスワードを指定します */
   IDENTIFIED BY '<パスワード>';
   ```

   MySQL 8.0 以前を DBMS として使用する場合、これらのバージョンでは「caching_sha2_password」認証がサポートされていないことに注意してください。既定の認証を「Caching SHA2 password」から「MySQL native password」に変更します：

   - 「mysql_native_password」認証を使用する DBMS アカウントを作成するには、次のコマンドを実行します：

```
CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<パスワード>';
```

- 既存の DBMS アカウントの認証を変更するには、次のコマンドを実行します：

  ```
  ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<パスワード>';
  ```

```
/* KSCAdmin に権限を付与します */
GRANT USAGE ON *.* TO 'KSCAdmin';
GRANT ALL ON kav.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
GRANT PROCESS ON *.* TO 'KSCAdmin';
GRANT SUPER ON *.* TO 'KSCAdmin';
```

> MariaDB 10.5 以前を DBMS として使用する場合、EXECUTE 権限を付与する必要はありません。この場合、次のコマンドをスクリプトから除外します：`GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`。

3. DBMS アカウントに付与された権限のリストを表示するには、次のスクリプトを実行します：

   ```
   SHOW grants for 'KSCAdmin';
   ```

4. 管理サーバーデータベースを手動で作成するには、次のスクリプトを実行します（このスクリプトでは、管理サーバーデータベース名は *kav* です）：

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

   DBMS アカウントを作成するスクリプトで指定したものと同じデータベース名を使用します。

5. インストーラーの実行に使用した Windows アカウントでシステムにログインします。

6. インストーラーを実行します。

   管理サーバーのセットアップウィザードが起動します。ウィザードの指示に従ってください。

7. ［管理サーバーのカスタムインストール］を選択します。

8. 管理サーバーデータベースを格納する DBMS として MySQL または MariaDB を選択します。

9. 管理サーバーデータベース名を指定します。スクリプトで指定したものと同じデータベース名を使用します。

10. スクリプトで作成した DBMS アカウントの資格情報を指定します。

11. 管理サーバーサービスを開始する Windows アカウントを指定します。

    インストーラーを使用して、既存の Windows ユーザーアカウントを選択するか、KL-AK-* 形式で新しい Windows アカウントを自動的に作成することができます。アカウントの選択にかかわらず、インストーラーは必要なシステム権限を管理サーバーサービスアカウントに割り当てます。

インストールが完了すると、管理サーバーデータベースが作成され、管理サーバーを使用できるようになります。

PostgreSQL および Postgres Pro を使用するためのアカウントの設定

必須条件

アカウントに権限を割り当てる前に、次のアクションを実行します：

1. ローカル管理者アカウントでシステムにログインしていることを確認します。
2. PostgreSQL および Postgres Pro を使用するための環境をインストールします。
3. 管理サーバーのインストールに使用する Windows アカウントがあることを確認します。
4. 管理サーバーサービスの開始に使用する Windows アカウントがあることを確認します。

管理サーバーをインストールするためのアカウントの設定（管理サーバーデータベースの自動作成）

管理サーバーのインストール用にアカウントを設定するには：

1. PostgreSQL および Postgres Pro を使用するための環境を実行します。
2. DBMS にアクセスするための Postgres ロールを選択します。次のロールのいずれかを使用できます：
   - ユーザー *Postgres*（Postgres の既定のロール）：
     ユーザー*Postgres*を使用する場合、追加の権限を付与する必要はありません。
   - Postgres の新しいロール：
     Postgres の新しいロールを使用する場合は、このロールを作成して CREATEDB 権限を付与します。これを行うには、次のスクリプトを実行します（このスクリプトでは、ロールは *KSCAdmin* です）：
     `CREATE USER "KSCAdmin" WITH PASSWORD '<パスワード>' CREATEDB;`
     作成されたロールは、管理サーバーデータベース（以降、サーバーデータベースとも表記）の所有者として使用されます。
3. 管理サーバーインストーラー（以降、インストーラーとも表記）の実行に使用される Windows アカウントでシステムにログインします。
4. インストーラーを実行します。
   管理サーバーのセットアップウィザードが起動します。ウィザードの指示に従ってください。
5. ［管理サーバーのカスタムインストール］を選択します。
6. 管理サーバーデータベースを格納する DBMS として PostgreSQL または Postgres Pro を選択します。
7. サーバーデータベース名を指定します。インストーラーはサーバーデータベースを自動的に作成します。
8. Postgres ロールの資格情報を指定します。
9. 管理サーバーサービスを開始する Windows アカウントを指定します。

インストーラーを使用して、既存の Windows ユーザーアカウントを選択するか、KL-AK-* 形式で新しい Windows アカウントを自動的に作成することができます。アカウントの選択にかかわらず、インストーラーは必要なシステム権限を管理サーバーサービスアカウントに割り当てます。

インストールが完了すると、サーバーデータベースが自動的に作成され、管理サーバーを使用できるようになります。

管理サーバーをインストールするためのアカウントの設定（管理サーバーデータベースの手動作成）

管理サーバーのインストール用にアカウントを設定するには：

1. Postgres を使用するための環境を実行します。
2. Postgres の新しいロールと管理サーバーデータベースを作成します。次に、このロールに管理サーバーデータベースに対するすべての権限を付与します。これを行うには、*Postgres* 定義データベースにユーザー *Postgres* でログインし、次のスクリプトを実行します（このスクリプトでは、ロールは *KSCAdmin*、管理サーバーの定義データベース名は *KAV* です）：

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '<パスワード>';
   CREATE DATABASE "KAV" ENCODING 'UTF8';
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

3. 作成した Postgres ロールに次の権限を付与します：

   - パブリックスキーマ内のすべてのテーブルに対する権限：ALL
   - パブリックスキーマ内のすべてのシーケンスに対する権限：ALL

   これを行うには、サーバー定義データベースにユーザー *Postgres* でログインし、次のスクリプトを実行します（このスクリプトでは、ロールは *KSCAdmin* です）：

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

4. インストーラーの実行に使用した Windows アカウントでシステムにログインします。
5. 管理サーバーのインストーラーを実行します。
   管理サーバーのセットアップウィザードが起動します。ウィザードの指示に従ってください。
6. ［管理サーバーのカスタムインストール］を選択します。
7. 管理サーバーデータベースを格納する DBMS として PostgreSQL または Postgres Pro を選択します。
8. サーバーデータベース名を指定します。スクリプトで指定したものと同じデータベース名を使用します。データベース名では大文字と小文字が区別されることに注意してください。
9. Postgres ロールの資格情報を指定します。
10. 管理サーバーサービスを開始する Windows アカウントを指定します。
    インストーラーを使用して、既存の Windows ユーザーアカウントを選択するか、KL-AK-* 形式で新しい Windows アカウントを自動的に作成することができます。アカウントの選択にかかわらず、インストーラーは必要なシステム権限を管理サーバーサービスアカウントに割り当てます。

インストールが完了すると、管理サーバーは作成されたデータベースを管理サーバーデータの保存に使用するようになります。管理サーバーが使用できるようになります。

シナリオ：Microsoft SQL Server の認証

このセクションの情報は、Kaspersky Security Center が Microsoft SQL Server をデータベース管理システムとして使用する設定のみを対象としています。

データベースと送受信する Kaspersky Security Center のデータおよびデータベースに保存されたデータを不正アクセスから保護するには、Kaspersky Security Center と SQL Server 間の通信を保護する必要があります。セキュアな通信を実現する最も確実な方法は、Kaspersky Security Center と SQL Server を同じデバイスにインストールし、両方のアプリケーションで共有メモリ機構を使用する方法です。それ以外の場合は、SSL または TLS 証明書を使って SQL Server インスタンスを認証することを推奨します。信頼できる証明機関（CA）の証明書または自己署名証明書を使用できます。いずれにしても、自己署名証明書による保護は限られているため、信頼できる CA の証明書を使用することを推奨します。

SQL Server 認証は段階的に行われます：

1. **「Certificate Requirements（証明書の要件）」に従った、SQL Server 用の SSL または TLS 自己署名証明書の生成**

   ISQL Server 用の証明書が既にある場合は、このステップを省略してください。

   SSL 証明書は、2016（13.x）より前のバージョンの SQL Server のみが対象です。SQL Server 2016（13.x）以降のバージョンには、TLS 証明書を使用します。

   たとえば、TLS 証明書を生成するには、PowerShell で次のコマンドを実行します：

   ```
   New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert:\LocalMachine
   -KeySpec KeyExchange
   ```

   ホストがドメインに含まれている場合、コマンドで SQL_HOST_NAME の代わりに SQL Server ホスト名を入力する必要があります。ホストがドメインに含まれていない場合は、ホストの*完全修飾ドメイン名*（FQDN）を入力する必要があります。管理サーバーのセットアップウィザードで、同じ名前（ホスト名または FQDN）を SQL Server インスタンス名に指定する必要があります。

2. **SQL Server インスタンスへの証明書の追加**

   この段階の手順は、SQL Server が実行されているプラットフォームによって異なります。詳細については、該当する製品の公式ドキュメントを参照してください：

   - Windows
   - Linux
   - Amazon Relational Database Service
   - Windows Azure

   フェールオーバークラスターで証明書を使用するには、フェールオーバークラスターの各ノードに証明書をインストールする必要があります。詳細は、Microsoft のドキュメントを参照してください。

3. **サービスアカウントの権限の割り当て**

SQL Server サービスが実行されているサービスアカウントに、秘密鍵にアクセスするためのフルコントロール権限があることを確認してください。詳細は、Microsoft のドキュメントを参照してください。

4. **Kaspersky Security Center 用の信頼できる証明書リストへの証明書の追加**

   管理サーバーデバイス上の信頼できる証明書リストに証明書を追加します。詳細は、Microsoft のドキュメントを参照してください。

5. **SQL Server インスタンスと Kaspersky Security Center 間での暗号化された通信の有効化**

   管理サーバーデバイスで、環境変数 `KLDBADO_UseEncryption` に値 `1` を設定します。たとえば、Windows Server 2012 R2 の場合、［**システムのプロパティ**］ウィンドウの［**詳細**］タブにある［**環境変数**］をクリックして、環境編集を変更できます。新しい変数を追加し、`KLDBADO_UseEncryption` という名前を付けてから、値 `1` を設定します。

6. **TLS 1.2 プロトコルを使用する追加の設定**

   TLS 1.2 プロトコルを使用する場合は、さらに次の手順を実行します：

   - インストールした SQL Server のバージョンが 64 ビットアプリケーションであることを確認します。
   - Microsoft OLE DB ドライバーを管理サーバーデバイスにインストールします。詳細は、Microsoft のドキュメントを参照してください。
   - 管理サーバーデバイスで、環境変数 `KLDBADO_UseMSOLEDBSQL` に値 `1` を設定します。たとえば、Windows Server 2012 R2 の場合、［**システムのプロパティ**］ウィンドウの［**詳細**］タブにある［**環境変数**］をクリックして、環境編集を変更できます。新しい変数を追加し、`KLDBADO_UseMSOLEDBSQL` という名前を付けてから、値 `1` を設定します。

     OLE DB ドライバーのバージョンが 19 以降の場合は、値「`MSOLEDBSQL19`」を環境変数「`KLDBADO_ProviderName`」にも設定します。

7. **SQL Server の名前付きインスタンスでの TCP/IP プロトコルの使用の有効化**

   SQL Server の名前付きインスタンスを使用する場合はさらに、TCP/IP プロトコルの使用を有効化し、SQL Server データベースエンジンに TCP/IP ポート番号を割り当てます。管理サーバーのセットアップウィザードで SQL Server の接続を設定する際には、SQL Server のホスト名とポート番号を［**DBMS のインスタンス名**］に指定します。

シナリオ：MySQL サーバーの認証

MySQL サーバーの認証には TLS 証明書を使用することを推奨します。信頼できる証明機関（CA）の証明書または自己署名証明書を使用できます。

管理サーバーは、MySQL に対して一方向および双方向の SSL 認証の両方をサポートします。

一方向 SSL 認証の有効化

MySQL の一方向 SSL 認証を設定するには、次の手順に従います：

1. **MySQL サーバー用の自己署名 TLS 証明書を生成する**

   PowerShell で、証明書を保存するフォルダーにディレクトリを変更します。次のコマンドを実行します：

```
$CertCA = New-SelfSignedCertificate `
-Subject "CN=CertCA" `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
```

```
-NotAfter (Get-Date).AddDays(365)

$CertCABase64 = [System.Convert]::ToBase64String($CertCA.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeaf = New-SelfSignedCertificate `
-Subject "CN=CertLeaf" `
-Signer $CertCA `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-KeyExportPolicy Exportable `
-NotAfter (Get-Date).AddDays(365)

$CertLeafBase64 = [System.Convert]::ToBase64String($CertLeaf.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeafRSACng =
[System.Security.Cryptography.X509Certificates.RSACertificateExtensions]::GetRSAPrivateKey($CertLeaf)
$CertLeafKeyBytes =
$CertLeafRSACng.Key.Export([System.Security.Cryptography.CngKeyBlobFormat]::Pkcs8PrivateBlob)
$CertLeafKeyBase64 = [System.Convert]::ToBase64String($CertLeafKeyBytes,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertCAPemCert = @"
-----BEGIN CERTIFICATE-----
$CertCABase64
-----END CERTIFICATE-----
"@

$CertLeafPemKey = @"
-----BEGIN PRIVATE KEY-----
$CertLeafKeyBase64
-----END PRIVATE KEY-----
"@

$CertLeafPemCert = @"
-----BEGIN CERTIFICATE-----
$CertLeafBase64
-----END CERTIFICATE-----
"@

# Output to file

$CertCAPemCert | Out-File -FilePath ca-cert.pem -Encoding Ascii

$CertLeafPemKey | Out-File -FilePath server-key.pem -Encoding Ascii
$CertLeafPemCert | Out-File -FilePath server-cert.pem -Encoding Ascii
```

これらのコマンドは、現在のユーザーの証明書を作成し、証明書を PEM 形式でエクスポートします。サーバーを認証するには、エクスポートされた PEM ファイルのみが必要です。作成された証明書を Windows から削除するには、PowerShell で次のコマンドを実行します：

```
certmgr.msc
```

作成された証明書を「**個人**」→「**証明書**」フォルダーで探して削除します。

2 サーバーフラグファイルの作成

Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

klscflag ユーティリティを使用して KLSRV_MYSQL_OPT_SSL_CA サーバーフラグを作成し、その値として証明書へのパスを指定します。

```
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ca-cert.pem へのパス> -t s
```

3 定義データベースの設定

ファイル my.cnf で証明書を指定します。テキストエディターでファイル my.cnf を開き、次の行を［mysqld］セクションに追加します：

```
[mysqld]
```

```
ssl-ca="...\mysqlcerts\ca-cert.pem"

ssl-cert="...\mysqlcerts\server-cert.pem"

ssl-key="...\mysqlcerts\server-key.pem"
```

双方向 SSL 認証の有効化

MySQL の双方向 SSL 認証を設定するには、次の手順に従います：

1. **サーバーフラグファイルの作成**

   Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

   klscflag ユーティリティを使用してサーバーフラグを作成し、その値として証明書ファイルへのパスを指定します。

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ca-cert.pem へのパス> -t s

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <server-cert.pem へのパス> -t s

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <server-key.pem へのパス> -t s
   ```

2. **パスフレーズを指定する（オプション）**

   server-key.pem にパスフレーズが必要な場合は、KLSRV_MARIADB_OPT_TLS_PASPHRASE フラグを作成し、その値としてパスフレーズを指定します：

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <パスフレーズ> -t s
   ```

3. **定義データベースの設定**

   ファイル my.cnf で証明書を指定します。テキストエディターでファイル my.cnf を開き、次の行を［mysqld］セクションに追加します：

   ```
   [mysqld]

   ssl-ca="...\ca-cert.pem"

   ssl-cert="...\server-cert.pem"

   ssl-key="...\server-key.pem"
   ```

シナリオ：PostgreSQL サーバーの認証

PostgreSQL サーバーの認証には TLS 証明書を使用することを推奨します。信頼できる証明機関（CA）の証明書または自己署名証明書を使用できます。自己署名証明書による保護は限られているため、信頼できる CA の証明書を使用します。

管理サーバーは、PostgreSQL に対して一方向および双方向の SSL 認証の両方をサポートします。

PostgreSQL の SSL 認証を設定するには、次の手順に従います：

1. **PostgreSQL サーバーの証明書を生成します。**

   OpenSSL ベースのクロスプラットフォームユーティリティで、次のコマンドを実行します。

```
openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj
"/CN=psql"

chmod og-rwx psql.key
```

2. **管理サーバーの証明書を生成します。**

   次のコマンドを実行します：CN 値は、管理サーバーの代わりに PostgreSQL に接続するユーザーの名前と一致する必要があります。ユーザー名は既定で postgres に設定されます。

```
openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -
subj "/CN=postgres"

chmod og-rwx postgres.key
```

3. **クライアント証明書認証を設定します。**

   pg_hba.conf を次のように変更します：

```
hostssl all all 0.0.0.0/0 md5
```

   pg_hba.conf に `host` で始まるレコードが含まれていないことを確認してください。

4. **PostgreSQL の証明書を指定します。**

   一方向 SSL 認証

   postgresql.conf を次のように変更します（.crt およびライセンス情報ファイルへの正しいパスを指定します）：

```
listen_addresses ='localhost, server-ip'
ssl = on
ssl_cert_file = '<psql.crt>'
ssl_key_file = '<psql.key>'
```

   双方向 SSL 認証

   postgresql.conf を次のように変更します（.crt およびライセンス情報ファイルへの正しいパスを指定します）：

```
listen_addresses ='localhost, server-ip'
ssl = on
ssl_ca_file = '<postgres.crt>'
ssl_cert_file = '<psql.crt>'
ssl_key_file = '<psql.key>'
```

5. **PostgreSQL デーモンを再起動します。**

   次のコマンドを実行します：

```
systemctl restart postgresql-14.service
```

6. **管理サーバーのサーバーフラグを指定します。**

   一方向 SSL 認証

klscflag ユーティリティを使用して KLSRV_POSTGRES_OPT_SSL_CA サーバーフラグを作成し、その値として証明書へのパスを指定します。

Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

次のコマンドを実行します：

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <psql.crt へのパス > -t s
```

双方向 SSL 認証

klscflag ユーティリティを使用してサーバーフラグを作成し、その値として証明書ファイルへのパスを指定します。

Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

次のコマンドを実行します：

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <psql.crt へのパス > -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <postgres.crt へのパス > -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <postgres.key へのパス > -t s
```

postgres.key にパスフレーズが必要な場合は、KLSRV_POSTGRES_OPT_TLS_PASPHRASE フラグを作成し、その値としてパスフレーズを指定します：

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <パスフレーズ> -t s
```

7. **管理サーバーサービスを再起動します。**

管理サーバーのインストールに関する推奨事項

このセクションでは、管理サーバーをインストールする際の推奨事項について説明します。また、管理サーバーデバイスの共有フォルダーを使用して、クライアントデバイスにネットワークエージェントを導入する方法についても説明します。

フェールオーバークラスターに管理サーバーサービス用のアカウントを作成する

既定では、インストーラーが自動的に管理サーバーのサービス用非特権アカウントを作成します。一般的なデバイスに管理サーバーをインストールする場合には、この動作を活用するのが最も便利です。

ただし、フェールオーバークラスターに管理サーバーをインストールする際には、別の方法で行います：

1. 管理サーバーのサービス用非特権ドメインアカウントを作成し、そのアカウントを KLAdmins という名前のグローバルドメインセキュリティグループに所属させます。

2. 管理サーバーのインストーラーで、サービス用に作成したドメインアカウントを指定します。

共有フォルダーの定義

管理サーバーのインストール時には、共有フォルダーの場所を指定できます。また、インストール後に管理サーバーのプロパティで、共有フォルダーの場所を指定することもできます。既定では、共有フォルダーは管理サーバーがインストールされているデバイス上に作成されます（「**すべてのユーザー**」サブグループの読み取り権限が付与）。ただし、特定のケース（高負荷、分離されたネットワークからのアクセスが必要な場合など）においては、共有フォルダーを専用ファイルリソースに置くのが適切な方法です。

共有フォルダーは、ネットワークエージェントの導入時に使用されることもあります。

共有フォルダーでは、大文字と小文字の区別を無効にする必要があります。

管理サーバーツールによる、Active Directory グループポリシーを使用したリモートインストール

対象デバイスが（ワークグループではない）Windows ドメイン内に置かれている場合は、Active Directory グループポリシーを使用して初期導入（まだ管理されていないデバイスへのネットワークエージェントとセキュリティ製品のインストール）を実行する必要があります。導入作業を実行するには、Kaspersky Security Center のリモートインストール用の標準タスクを使用します。ネットワークが大規模な場合は、共有フォルダーを専用ファイルリソースに置き、管理サーバーデバイスのディスクサブシステムの負荷を低減させるのが有効です。

スタンドアロンパッケージへの UNC パスを配信することによるリモートインストール

組織内でネットワーク接続されているデバイスのユーザーにローカル管理者権限が付与されている場合の別の初期導入方法は、スタンドアロンのネットワークエージェントパッケージを作成することです（または、セキュリティ製品と「結合した」ネットワークエージェントパッケージを作成）。スタンドアロンパッケージを作成したら、ユーザーに対してそのパッケージへのリンクを送信します。このパッケージは共有フォルダーに格納されています。ユーザーがこのリンクをクリックすると、インストールが開始されます。

管理サーバーの共有フォルダーからのアップデート

アンチウイルスのアップデートタスクでは、管理サーバーの共有フォルダーからのアップデートを設定できます。このタスクを多数のデバイスに割り当てる場合は、共有フォルダーを専用ファイルリソースに置くのが適切な方法です。

オペレーティングシステムイメージのインストール

オペレーティングシステムイメージは、常に共有フォルダーを介してインストールされます。デバイスは共有フォルダーからオペレーティングシステムイメージを読み取ります。組織の多数のデバイスにイメージを導入する場合は、共有フォルダーを専用ファイルリソースに置くのが適切な方法です。

管理サーバーのアドレスの指定

管理サーバーのインストール時には、管理サーバーのアドレスを指定できます。このアドレスは、ネットワークエージェントのインストールパッケージを作成する際の既定のアドレスとして使用されます。

管理サーバーのアドレスとして、以下を指定できます：

- 既定で指定される管理サーバーの NetBIOS 名
- 組織のネットワーク上のドメイン名システム（DNS）が構成され、正しく機能している場合は、管理サーバーの完全修飾ドメイン名（FQDN）
- 管理サーバーが非武装地帯（DMZ）にインストールされている場合は外部アドレス

外部アドレスを指定すると、管理コンソールツールを使用して管理サーバーのアドレスを変更できるようになります。この場合、作成済みのネットワークエージェントのインストールパッケージでは、アドレスは自動的には変更されません。

標準インストール

標準インストールとは、アプリケーションファイル用に既定パスを使用し、既定のセットのプラグインをインストールして、モバイルデバイス管理を有効にしない管理サーバーインストールのことです。

Kaspersky Security Center 管理サーバーをローカルデバイスにインストールするには：

ksc_<バージョン番号>.<ビルド番号>_full_<ローカリゼーション言語>.exe 実行ファイルを実行します。

ウィンドウが開き、インストールするカスペルスキー製品の選択を要求されます。製品を選択するウィンドウで、［**Kaspersky Security Center 管理サーバーをインストール**］をクリックし、管理サーバーのセットアップウィザードを開始します。ウィザードの指示に従ってください。

ステップ1：使用許諾契約書とプライバシーポリシーの確認

セットアップウィザードのこの段階では、ユーザーとカスペルスキーとの間で締結される使用許諾契約書およびプライバシーポリシーの内容を読む必要があります。

Kaspersky Security Center 配布キットに含まれるアプリケーション管理プラグインの使用許諾契約書およびプライバシーポリシーの確認を要求される場合があります。

使用許諾契約書とプライバシーポリシーをよく読んでください。使用許諾契約書とプライバシーポリシーのすべての条件に同意する場合は、該当するチェックボックスをオンにすることで確認してください。

両方のチェックボックスをオンにすると、製品のデバイスへのインストールが続行されます。

使用許諾契約書またはプライバシーポリシーに同意しない場合、［**キャンセル**］をクリックしてインストールを中断します。

ステップ 2：インストール方法の選択

インストール方法を選択するウィンドウで、［**標準**］を選択します。

企業ネットワーク内の小規模エリアで動作をテストするなど、Kaspersky Security Center を試したい場合は、標準インストールを推奨します。標準インストール中は、データベースのみを設定します。管理サーバーの設定は指定しません。代わりに管理サーバーの既定値が使用されます。標準インストールでは管理プラグインをインストールする選択はできません。既定の一連のプラグインのみがインストールされます。標準インストール中は、モバイルデバイス用のインストールパッケージは作成されません。後で、管理コンソールから作成できます。

ステップ 3：Kaspersky Security Center Web コンソールのインストール

このステップは、64 ビットのオペレーティングシステムを使用している場合にのみ表示されます。これ以外の場合、Kaspersky Security Center Web コンソールは 32 ビットオペレーティングシステムでは動作しないため、このステップは表示されません。

既定では、Kaspersky Security Center Web コンソールと MMC ベースの管理コンソールの両方がインストールされます。

Kaspersky Security Center Web コンソールのみをインストールする場合：

1. ［**このコンソールのみをインストール**］を選択します。
2. ドロップダウンリストで［**Web ベースのコンソール**］を選択します。

管理サーバーのインストールが完了すると、Kaspersky Security Center Web コンソールのインストールが自動的に開始されます。

MMC ベースの管理コンソールのみをインストールする場合：

1. ［**このコンソールのみをインストール**］を選択します。
2. ドロップダウンリストで［**MMC ベースのコンソール**］を選択します。

ステップ 4：ネットワークの規模の選択

Kaspersky Security Center をインストールするネットワークの規模を指定します。ネットワーク上のデバイス数に応じて、ウィザードが本製品のインストールおよび本製品のインターフェイスの表示を設定します。

次の表に、ネットワークの規模に応じて調整される本製品のインストールの設定およびインターフェイスの表示の設定についてまとめています。

選択したネットワーク規模に応じたインストール設定

設定	1～100 台	100～1000 台	1000～5000	デバイスが

	のデバイス	のデバイス	台のデバイス	5000 台以上
コンソールツリーにセカンダリ管理サーバーおよび仮想管理サーバーのノードとそれらに関連するすべての設定を表示する	なし	なし	あり	あり
サーバーおよび管理グループのプロパティウィンドウに［**セキュリティ**］セクションを表示する	なし	なし	あり	あり
クライアントデバイスでのアップデートタスクの開始時間をランダムに配分する	なし	5 分以上の間隔	10 分以上の間隔	10 分以上の間隔

管理サーバーから接続しているデータベースサーバーが MySQL 5.7 または SQL Express の場合、10,000 台を超えるデバイスを管理しないようにすることを推奨します。MariaDB のデータベース管理システムでは、推奨される最大の管理対象デバイス数は 20,000 台です。

ステップ 5：データベースの選択

ウィザードのこの手順では、管理サーバーデータベースの格納に使用する次のデータベース管理システム（DBMS）のいずれかを選択します：

- **Microsoft SQL Server または SQL Server Express**
- **MySQL または MariaDB**
- **PostgreSQL または Postgres Pro**

管理サーバーは、ドメインコントローラーではなく専用サーバーにインストールすることを推奨します。ただし、読み取り専用ドメインコントローラー（RODC）として動作するサーバーに Kaspersky Security Center をインストールする場合は、Microsoft SQL Server（SQL Express）をローカル（同じデバイス）にインストールしないでください。この場合、Microsoft SQL Server（SQL Express）と Kaspersky Security Center とは別のデバイスにインストールするか、Kaspersky Security Center と同じデバイスに DBMS をインストールする必要がある場合には MySQL、MariaDB、または PostgreSQL を使用することを推奨します。

管理サーバーのデータベース構造は、Kaspersky Security Center のインストールフォルダーにある klakdb.chm ファイルで提供しています。このファイルは、カスペルスキーポータルのアーカイブからも入手できます：klakdb.zip。

ステップ 6：SQL Server の設定

ウィザードのこの手順では、選択したデータベース管理システム（DBMS）に応じて、次の接続設定を指定します。

- 前のステップで［**Microsoft SQL Server または SQL Server Express**］を選択した場合：
  - ［**DBMS のインスタンス名**］に、ネットワーク上の SQL Server の名前を指定します。ネットワークにインストールされているすべての SQL Server のリストを表示するには、［**参照**］をクリックします。既定では、このフィールドは空白です。

    カスタムポート経由で SQL Server に接続した場合は、SQL Server ホスト名とともに、ポート番号を次のようにカンマで区切って指定します：

    ```
    SQL_Server_host_name,1433
    ```

管理サーバーと SQL Server 間の通信を証明書によって保護する場合は、証明書の生成時に使用したのと同じホスト名を［**DBMS のインスタンス名**］に指定します。SQL Server の名前付きインスタンスを使用する場合は、SQL Server ホスト名とともに、ポート番号を次のようにカンマで区切って指定します：

```
SQL_Server_name,1433
```

SQL Server の複数のインスタンスを同じホスト上で使用する場合は、インスタンス名を次のようにバックスラッシュで区切って指定します：

```
SQL_Server_name\SQL_Server_instance_name,1433
```

企業ネットワーク上の SQL Server で Always On 機能が有効化されている場合、可用性グループのリスナーの名前を［**DBMS のインスタンス名**］で指定します。Always On 機能が有効な時、管理サーバーがサポートする可用性モードは同期コミットモードのみであることに注意してください。

- ［**データベース名**］に、管理サーバーのデータの保管用に作成されている DBMS の名前を指定します。既定値は *KAV* です。

この段階で、Kaspersky Security Center をインストールしているデバイスに SQL Server をインストールする場合は、インストールを中断し、SQL Server のインストール後に再開する必要があります。サポートする SQL Server のバージョンは、システム要件に一覧で掲載しています。

リモートデバイスに SQL Server をインストールする場合は、Kaspersky Security Center のセットアップウィザードを中断する必要はありません。SQL サーバーをインストールし、Kaspersky Security Center のインストールを続けます。

- 前のステップで［**MySQL または MariaDB**］を選択した場合：
  - ［**DBMS のインスタンス名**］に、DBMS インスタンスの名前を指定します。既定では、この名前は Kaspersky Security Center をインストールするデバイスの IP アドレスです。
  - ［**ポート**］に、管理サーバーを DBMS へ接続するポートを指定します。既定のポート番号は 3306 です。
  - ［**データベース名**］に、管理サーバーのデータの保管用に作成されている DBMS の名前を指定します。既定値は *KAV* です。
- 前のステップで［**PostgreSQL または Postgres Pro**］を選択した場合：
  - ［**PostgreSQL または Postgres Pro サーバー**］に、DBMS インスタンスの名前を指定します。既定では、この名前は Kaspersky Security Center をインストールするデバイスの IP アドレスです。
  - ［**ポート**］フィールドに、管理サーバーを DBMS へ接続するポートを指定します。既定のポート番号は 5432 です。
  - ［**データベース名**］に、管理サーバーのデータの保管用に作成されている DBMS の名前を指定します。既定値は *KAV* です。

ステップ 7：認証方法の選択

管理サーバーとデータベース管理システム（DBMS）の接続時に使用される認証モードを決定します。

選択した DBMS の種別に応じて、次の認証モードから選択できます：

- SQL Express または Microsoft SQL Server の場合は、次のいずれかをオンにします：
  - **Microsoft Windows 認証モード**。権限の検証には、管理サーバーの起動に使用したアカウントが使用されます。

- **SQL Server 認証モード**。このオプションをオンにすると、ウィンドウで指定したアカウントがアクセス権限の検証に使用されます。［**アカウント**］および［**パスワード**］に情報を入力します。

  入力したパスワードを表示するには、［**入力した文字を表示する**］をクリックしたままにします。

どちらの認証モードでも、データベースが利用可能かどうかのチェックが行われます。データベースを使用できない場合、エラーメッセージが表示され、正しい認証情報の入力が要求されます。

管理サーバーデータベースが別のデバイスに保存されており、管理サーバーアカウントからデータベースサーバーにアクセスできない場合は、管理サーバーのインストールまたはアップグレード時に SQL Server 認証モードを使用する必要があります。このような状況は、データベースを保管するデバイスがドメイン外にある場合、またはローカルシステムアカウントで管理サーバーがインストールされている場合に発生します。

- MySQL、MariaDB、PostgreSQL、または Postgres Pro の場合は、アカウントとパスワードを指定します。

ステップ 8：ハードディスク上へのファイルの解凍とインストール

Kaspersky Security Center のインストールを設定した後に、ハードディスク上のファイルのインストールを開始できます。

インストールに追加プログラムが必要な場合は、Kaspersky Security Center のインストールが開始される前に、セットアップウィザードの［**必要項目のインストール**］ウィンドウに、通知が表示されます。［**次へ**］をクリックすると、必要なプログラムが自動的にインストールされます。

最後のウィンドウでは、どちらのコンソールで Kaspersky Security Center の使用を開始するかを選択できます。

- **MMC ベースの管理コンソールを起動**
- **Kaspersky Security Center Web コンソールの開始**

  このオプションは、ここまでのステップで Kaspersky Security Center Web コンソールのインストールを選択した場合にのみ使用できます。

また、［**終了**］をクリックして、Kaspersky Security Center の使用を開始せずにウィザードを終了することもできます。ウィザードの終了後も、いつでも使用を開始できます。

管理コンソールまたは Kaspersky Security Center Web コンソールの初回起動時に、製品の初期設定を実行することができます。

セットアップウィザードが終了したら、オペレーティングシステムがインストールされているハードディスクに、次のアプリケーションコンポーネントがインストールされます：

- 管理サーバー（サーバー向けネットワークエージェントを含む）
- MMC ベースの管理コンソール
- Kaspersky Security Center Web コンソール（インストール対象として選択した場合）
- 配布キットに含まれるアプリケーション管理プラグイン

また、Microsoft Windows Installer 4.5 が前もってインストールされていない場合はインストールされます。

カスタムインストール

カスタムインストールは、インストールするコンポーネントを選択して、アプリケーションのインストール先フォルダーを指定するように求められる管理サーバーインストールです。

この種別のインストールを使用すると、データベースと管理サーバーを設定でき、各種カスペルスキー製品の標準インストールまたは管理プラグインに含まれていないコンポーネントをインストールできます。また、モバイルデバイス管理を有効にすることもできます。

Kaspersky Security Center 管理サーバーをローカルデバイスにインストールするには：

ksc_<バージョン番号>.<ビルド番号>_full_<ローカリゼーション言語>.exe 実行ファイルを実行します。

ウィンドウが開き、インストールするカスペルスキー製品の選択を要求されます。製品を選択するウィンドウで、［**Kaspersky Security Center 管理サーバーをインストール**］をクリックし、管理サーバーのセットアップウィザードを開始します。ウィザードの指示に従ってください。

ステップ1：使用許諾契約書とプライバシーポリシーの確認

セットアップウィザードのこの段階では、ユーザーとカスペルスキーとの間で締結される使用許諾契約書およびプライバシーポリシーの内容を読む必要があります。

Kaspersky Security Center 配布キットに含まれるアプリケーション管理プラグインの使用許諾契約書およびプライバシーポリシーの確認を要求される場合があります。

使用許諾契約書とプライバシーポリシーをよく読んでください。使用許諾契約書とプライバシーポリシーのすべての条件に同意する場合は、該当するチェックボックスをオンにすることで確認してください。

両方のチェックボックスをオンにすると、製品のデバイスへのインストールが続行されます。

使用許諾契約書またはプライバシーポリシーに同意しない場合、［**キャンセル**］をクリックしてインストールを中断します。

ステップ2：インストール方法の選択

インストール方法を選択するウィンドウで、「**カスタム**」を指定します。

カスタムインストールでは、Kaspersky Security Center 設定の編集が可能です。たとえば、共有フォルダーのパス、管理サーバーへの接続用アカウントおよびポート、データベース設定などです。カスタムインストールでは、インストールするカスペルスキー製品の管理プラグインの指定ができます。カスタムインストール中に、該当するオプションをオンにすると、モバイルデバイス用のインストールパッケージを作成できます。

ステップ3：インストールするコンポーネントの選択

インストールしたい Kaspersky Security Center 管理サーバーのコンポーネントを選択します：

- **モバイルデバイス管理**：Kaspersky Security Center のセットアップウィザードの実行時にモバイルデバイスのインストールパッケージを作成する必要がある場合は、このチェックボックスを選択します。管理サー

バーのインストール後、管理コンソールツールを使用して、モバイルデバイス用のインストールパッケージを手動で作成することもできます。

- **SNMP エージェント**：このコンポーネントは、SNMP プロトコルを使用する管理サーバーに関する統計情報を取得します。SNMP がインストールされているデバイスにアプリケーションをインストールする場合、このコンポーネントを利用できます。

  Kaspersky Security Center のインストール後、統計情報の取得に必要な mib ファイルが、本製品のインストールフォルダーのサブフォルダー SNMP に保存されます。

ネットワークエージェントおよび管理コンソールは、コンポーネントリストには表示されません。これらのコンポーネントは自動的にインストールされ、インストールを取り消すことはできません。

このステップでは、管理サーバーのインストールフォルダーを指定する必要があります。既定では、<ドライブ名>:\Program Files\Kaspersky Lab\Kaspersky Security Center にコンポーネントがインストールされます。このフォルダーがない場合は、インストール中に自動的に作成されます。インストール先フォルダーは、［**参照**］を使用して変更できます。

ステップ 4：Kaspersky Security Center Web コンソールのインストール

このステップは、64 ビットのオペレーティングシステムを使用している場合にのみ表示されます。これ以外の場合、Kaspersky Security Center Web コンソールは 32 ビットオペレーティングシステムでは動作しないため、このステップは表示されません。

既定では、Kaspersky Security Center Web コンソールと MMC ベースの管理コンソールの両方がインストールされます。

Kaspersky Security Center Web コンソールのみをインストールする場合：

1. ［**このコンソールのみをインストール**］を選択します。
2. ドロップダウンリストで［**Web ベースのコンソール**］を選択します。

管理サーバーのインストールが完了すると、Kaspersky Security Center Web コンソールのインストールが自動的に開始されます。

MMC ベースの管理コンソールのみをインストールする場合：

1. ［**このコンソールのみをインストール**］を選択します。
2. ドロップダウンリストで［**MMC ベースのコンソール**］を選択します。

ステップ 5：ネットワークの規模の選択

Kaspersky Security Center をインストールするネットワークの規模を指定します。ネットワーク上のデバイス数に応じて、ウィザードが本製品のインストールおよび本製品のインターフェイスの表示を設定します。

次の表に、ネットワークの規模に応じて調整される本製品のインストールの設定およびインターフェイスの表示の設定についてまとめています。

選択したネットワーク規模に応じたインストール設定

設定	1～100 台のデバイス	100～1000 台のデバイス	1000～5000 台のデバイス	デバイスが 5000 台以上
コンソールツリーにセカンダリ管理サーバーおよび仮想管理サーバーのノードとそれらに関連するすべての設定を表示する	なし	なし	あり	あり
サーバーおよび管理グループのプロパティウィンドウに［**セキュリティ**］セクションを表示する	なし	なし	あり	あり
クライアントデバイスでのアップデートタスクの開始時間をランダムに配分する	なし	5 分以上の間隔	10 分以上の間隔	10 分以上の間隔

管理サーバーから接続しているデータベースサーバーが MySQL 5.7 または SQL Express の場合、10,000 台を超えるデバイスを管理しないようにすることを推奨します。MariaDB のデータベース管理システムでは、推奨される最大の管理対象デバイス数は 20,000 台です。

ステップ 6：データベースの選択

ウィザードのこの手順では、管理サーバーデータベースの格納に使用する次のデータベース管理システム（DBMS）のいずれかを選択します：

- **Microsoft SQL Server または SQL Server Express**
- **MySQL または MariaDB**
- **PostgreSQL または Postgres Pro**

管理サーバーは、ドメインコントローラーではなく専用サーバーにインストールすることを推奨します。ただし、読み取り専用ドメインコントローラー（RODC）として動作するサーバーに Kaspersky Security Center をインストールする場合は、Microsoft SQL Server（SQL Express）をローカル（同じデバイス）にインストールしないでください。この場合、Microsoft SQL Server（SQL Express）と Kaspersky Security Center とは別のデバイスにインストールするか、Kaspersky Security Center と同じデバイスに DBMS をインストールする必要がある場合には MySQL、MariaDB、または PostgreSQL を使用することを推奨します。

管理サーバーのデータベース構造は、Kaspersky Security Center のインストールフォルダーにある klakdb.chm ファイルで提供しています。このファイルは、カスペルスキーポータルのアーカイブからも入手できます：klakdb.zip。

ステップ 7：SQL Server の設定

ウィザードのこの手順では、選択したデータベース管理システム（DBMS）に応じて、次の接続設定を指定します。

- 前のステップで［**Microsoft SQL Server または SQL Server Express**］を選択した場合：
  - ［**DBMS のインスタンス名**］に、ネットワーク上の SQL Server の名前を指定します。ネットワークにインストールされているすべての SQL Server のリストを表示するには、［**参照**］をクリックします。既

定では、このフィールドは空白です。

カスタムポート経由で SQL Server に接続した場合は、SQL Server ホスト名とともに、ポート番号を次のようにカンマで区切って指定します：

```
SQL_Server_host_name,1433
```

管理サーバーと SQL Server 間の通信を証明書によって保護する場合は、証明書の生成時に使用したのと同じホスト名を［**DBMS のインスタンス名**］に指定します。SQL Server の名前付きインスタンスを使用する場合は、SQL Server ホスト名とともに、ポート番号を次のようにカンマで区切って指定します：

```
SQL_Server_name,1433
```

SQL Server の複数のインスタンスを同じホスト上で使用する場合は、インスタンス名を次のようにバックスラッシュで区切って指定します：

```
SQL_Server_name\SQL_Server_instance_name,1433
```

企業ネットワーク上の SQL Server で Always On 機能が有効化されている場合、可用性グループのリスナーの名前を［**DBMS のインスタンス名**］で指定します。Always On 機能が有効な時、管理サーバーがサポートする可用性モードは同期コミットモードのみであることに注意してください。

- ［**データベース名**］に、管理サーバーのデータの保管用に作成されている DBMS の名前を指定します。既定値は *KAV* です。

この段階で、Kaspersky Security Center をインストールしているデバイスに SQL Server をインストールする場合は、インストールを中断し、SQL Server のインストール後に再開する必要があります。サポートする SQL Server のバージョンは、システム要件に一覧で掲載しています。

リモートデバイスに SQL Server をインストールする場合は、Kaspersky Security Center のセットアップウィザードを中断する必要はありません。SQL サーバーをインストールし、Kaspersky Security Center のインストールを続けます。

- 前のステップで［**MySQL または MariaDB**］を選択した場合：
  - ［**DBMS のインスタンス名**］に、DBMS インスタンスの名前を指定します。既定では、この名前は Kaspersky Security Center をインストールするデバイスの IP アドレスです。
  - ［**ポート**］に、管理サーバーを DBMS へ接続するポートを指定します。既定のポート番号は 3306 です。
  - ［**データベース名**］に、管理サーバーのデータの保管用に作成されている DBMS の名前を指定します。既定値は *KAV* です。
- 前のステップで［**PostgreSQL または Postgres Pro**］を選択した場合：
  - ［**PostgreSQL または Postgres Pro サーバー**］に、DBMS インスタンスの名前を指定します。既定では、この名前は Kaspersky Security Center をインストールするデバイスの IP アドレスです。
  - ［**ポート**］フィールドに、管理サーバーを DBMS へ接続するポートを指定します。既定のポート番号は 5432 です。
  - ［**データベース名**］に、管理サーバーのデータの保管用に作成されている DBMS の名前を指定します。既定値は *KAV* です。

ステップ 8：認証方法の選択

管理サーバーとデータベース管理システム（DBMS）の接続時に使用される認証モードを決定します。

選択した DBMS の種別に応じて、次の認証モードから選択できます：

- SQL Express または Microsoft SQL Server の場合は、次のいずれかをオンにします：

  - **Microsoft Windows 認証モード**。権限の検証には、管理サーバーの起動に使用したアカウントが使用されます。

  - **SQL Server 認証モード**。このオプションをオンにすると、ウィンドウで指定したアカウントがアクセス権限の検証に使用されます。［**アカウント**］および［**パスワード**］に情報を入力します。

    入力したパスワードを表示するには、［**入力した文字を表示する**］をクリックしたままにします。

  どちらの認証モードでも、データベースが利用可能かどうかのチェックが行われます。データベースを使用できない場合、エラーメッセージが表示され、正しい認証情報の入力が要求されます。

  管理サーバーデータベースが別のデバイスに保存されており、管理サーバーアカウントからデータベースサーバーにアクセスできない場合は、管理サーバーのインストールまたはアップグレード時に SQL Server 認証モードを使用する必要があります。このような状況は、データベースを保管するデバイスがドメイン外にある場合、またはローカルシステムアカウントで管理サーバーがインストールされている場合に発生します。

- MySQL、MariaDB、PostgreSQL、または Postgres Pro の場合は、アカウントとパスワードを指定します。

ステップ 9：管理サーバーを開始するアカウントの選択

サービスとして管理サーバーを開始する場合に使用するアカウントを選択します。

- **アカウントを自動的に作成**：kladminserver を実行する KL-AK-* という名前のアカウントを作成します。

  共有フォルダーと DBMS を管理サーバーと同じデバイスに配置する場合、このオプションを選択します。

- **アカウントの選択**：管理サーバーのサービス（kladminserver）は選択したアカウントで実行されます。

  次のような場合は、ドメインアカウントを選択する必要があります：別のデバイスにある SQL Server（SQL Express を含む）を DBMS として使用する場合、または共有フォルダーを別のデバイスに配置する場合。

  Kaspersky Security Center は、管理対象サービスアカウント（MSA）とグループ管理対象サービスアカウント（gMSA）をサポートしています。これらの種別のアカウントをドメインで使用している場合は、それらの 1 つを管理サーバーのサービス用のアカウントとして選択できます。

  MSA または gMSA を指定する前に、管理サーバーをインストールするのと同じデバイスにアカウントをインストールする必要があります。アカウントがまだインストールされていない場合は、管理サーバーのインストールをキャンセルし、アカウントをインストールしてから管理サーバーのインストールを再開してください。ローカルデバイスへの管理対象サービスアカウントのインストールの詳細は、Microsoft 公式ドキュメントを参照してください。

  MSA または gMSA を指定するには：

  1. ［**参照**］をクリックします。
  2. ウィンドウが表示されたら、［**オブジェクト種別**］をクリックします。
  3. ［**サービスのアカウント**］の種別を選択して、［**OK**］をクリックします。
  4. 関連するアカウントを選択して［**OK**］をクリックします。

選択したアカウントは、使用する DBMS に応じた権限を持っている必要があります。

セキュリティ上の理由から、管理サーバーを実行するアカウントには特権ステータスを割り当てないでください。

後で管理サーバーのアカウントを変更する場合は、管理サーバーのアカウントを切り替えるユーティリティ（klsrvswch）を使用する必要があります。管理サーバーのインストールに使用した管理者権限を持つアカウントで、管理サーバーデバイス上で klsrvswch ユーティリティを起動する必要があることに注意してください。

ステップ 10：Kaspersky Security Center のサービスを実行するために使用するアカウントの選択

Kaspersky Security Center のサービスをこのデバイスで実行する場合のアカウントを選択します：

- **アカウントを自動的に作成**：Kaspersky Security Center が kladmins グループ内のこのデバイス上に KlScSvc という名前のローカルアカウントを作成します。作成したアカウントで Kaspersky Security Center のサービスが実行されます。
- **アカウントの選択**：選択したアカウントで Kaspersky Security Center のサービスが実行されます。

  レポートの保存先に別のデバイス内のフォルダーを指定する場合や、企業のセキュリティポリシーで定められている場合などには、ドメインアカウントを選択する必要があります。また、フェールオーバークラスターに管理サーバーをインストールする場合も、ドメインアカウントを選択する必要があります。

セキュリティ上の理由により、サービスを実行しているアカウントには権限ステータスを付与しないでください。

KSN プロキシサービス（ksnproxy）、カスペルスキーアクティベーションプロキシサービス（klactprx）、カスペルスキー認証ポータルサービス（klwebsrv）は、選択したアカウントで実行されます。

ステップ 11：共有フォルダーの選択

次の目的で使用する共有フォルダーの場所と名前を定義します：

- アプリケーションのリモートインストールに必要なファイルを保管する（ファイルは、インストールパッケージの作成時に管理サーバーへコピーされます）
- アップデート元から管理サーバーにダウンロードされたアップデートを保管する

ファイル共有（読み取り専用）はすべてのユーザーで有効になります。

次のオプションからいずれかをオンにできます：

- **共有フォルダーの作成**：フォルダーを新規作成します。テキストボックスにフォルダーへのパスを指定します。
- **既存共有フォルダーの選択**：既に作成されている共有フォルダーを選択します。

共有フォルダーとして選択できるのは、インストールを実行しているデバイス上のローカルフォルダー、または企業ネットワーク内の任意のクライアントデバイス上にあるリモートディレクトリです。［**参照**］を使用して共有フォルダーを選択するか、共有フォルダーの UNC パス（「\\server\Share」など）を該当フィールドに入力して手動で指定します。

既定では、Kaspersky Security Center のインストール先として指定したフォルダー内にローカルサブフォルダー Share が作成されます。

必要に応じて、後で共有フォルダーを定義できます。

ステップ 12：管理サーバーへの接続の設定

管理サーバーへの接続の設定：

- **ポート**

  管理サーバーへの接続に使用するポート番号。

  既定のポート番号は 14000 です。

- **SSL ポート**

  SSL を使用して、管理サーバーへ安全に接続するために使用する Secure Sockets Layer（SSL）ポート番号。

  既定のポート番号は 13000 です。

- **暗号化鍵長**

  暗号化鍵の長さとして、1024 ビットまたは 2048 ビットを選択します。

  1024 ビットの暗号化鍵の場合は CPU の負荷が小さくなりますが、技術的仕様により信頼できる暗号化が行えないため、現在の要件に対応していないと考えられます。また、既存のハードウェアが 1024 ビットの鍵に基づく SSL 証明書に対応していないと考えられます。

  2048 ビットの暗号化鍵はすべての最新の暗号化の標準に対応しています。ただし、2048 ビットの暗号化鍵を使用すると CPU の負荷が高くなる可能性があります。

  既定では、［**2048 ビット（最高の安全性）**］が選択されています。

管理サーバーに接続するためのパラメータは、次のように後から変更することもできます。

- 管理サーバーのプロパティの［**接続ポート**］セクションで、後でポート番号と SSL ポート番号を変更することもできます。管理サーバーの接続ポートの詳細については、「Kaspersky Security Center で使用されるポート」を参照してください。

- 管理サーバー証明書を klsetsrvcert ユーティリティで置き換える時に、`-o RsaKeyLen:<鍵長>` パラメータを使用して暗号化鍵の長さを変更できます。

ステップ 13：管理サーバーアドレスの定義

次のいずれかの方法で、管理サーバーアドレスを指定します：

- **DNS ドメイン名**：この方法は、ネットワークに DNS サーバーがあり、クライアントデバイスが DNS サーバーを使用して管理サーバーアドレスを取得できる場合に使用可能です。
- **NetBIOS 名**：この方法は、クライアントデバイスが NetBIOS プロトコルを使用して管理サーバーアドレスを取得する場合、またはネットワークに WINS サーバーがある場合に使用可能です。
- **IP アドレス**：この方法は、管理サーバーに固定 IP アドレスが割り当てられている場合に使用可能です。

Kaspersky Security Center のフェールオーバークラスターのアクティブなノードに Kaspersky Security Center をインストールし、クラスターノードの準備の際にセカンダリネットワークアダプターを作成した場合は、このアダプターの IP アドレスを指定します。そうでない場合は、使用するサードパーティのロードバランサーの IP アドレスを入力します。

ステップ 14：モバイルデバイスの接続に使用する管理サーバーアドレスの指定

ウィザードのこのステップは、モバイルデバイス管理のインストールをオンにした場合のみ使用可能です。

［**モバイルデバイスとの接続に使用するアドレス**］ウィンドウで、ローカルネットワークの外部にあるモバイルデバイスへの接続に使用する管理サーバーの外部アドレスを指定します。管理サーバーの IP アドレスまたはドメイン名システム（DNS）を指定できます。

ステップ 15：アプリケーション管理プラグインの選択

Kaspersky Security Center と併せてインストールするアプリケーション管理プラグインをオンにします。

検索を簡単にするため、安全なオブジェクトの種別に応じてプラグインがグループに分割されます。

ステップ 16：ハードディスク上へのファイルの解凍とインストール

Kaspersky Security Center のインストールを設定した後に、ハードディスク上のファイルのインストールを開始できます。

インストールに追加プログラムが必要な場合は、Kaspersky Security Center のインストールが開始される前に、セットアップウィザードの［**必要項目のインストール**］ウィンドウに、通知が表示されます。［**次へ**］をクリックすると、必要なプログラムが自動的にインストールされます。

最後のウィンドウでは、どちらのコンソールで Kaspersky Security Center の使用を開始するかを選択できます。

- **MMC ベースの管理コンソールを起動**
- **Kaspersky Security Center Web コンソールの開始**

  このオプションは、ここまでのステップで Kaspersky Security Center Web コンソールのインストールを選択した場合にのみ使用できます。

また、［**終了**］をクリックして、Kaspersky Security Center の使用を開始せずにウィザードを終了することもできます。ウィザードの終了後も、いつでも使用を開始できます。

管理コンソールまたは Kaspersky Security Center Web コンソールの初回起動時に、製品の初期設定を実行することができます。

Kaspersky Security Center のフェールオーバークラスターの導入

このセクションでは、Kaspersky Security Center のフェールオーバークラスターに関する全般的な情報と、ネットワークに Kaspersky Security Center のフェールオーバークラスターを導入するための準備と導入に関する手順の両方を説明します。

シナリオ：Kaspersky Security Center のフェールオーバークラスターの導入

Kaspersky Security Center のフェールオーバークラスターは Kaspersky Security Center の高可用性を提供し、障害時の管理サーバーのダウンタイムを最小限に抑えます。フェールオーバークラスターは 2 台のコンピューターにインストールされた 2 つの同一な Kaspersky Security Center のインスタンスから構成されます。インスタンスの 1 つはアクティブノードとして、もう 1 つはパッシブノードとして動作します。アクティブノードはクライアントデバイスの保護を管理し、パッシブノードはアクティブノードの障害発生時にすべての機能を継承するよう準備されています。障害が発生した場合、パッシブノードはアクティブノードに、アクティブノードはパッシブノードになります。

必須条件

フェールオーバークラスタの要件を満たすハードウェアを持っている。

実行するステップ

カスペルスキー製品の導入シナリオは、以下の手順で進みます：

1. **Kaspersky Security Center サービス用のアカウントの作成**

   新しいドメイングループ（このシナリオではこのグループに「KLAdmins」という名前を使用します）を作成し、両方のノードおよびファイルサーバーでそのグループにローカル管理者権限を付与します。次に、2 つの新しいドメインユーザーアカウント（このシナリオではこれらのアカウントに「ksc」と「rightless」という名前を使用します）を作成し、アカウントを KLAdmins ドメイングループに追加します。

   Kaspersky Security Center をインストールするユーザーアカウントを、事前に作成した KLAdmins ドメイングループに追加します。

2. **ファイルサーバーの準備**

   Kaspersky Security Center のフェールオーバークラスターのコンポーネントとして動作するファイルサーバーを準備します。ファイルサーバーがシステム要件を満たしていることを確認して、Kaspersky Security Center のデータ用に 2 つの共有フォルダーを作成し、それらの共有フォルダーのアクセス権を設定します。

   実行手順の説明：Kaspersky Security Center のフェールオーバークラスター用のファイルサーバーの準備

3. **アクティブおよびパッシブノードの準備**

アクティブおよびパッシブノードとして動作する同一のハードウェアおよびソフトウェアを持つ 2 台のコンピューターを準備します。

実行手順の説明：Kaspersky Security Center のフェールオーバークラスター用のノードの準備

4. **DBMS（データベース管理システム）のインストール**

   サポート対象の DBMS を選択し、専用のコンピューターに DBMS をインストールします。DBMS のインストール方法については、該当製品のマニュアルを参照してください。

5. **Kaspersky Security Center のインストール**

   両方のノードのフェールオーバークラスターモードで Kaspersky Security Center をインストールします。最初にアクティブノードに Kaspersky Security Center インストールしてからパッシブノードにもインストールします。

   さらに、クラスターノードではない別のデバイスに Kaspersky Security Center Web コンソールをインストールできます。

   実行手順の説明：Kaspersky Security Center のフェールオーバークラスターノードへの Kaspersky Security Center のインストール

6. **フェールオーバークラスターのテスト**

   フェールオーバークラスターが正しく設定され、問題なく動作していることを確認してください。たとえば、アクティブノードの Kaspersky Security Center のサービス（kladminserver、klnagent、ksnproxy、klactprx または klwebsrv）のうち 1 つを停止します。サービスが停止された後、保護管理は自動的にパッシブノードに切り替わります。

結果

Kaspersky Security Center のフェールオーバークラスターが導入されます。アクティブおよびパッシブノードの切り替えが発生するイベントについてはしっかりと把握するようにしてください。

Kaspersky Security Center のフェールオーバークラスターについて

Kaspersky Security Center のフェールオーバークラスターは Kaspersky Security Center の高可用性を提供し、障害時の管理サーバーのダウンタイムを最小限に抑えます。フェールオーバークラスターは 2 台のコンピューターにインストールされた 2 つの同一な Kaspersky Security Center のインスタンスから構成されます。インスタンスの 1 つはアクティブノードとして、もう 1 つはパッシブノードとして動作します。アクティブノードはクライアントデバイスの保護を管理し、パッシブノードはアクティブノードの障害発生時にすべての機能を継承するよう準備されています。障害が発生した場合、パッシブノードはアクティブノードに、アクティブノードはパッシブノードになります。

システム要件

Kaspersky Security Center のフェールオーバークラスターを導入するには、次のハードウェアを準備する必要があります：

- 同一のハードウェアおよびソフトウェアを持つ 2 台のコンピューター。これらのコンピューターはアクティブおよびパッシブノードとして動作します。
- バージョン 2.0 以降の CIFS/SMB プロトコルをサポートするファイルサーバー。ファイルサーバーとして動作する専用のコンピューターを準備する必要があります。

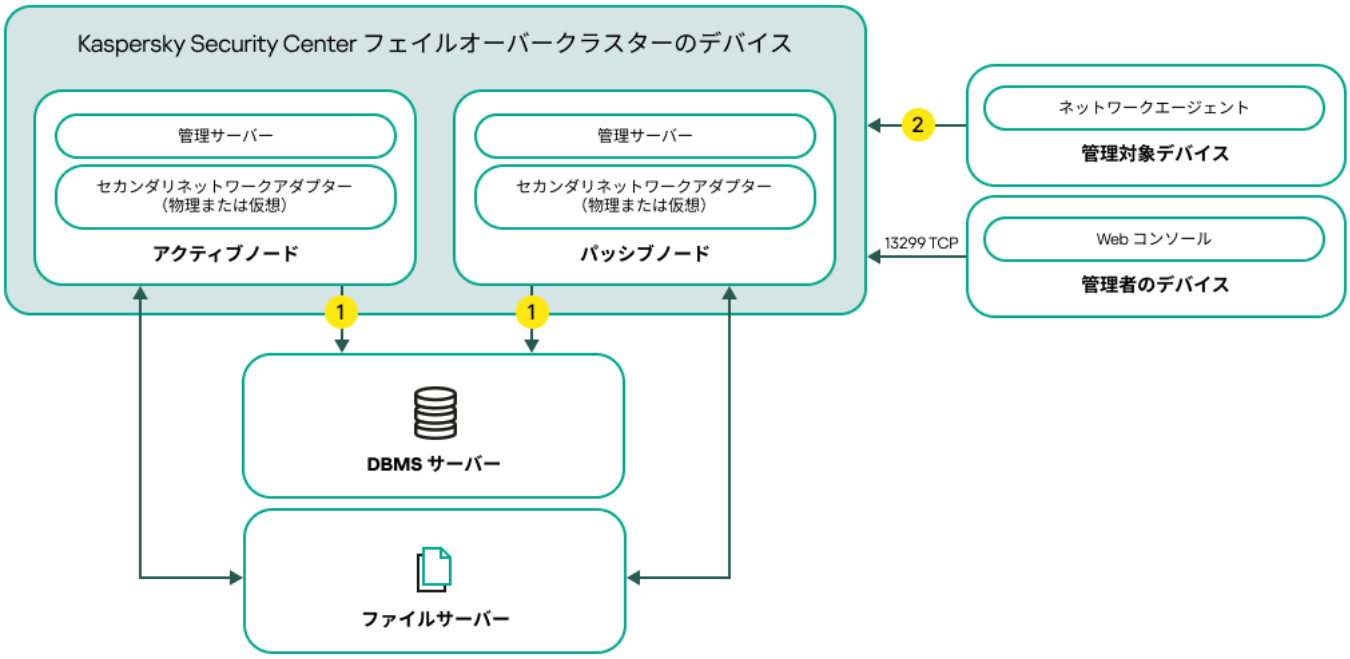
ファイルサーバーとアクティブおよびパッシブノードには高帯域幅ネットワークを使用していることを確認してください。

- DBMS（データベース管理システム）がインストールされたコンピューター。

導入スキーム

Kaspersky Security Center Linux のフェールオーバークラスターを導入するには、次のいずれかのスキームを選択できます：

- セカンダリネットワークアダプターを使用するスキーム。
- サードパーティのロードバランサーを使用するスキーム。

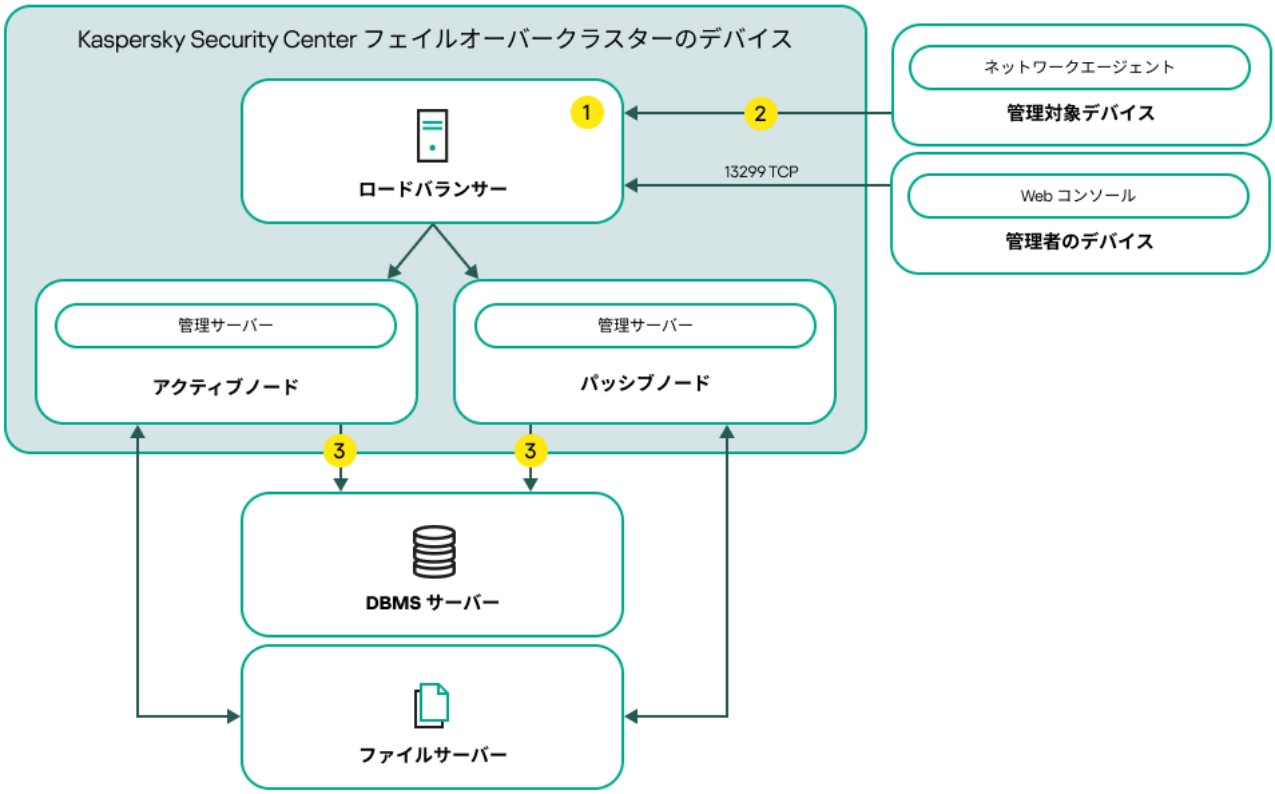


セカンダリネットワークアダプターを使用するスキーム

スキームの凡例：

1 管理サーバーがデータベースにデータを送信します。定義データベースが配置されているデバイス上で必要なポートを開きます（たとえば、MySQL サーバーの場合はポート 3306、Microsoft SQL Server の場合はポート 1433）。関連する情報については、DBMS のドキュメントを参照してください。

2 管理対象デバイスで、TCP 13000、UDP 13000、TCP 17000 の各ポートを開きます。



サードパーティのロードバランサーを使用するスキーム

スキームの凡例：

1 ロードバランサーデバイスで、管理サーバーのポートをすべて開きます：TCP 13000、UDP 13000、TCP 13291、TCP 13299 および TCP 17000。

2 管理対象デバイスで、TCP 13000、UDP 13000、TCP 17000 の各ポートを開きます。

3 管理サーバーがデータベースにデータを送信します。定義データベースが配置されているデバイス上で必要なポートを開きます（たとえば、MySQL サーバーの場合はポート 3306、Microsoft SQL Server の場合はポート 1433）。関連する情報については、DBMS のドキュメントを参照してください。

切り替えの条件

アクティブノードに次のイベントが発生した場合、フェールオーバークラスターはクライアントデバイスの保護の管理をアクティブノードからパッシブノードに切り替えます：

- ソフトウェアまたはハードウェアの障害によりアクティブノードが破損した。
- メンテナンス操作のためアクティブノードが一時的に停止した。
- Kaspersky Security Center のサービスまたはプロセスで障害が発生したかユーザーにより意図的に中断された。Kaspersky Security Center のサービスは次の通りです：kladminserver、klnagent、klactprx および klwebsrv。
- アクティブノードとファイルサーバー上の保管領域のネットワーク接続が中断または切断された。

Kaspersky Security Center のフェールオーバークラスター用のファイルサーバーの準備

Kaspersky Security Center のフェールオーバークラスタの必須コンポーネントとして動作するファイルサーバーです。

ファイルサーバーを準備するには：

1. ファイルサーバーがシステム要件を満たしていることを確認してください。

2. ファイルサーバーおよび両方のノード（アクティブおよびパッシブ）が同じドメインに含まれているか、ファイルサーバーがドメインコントローラーであることを確認してください。

3. ファイルサーバーで 2 つの共有フォルダーを作成します。2 つのうち 1 つは、フェールオーバークラスターの状態に関する情報を保持するために使用されます。別の 1 つは Kaspersky Security Center のデータおよび設定を保存するために使用されます。Kaspersky Security Center のインストールの設定時に共有フォルダーのパスを指定することになります。

4. 次のユーザーアカウントおよびグループに、作成された共有フォルダーへのフルアクセス権（共有権限および NTFS 権限の両方）を付与します：

   - ドメイングループ KLAdmins。

   - ユーザーアカウント $<ノード1> および $<ノード 2>。ここでの <ノード 1> および <ノード 2> はアクティブおよびパッシブノードのコンピューター名です。

ファイルサーバーの準備ができました。Kaspersky Security Center のフェールオーバークラスターを導入するには、シナリオの手順に従ってください。

Kaspersky Security Center のフェールオーバークラスター用のノードの準備

Kaspersky Security Center のフェールオーバークラスタのアクティブノードとパッシブノードとして動作する 2 台のコンピューターを準備します。

Kaspersky Security Center のフェールオーバークラスター向けのノードを準備するには：

1. 2 台のコンピューターがシステム要件を満たしていることを確認してください。これらのコンピューターはフェールオーバークラスターのアクティブノードおよびパッシブノードとして動作します。

2. ファイルサーバーと両方のノードが同じドメインに属していることを確認してください。

3. 次のいずれかの手順を実行します：

   - 各ノードでセカンダリネットワークアダプターを設定します。

     セカンダリネットワークアダプターは、物理的または仮想的に使用することができます。物理ネットワークアダプターを使用する場合は、標準のオペレーティングシステムツールを使用して接続し、設定してください。仮想ネットワークアダプターを使用する場合は、サードパーティ製ソフトウェアを使用して作成してください。

     次の条件を満たしていることを確認してください：

     - セカンダリネットワークアダプターが無効になっています。

       セカンダリネットワークアダプターを無効な状態で作成するか、作成後無効にすることができます。

     - 両方のノードのセカンダリネットワークアダプターは同じ IP アドレスを持っています。

- サードパーティのロードバランサーを使用している。たとえば、nginx サーバーを使用できます。この場合、次の操作を行ってください：

  a. Linux ベースで nginx がインストールされた専用のコンピューターを準備します。

  b. ロードバランシングの設定をします。アクティブノードをメインサーバー、パッシブノードをバックアップサーバーとして設定します。

  c. nginx サーバーで、管理サーバーのポートをすべて開きます： TCP 13000、UDP 13000、TCP 13291、TCP 13299 および TCP 17000。

4. 両方のノードとファイルサーバーを再起動します。

5. ファイルサーバーの準備のステップで作成した 2 つの共有フォルダーを各ノードにマップします。共有ドライブはネットワークドライブとしてマップする必要があります。2 つのフォルダーをマップする際、使用されていないドライブ文字を選択することができます。共有フォルダーにアクセスするには、シナリオのステップ 1 で作成したユーザーアカウントの資格情報を使用してください。

ノードの準備ができました。Kaspersky Security Center のフェールオーバークラスターを導入するには、シナリオの手順に従ってください。

Kaspersky Security Center のフェールオーバークラスターノードへの Kaspersky Security Center のインストール

Kaspersky Security Center は Kaspersky Security Center のフェールオーバークラスターの両方のノードに個別にインストールされます。まず最初にアクティブなノードに製品をインストールしてから、パッシブなノードにインストールします。インストール中に、どのノードがアクティブでどのノードがパッシブになるかを選択します。

すべてのノードに Kaspersky Security Center をインストールできるのは KLAdmins ドメイングループのユーザーのみです。

Kaspersky Security Center のフェールオーバークラスターのアクティブなノードに Kaspersky Security Center をインストールするには：

1. 実行ファイル ksc_15.1_<ビルド番号>_full_<ローカリゼーション言語>.exe を実行します。

   ウィンドウが開き、インストールするカスペルスキー製品の選択を要求されます。製品を選択するウィンドウで、［**Kaspersky Security Center 管理サーバーをインストールします**］をクリックし、管理サーバーのセットアップウィザードを開始します。ウィザードの指示に従ってください。

2. 使用許諾契約書とプライバシーポリシーをよく読んでください。使用許諾契約書とプライバシーポリシーのすべての条項に同意する場合、［**次の文書をすべて確認し、理解した上で条項に同意する**］セクションで、次のチェックボックスをオンにします：

   - **使用許諾契約書の諸条件**
   - **データの取り扱い方法を記載しているプライバシーポリシー**

   両方のチェックボックスをオンにすると、製品のデバイスへのインストールが続行されます。

   使用許諾契約書またはプライバシーポリシーに同意しない場合、［**キャンセル**］をクリックしてインストールを中断します。

3. アクティブなノードに製品をインストールするには［**Kaspersky Security Center フェイルオーバークラスターのプライマリノード**］を選択します。

4. ［**共有フォルダー**］ウィンドウで、次のように操作します：

   - ［**ステータス共有**］および［**データ共有**］フィールドで、準備中にファイルサーバーに作成した共有フォルダーのパスを指定します。
   - ［**ステータス共有ドライブ**］および［**データ共有ドライブ**］フィールドで、ノードの準備中に共有フォルダーをマップしたネットワークドライブを選択します。
   - クラスター接続モードを選択します：セカンダリネットワークアダプターまたはサードパーティのロードバランサー。

5. 手順 3 からカスタムインストールのその他の手順を進めます。

> 手順 13 で、クラスターノードの準備中にアダプターを作成した場合はセカンダリネットワークアダプターの IP アドレスを指定します。そうでない場合は、使用するサードパーティのロードバランサーの IP アドレスを入力します。

Kaspersky Security Center がアクティブノードにインストールされます。

Kaspersky Security Center のフェールオーバークラスターのパッシブなノードに Kaspersky Security Center をインストールするには：

1. 実行ファイル ksc_15.1_<ビルド番号>_full_<ローカリゼーション言語>.exe を実行します。

   ウィンドウが開き、インストールするカスペルスキー製品の選択を要求されます。製品を選択するウィンドウで、［**Kaspersky Security Center 管理サーバーをインストールします**］をクリックし、管理サーバーのセットアップウィザードを開始します。ウィザードの指示に従ってください。

2. 使用許諾契約書とプライバシーポリシーをよく読んでください。使用許諾契約書とプライバシーポリシーのすべての条項に同意する場合、［**次の文書をすべて確認し、理解した上で条項に同意する**］セクションで、次のチェックボックスをオンにします：

   - **使用許諾契約書の諸条件**
   - **データの取り扱い方法を記載しているプライバシーポリシー**

   両方のチェックボックスをオンにすると、製品のデバイスへのインストールが続行されます。

   使用許諾契約書またはプライバシーポリシーに同意しない場合、［**キャンセル**］をクリックしてインストールを中断します。

3. パッシブノードに本製品をインストールする場合は［**Kaspersky Security Center フェイルオーバークラスターのセカンダリノード**］を選択します。

4. ［**共有フォルダー**］の［**ステータス共有**］フィールドに、準備中にファイルサーバー上に作成した共有フォルダーのパスとクラスターの状態に関する情報を指定してください。

5. ［**インストール**］をクリックします。インストールが完了したら、［**終了**］をクリックします。

Kaspersky Security Center がパッシブノードにインストールされます。Kaspersky Security Center のフェールオーバークラスターが正しく設定され、クラスターが正しく動作するか確認するためテストできる状態になりました。

手動でのクラスターノードの開始と終了

Kaspersky Security Center のフェールオーバークラスター全体を停止したり、メンテナンスでクラスターのノードの一部を一時的に分離したりする必要がある場合があります。その場合はこのセクションの手順に従ってください。別の方法でフェールオーバークラスターに関連するサービスやプロセスを開始または停止しないでください。データを損失する可能性があります。

メンテナンス目的でのフェールオーバークラスター全体の開始および停止

フェールオーバークラスター全体を開始または停止するには：

1. アクティブノードで、<ディスク>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center に移動します。
2. コマンドラインを開いて、次のコマンドのうち1つを実行してください：
   - クラスターを停止するには、`klfoc -stopcluster --stp klfoc` を実行します。
   - クラスターを開始するには、`klfoc -startcluster --stp klfoc` を実行します。

フェールオーバークラスターは実行したコマンドに基づいて開始または停止されます。

ノードの一部のメンテナンス

ノードの一部をメンテナンスするには：

1. アクティブなノードで、コマンド「`klfoc -stopcluster --stp klfoc`」を使用してフェールオーバークラスターを停止します。
2. メンテナンス対象のノードで、<ディスク>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center に移動します。
3. コマンドラインを開き、コマンド「`detach_node.cmd`」を実行してクラスターからノードを分離します。
4. アクティブなノードで、コマンド「 `klfoc -startcluster --stp klfoc` 」を使用してフェールオーバークラスターを開始します。
5. メンテナンスを行います。
6. アクティブなノードで、コマンド「`klfoc -stopcluster --stp klfoc`」を使用してフェールオーバークラスターを停止します。
7. メンテナンスしたノードで、<ディスク>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center に移動します。
8. コマンドラインを開き、コマンド「`attach_node.cmd`」を実行してクラスターにノードを接続します。
9. アクティブなノードで、コマンド「 `klfoc -startcluster --stp klfoc` 」を使用してフェールオーバークラスターを開始します。

ノードのメンテナンスは完了し、フェールオーバークラスターに接続されます。

Windows Server のフェールオーバークラスターへの管理サーバーのインストール

フェールオーバークラスターへの管理サーバーのインストール手順には、標準の方法とスタンドアロンのインストールデバイスへのカスタムインストール方法があり、それぞれ異なります。

このセクションで説明する手順を、クラスターの共通のデータストレージがあるノードに対して実行してください。

Kaspersky Security Center 管理サーバーをクラスターにインストールするには：

ksc_<バージョン番号>.<ビルド番号>_full_<ローカリゼーション言語>.exe 実行ファイルを実行します。

ウィンドウが開き、インストールするカスペルスキー製品の選択を要求されます。製品を選択するウィンドウで、［**Kaspersky Security Center 管理サーバーをインストール**］をクリックし、管理サーバーのセットアップウィザードを開始します。ウィザードの指示に従ってください。

ステップ 1：使用許諾契約書とプライバシーポリシーの確認

セットアップウィザードのこの段階では、ユーザーとカスペルスキーとの間で締結される使用許諾契約書およびプライバシーポリシーの内容を読む必要があります。

Kaspersky Security Center 配布キットに含まれるアプリケーション管理プラグインの使用許諾契約書およびプライバシーポリシーの確認を要求される場合があります。

使用許諾契約書とプライバシーポリシーをよく読んでください。使用許諾契約書とプライバシーポリシーのすべての条件に同意する場合は、該当するチェックボックスをオンにすることで確認してください。

両方のチェックボックスをオンにすると、製品のデバイスへのインストールが続行されます。

使用許諾契約書またはプライバシーポリシーに同意しない場合、［**キャンセル**］をクリックしてインストールを中断します。

ステップ 2：クラスターへのインストール種別の選択

クラスターへのインストール種別を選択します：

- **クラスター（すべてのクラスターノードにインストール）**

  推奨されるオプションです。このオプションをオンにすると、管理サーバーがクラスターの全ノードに同時にインストールされます。

インストールする管理コンソールを選択するステップで、現在のクラスタ ノードにインストールするコンソールを選択する必要があります。クラスターノードにのみコンソールをインストールすると、ノードに障害が発生すると、管理サーバーにアクセスできなくなります。この手順では、すべてのクラスターノードにインストールする MMC ベースの管理コンソールを選択することを推奨します。管理サーバーをインストールした後、クラスターノードではない別のデバイスに Kaspersky Security Center Web コンソールをインストールします。これにより、クラスター ノードに障害が発生した場合に、Kaspersky Security Center Web Consoleを使用して管理サーバーを管理できます。

- **ローカル（このデバイスにのみインストール）**

  このオプションをオンにすると、スタンドアロンのサーバーのように、管理サーバーが現在のノードにのみインストールされます。管理サーバーは、クラスターを考慮しないアプリケーションとして動作します。たとえば、管理サーバーがフォールトトレランスを必要としない場合に、この方法を選択して共有ストレージの容量を節約できます。現在のノードで失敗した場合、別のノードの管理サーバーに管理サーバーをインストールし、管理サーバーの状態をバックアップから復旧する必要があります。

これ以降のステップは、標準、カスタムのインストール方法で共通であり、インストール方法を選択するステップから開始されます。

ステップ 3：仮想管理サーバー名の指定

新しい仮想管理サーバーのネットワーク名を指定します。指定した名前を、管理コンソールまたは Kaspersky Security Center Web コンソールの管理サーバーへの接続に使用できます。

クラスターの名前とは異なる名前を指定する必要があります。

ステップ 4：仮想管理サーバーのネットワークの詳細の設定

仮想管理サーバーのインスタンスのネットワークの詳細を指定するには：

1. ［**使用するネットワーク**］で、現在のクラスターノードの接続先であるドメインネットワークを選択します。
2. 次のいずれかの手順を実行します：
   - 選択したネットワークへの IP アドレスの割り当てに DHCP を使用する場合は、［**DHCP を使用する**］を選択します。
   - 選択したネットワークで DHCP が使用されていない場合は、必要な IP アドレスを指定します。

     クラスターの IP アドレスとは異なるアドレスを指定する必要があります。
3. ［**追加**］をクリックし、指定した設定を適用します。

自動的に割り当てられたか、または指定された IP アドレスを使用して、管理コンソールまたは Kaspersky Security Center Web コンソールを管理サーバーへ接続できます。

ステップ 5：クラスターグループの指定

クラスターグループは、全ノードに共通のリソースを含む専用のフェールオーバークラスターのロールです。次の 2 つがあります：

- クラスターグループの新規作成

  ほとんどの場合に推奨されるオプションです。新規クラスターグループにはすべての共通リソースが含まれており、管理サーバーのインスタンスと関連しています。

- 既存のクラスターグループの選択

  既存のクラスターグループに関連付けられた共通リソースを使用する場合に、このオプションを選択します。たとえば、既存のクラスターグループと関連付けられたストレージを使用する場合や、新規のクラスターグループに使用可能なストレージが他にない場合などにこのオプションを使用できます。

ステップ 6：クラスターのデータ保管領域の選択

クラスターのデータストレージを選択するには：

1. ［**使用可能なリポジトリ**］で、仮想管理サーバーのインスタンスの共通リソースがインストールされるデータストレージを選択します。
2. 選択したデータストレージに複数のボリュームが含まれている場合、［**ディスクドライブで使用可能なセクション**］から必要なボリュームを選択します。
3. ［**インストールパス**］で、仮想管理サーバーのインスタンスの共通リソースがインストールされるデータストレージのパスを入力します。

データストレージが選択されます。

ステップ 7：リモートインストール用のアカウントの指定

クラスターのパッシブノードへの仮想管理サーバーのインスタンスのリモートインストールに使用するユーザー名とパスワードを指定します。

指定するアカウントには、クラスターの全ノードの管理者権限が付与されている必要があります。

ステップ 8：インストールするコンポーネントの選択

インストールしたい Kaspersky Security Center 管理サーバーのコンポーネントを選択します：

- **モバイルデバイス管理**：Kaspersky Security Center のセットアップウィザードの実行時にモバイルデバイスのインストールパッケージを作成する必要がある場合は、このチェックボックスを選択します。管理サーバーのインストール後、管理コンソールツールを使用して、モバイルデバイス用のインストールパッケージを手動で作成することもできます。
- **SNMP エージェント**：このコンポーネントは、SNMP プロトコルを使用する管理サーバーに関する統計情報を取得します。SNMP がインストールされているデバイスにアプリケーションをインストールする場合、このコンポーネントを利用できます。

  Kaspersky Security Center のインストール後、統計情報の取得に必要な mib ファイルが、本製品のインストールフォルダーのサブフォルダー SNMP に保存されます。

ネットワークエージェントおよび管理コンソールは、コンポーネントリストには表示されません。これらのコンポーネントは自動的にインストールされ、インストールを取り消すことはできません。

このステップでは、管理サーバーのインストールフォルダーを指定する必要があります。既定では、<ドライブ名>:\Program Files\Kaspersky Lab\Kaspersky Security Center にコンポーネントがインストールされます。このフォルダーがない場合は、インストール中に自動的に作成されます。インストール先フォルダーは、［**参照**］を使用して変更できます。

ステップ 9：ネットワークの規模の選択

Kaspersky Security Center をインストールするネットワークの規模を指定します。ネットワーク上のデバイス数に応じて、ウィザードが本製品のインストールおよび本製品のインターフェイスの表示を設定します。

次の表に、ネットワークの規模に応じて調整される本製品のインストールの設定およびインターフェイスの表示の設定についてまとめています。

選択したネットワーク規模に応じたインストール設定

設定	1～100 台のデバイス	100～1000 台のデバイス	1000～5000 台のデバイス	デバイスが 5000 台以上
コンソールツリーにセカンダリ管理サーバーおよび仮想管理サーバーのノードとそれらに関連するすべての設定を表示する	なし	なし	あり	あり
サーバーおよび管理グループのプロパティウィンドウに［**セキュリティ**］セクションを表示する	なし	なし	あり	あり
クライアントデバイスでのアップデートタスクの開始時間をランダムに配分する	なし	5 分以上の間隔	10 分以上の間隔	10 分以上の間隔

管理サーバーから接続しているデータベースサーバーが MySQL 5.7 または SQL Express の場合、10,000 台を超えるデバイスを管理しないようにすることを推奨します。MariaDB のデータベース管理システムでは、推奨される最大の管理対象デバイス数は 20,000 台です。

ステップ 10：データベースの選択

ウィザードのこの手順では、管理サーバーデータベースの格納に使用する次のデータベース管理システム（DBMS）のいずれかを選択します：

- **Microsoft SQL Server または SQL Server Express**
- **MySQL または MariaDB**
- **PostgreSQL または Postgres Pro**

管理サーバーは、ドメインコントローラーではなく専用サーバーにインストールすることを推奨します。ただし、読み取り専用ドメインコントローラー（RODC）として動作するサーバーに Kaspersky Security Center をインストールする場合は、Microsoft SQL Server（SQL Express）をローカル（同じデバイス）にインストールしないでください。この場合、Microsoft SQL Server（SQL Express）と Kaspersky Security Center とは別のデバイスにインストールするか、Kaspersky Security Center と同じデバイスに DBMS をインストールする必要がある場合には MySQL、MariaDB、または PostgreSQL を使用することを推奨します。

管理サーバーのデータベース構造は、Kaspersky Security Center のインストールフォルダーにある klakdb.chm ファイルで提供しています。このファイルは、カスペルスキーポータルのアーカイブからも入手できます：klakdb.zip。

ステップ 11：SQL Server の設定

ウィザードのこの手順では、選択したデータベース管理システム（DBMS）に応じて、次の接続設定を指定します。

- 前のステップで［**Microsoft SQL Server または SQL Server Express**］を選択した場合：
  - ［**DBMS のインスタンス名**］に、ネットワーク上の SQL Server の名前を指定します。ネットワークにインストールされているすべての SQL Server のリストを表示するには、［**参照**］をクリックします。既定では、このフィールドは空白です。

    カスタムポート経由で SQL Server に接続した場合は、SQL Server ホスト名とともに、ポート番号を次のようにカンマで区切って指定します：

    ```
    SQL_Server_host_name,1433
    ```

    管理サーバーと SQL Server 間の通信を証明書によって保護する場合は、証明書の生成時に使用したのと同じホスト名を［**DBMS のインスタンス名**］に指定します。SQL Server の名前付きインスタンスを使用する場合は、SQL Server ホスト名とともに、ポート番号を次のようにカンマで区切って指定します：

    ```
    SQL_Server_name,1433
    ```

    SQL Server の複数のインスタンスを同じホスト上で使用する場合は、インスタンス名を次のようにバックスラッシュで区切って指定します：

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    企業ネットワーク上の SQL Server で Always On 機能が有効化されている場合、可用性グループのリスナーの名前を［**DBMS のインスタンス名**］で指定します。Always On 機能が有効な時、管理サーバーがサポートする可用性モードは同期コミットモードのみであることに注意してください。

  - ［**データベース名**］に、管理サーバーのデータの保管用に作成されている DBMS の名前を指定します。既定値は *KAV* です。

  この段階で、Kaspersky Security Center をインストールしているデバイスに SQL Server をインストールする場合は、インストールを中断し、SQL Server のインストール後に再開する必要があります。サポートする SQL Server のバージョンは、システム要件に一覧で掲載しています。

  リモートデバイスに SQL Server をインストールする場合は、Kaspersky Security Center のセットアップウィザードを中断する必要はありません。SQL サーバーをインストールし、Kaspersky Security Center のインストールを続けます。

- 前のステップで［**MySQL または MariaDB**］を選択した場合：
  - ［**DBMS のインスタンス名**］に、DBMS インスタンスの名前を指定します。既定では、この名前は Kaspersky Security Center をインストールするデバイスの IP アドレスです。
  - ［**ポート**］に、管理サーバーを DBMS へ接続するポートを指定します。既定のポート番号は 3306 です。
  - ［**データベース名**］に、管理サーバーのデータの保管用に作成されている DBMS の名前を指定します。既定値は *KAV* です。
- 前のステップで［**PostgreSQL または Postgres Pro**］を選択した場合：
  - ［**PostgreSQL または Postgres Pro サーバー**］に、DBMS インスタンスの名前を指定します。既定では、この名前は Kaspersky Security Center をインストールするデバイスの IP アドレスです。

- ［**ポート**］フィールドに、管理サーバーを DBMS へ接続するポートを指定します。既定のポート番号は 5432 です。

［**データベース名**］に、管理サーバーのデータの保管用に作成されている DBMS の名前を指定します。既定値は *KAV* です。

ステップ 12：認証方法の選択

管理サーバーとデータベース管理システム（DBMS）の接続時に使用される認証モードを決定します。

選択した DBMS の種別に応じて、次の認証モードから選択できます：

- SQL Express または Microsoft SQL Server の場合は、次のいずれかをオンにします：
  - **Microsoft Windows 認証モード**。権限の検証には、管理サーバーの起動に使用したアカウントが使用されます。
  - **SQL Server 認証モード**。このオプションをオンにすると、ウィンドウで指定したアカウントがアクセス権限の検証に使用されます。［**アカウント**］および［**パスワード**］に情報を入力します。

    入力したパスワードを表示するには、［**入力した文字を表示する**］をクリックしたままにします。

  どちらの認証モードでも、データベースが利用可能かどうかのチェックが行われます。データベースを使用できない場合、エラーメッセージが表示され、正しい認証情報の入力が要求されます。

  管理サーバーデータベースが別のデバイスに保存されており、管理サーバーアカウントからデータベースサーバーにアクセスできない場合は、管理サーバーのインストールまたはアップグレード時に SQL Server 認証モードを使用する必要があります。このような状況は、データベースを保管するデバイスがドメイン外にある場合、またはローカルシステムアカウントで管理サーバーがインストールされている場合に発生します。

MySQL、MariaDB、PostgreSQL、または Postgres Pro の場合は、アカウントとパスワードを指定します。

ステップ 13：管理サーバーを開始するアカウントの選択

サービスとして管理サーバーを開始する場合に使用するアカウントを選択します。

- **アカウントを自動的に作成**：kladminserver を実行する KL-AK-* という名前のアカウントを作成します。

  共有フォルダー と DBMS を管理サーバーと同じデバイスに配置する場合、このオプションを選択します。

- **アカウントの選択**：管理サーバーのサービス（kladminserver）は選択したアカウントで実行されます。

  次のような場合は、ドメインアカウントを選択する必要があります：別のデバイスにある SQL Server（SQL Express を含む） を DBMS として使用する場合、または共有フォルダーを別のデバイスに配置する場合。

  Kaspersky Security Center は、管理対象サービスアカウント（MSA）とグループ管理対象サービスアカウント（gMSA）をサポートしています。これらの種別のアカウントをドメインで使用している場合は、それらの 1 つを管理サーバーのサービス用のアカウントとして選択できます。

MSA または gMSA を指定する前に、管理サーバーをインストールするのと同じデバイスにアカウントをインストールする必要があります。アカウントがまだインストールされていない場合は、管理サーバーのインストールをキャンセルし、アカウントをインストールしてから管理サーバーのインストールを再開してください。ローカルデバイスへの管理対象サービスアカウントのインストールの詳細は、Microsoft 公式ドキュメントを参照してください。

MSA または gMSA を指定するには：

1. ［**参照**］をクリックします。
2. ウィンドウが表示されたら、［**オブジェクト種別**］をクリックします。
3. ［**サービスのアカウント**］の種別を選択して、［**OK**］をクリックします。
4. 関連するアカウントを選択して［**OK**］をクリックします。

選択したアカウントは、使用する DBMS に応じた権限を持っている必要があります。

セキュリティ上の理由から、管理サーバーを実行するアカウントには特権ステータスを割り当てないでください。

後で管理サーバーのアカウントを変更する場合は、管理サーバーのアカウントを切り替えるユーティリティ（klsrvswch）を使用する必要があります。管理サーバーのインストールに使用した管理者権限を持つアカウントで、管理サーバーデバイス上で klsrvswch ユーティリティを起動する必要があることに注意してください。

ステップ 14：Kaspersky Security Center のサービスを実行するために使用するアカウントの選択

Kaspersky Security Center のサービスをこのデバイスで実行する場合のアカウントを選択します：

- **アカウントを自動的に作成**：Kaspersky Security Center が kladmins グループ内のこのデバイス上に KlScSvc という名前のローカルアカウントを作成します。作成したアカウントで Kaspersky Security Center のサービスが実行されます。
- **アカウントの選択**：選択したアカウントで Kaspersky Security Center のサービスが実行されます。

  レポートの保存先に別のデバイス内のフォルダーを指定する場合や、企業のセキュリティポリシーで定められている場合などには、ドメインアカウントを選択する必要があります。また、フェールオーバークラスターに管理サーバーをインストールする場合も、ドメインアカウントを選択する必要があります。

セキュリティ上の理由により、サービスを実行しているアカウントには権限ステータスを付与しないでください。

KSN プロキシサービス（ksnproxy）、カスペルスキーアクティベーションプロキシサービス（klactprx）、カスペルスキー認証ポータルサービス（klwebsrv）は、選択したアカウントで実行されます。

ステップ 15：共有フォルダーの選択

次の目的で使用する共有フォルダーの場所と名前を定義します：

- アプリケーションのリモートインストールに必要なファイルを保管する（ファイルは、インストールパッケージの作成時に管理サーバーへコピーされます）
- アップデート元から管理サーバーにダウンロードされたアップデートを保管する

ファイル共有（読み取り専用）はすべてのユーザーで有効になります。

次のオプションからいずれかをオンにできます：

- **共有フォルダーの作成**：フォルダーを新規作成します。テキストボックスにフォルダーへのパスを指定します。
- **既存共有フォルダーの選択**：既に作成されている共有フォルダーを選択します。

共有フォルダーとして選択できるのは、インストールを実行しているデバイス上のローカルフォルダー、または企業ネットワーク内の任意のクライアントデバイス上にあるリモートディレクトリです。［**参照**］を使用して共有フォルダーを選択するか、共有フォルダーの UNC パス（「\\server\Share」など）を該当フィールドに入力して手動で指定します。

既定では、Kaspersky Security Center のインストール先として指定したフォルダー内にローカルサブフォルダー Share が作成されます。

必要に応じて、後で共有フォルダーを定義できます。

ステップ 16：管理サーバーへの接続の設定

管理サーバーへの接続の設定：

- **ポート**

  管理サーバーへの接続に使用するポート番号。

  既定のポート番号は 14000 です。

- **SSL ポート**

  SSL を使用して、管理サーバーへ安全に接続するために使用する Secure Sockets Layer（SSL）ポート番号。

  既定のポート番号は 13000 です。

- **暗号化鍵長**

  暗号化鍵の長さとして、1024 ビットまたは 2048 ビットを選択します。

  1024 ビットの暗号化鍵の場合は CPU の負荷が小さくなりますが、技術的仕様により信頼できる暗号化が行えないため、現在の要件に対応していないと考えられます。また、既存のハードウェアが 1024 ビットの鍵に基づく SSL 証明書に対応していないと考えられます。

  2048 ビットの暗号化鍵はすべての最新の暗号化の標準に対応しています。ただし、2048 ビットの暗号化鍵を使用すると CPU の負荷が高くなる可能性があります。

  既定では、［**2048 ビット（最高の安全性）**］が選択されています。

管理サーバーに接続するためのパラメータは、次のように後から変更することもできます。

- 管理サーバーのプロパティの［**接続ポート**］セクションで、後でポート番号と SSL ポート番号を変更することもできます。管理サーバーの接続ポートの詳細については、「Kaspersky Security Center で使用されるポート」を参照してください。
- 管理サーバー証明書を klsetsrvcert ユーティリティで置き換える時に、 `-o RsaKeyLen:<` 鍵長 `>` パラメータを使用して暗号化鍵の長さを変更できます。

ステップ 17：管理サーバーアドレスの定義

管理サーバーアドレスを定義します。次の中からいずれかを選択できます：

- **DNS ドメイン名**：この方法は、ネットワークに DNS サーバーがあり、クライアントデバイスが DNS サーバーを使用して管理サーバーアドレスを取得できる場合に使用可能です。
- **NetBIOS 名**：この方法は、クライアントデバイスが NetBIOS プロトコルを使用して管理サーバーアドレスを取得する場合、またはネットワークに WINS サーバーがある場合に使用可能です。
- **IP アドレス**：この方法は、管理サーバーに固定 IP アドレスが割り当てられている場合に使用可能です。

ステップ 18：モバイルデバイスの接続に使用する管理サーバーアドレスの指定

ウィザードのこのステップは、モバイルデバイス管理のインストールをオンにした場合のみ使用可能です。

［**モバイルデバイスとの接続に使用するアドレス**］ウィンドウで、ローカルネットワークの外部にあるモバイルデバイスへの接続に使用する管理サーバーの外部アドレスを指定します。管理サーバーの IP アドレスまたはドメイン名システム（DNS）を指定できます。

ステップ 19：ハードディスク上へのファイルの解凍とインストール

Kaspersky Security Center のインストールを設定した後に、ハードディスク上のファイルのインストールを開始できます。

インストールに追加プログラムが必要な場合は、Kaspersky Security Center のインストールが開始される前に、セットアップウィザードの［**必要項目のインストール**］ウィンドウに、通知が表示されます。［**次へ**］をクリックすると、必要なプログラムが自動的にインストールされます。

最後のウィンドウでは、どちらのコンソールで Kaspersky Security Center の使用を開始するかを選択できます。

- **MMC ベースの管理コンソールを起動**
- **Kaspersky Security Center Web コンソールの開始**

このオプションは、ここまでのステップで Kaspersky Security Center Web コンソールのインストールを選択した場合にのみ使用できます。

また、［**終了**］をクリックして、Kaspersky Security Center の使用を開始せずにウィザードを終了することもできます。ウィザードの終了後も、いつでも使用を開始できます。

管理コンソールまたは Kaspersky Security Center Web コンソールの初回起動時に、製品の初期設定を実行することができます。

サイレントモードでの管理サーバーのインストール

管理サーバーは、サイレントモード、つまりインストール設定を対話的に入力することなくインストールすることができます。

ローカルデバイスにサイレントモードで管理サーバーをインストールするには：

1. 使用許諾契約書をお読みください。以下のコマンドは、使用許諾契約書の内容を理解して条項に同意する場合にのみ使用してください。

2. プライバシーポリシーをお読みください。以下のコマンドは、プライバシーポリシーに従ってデータが処理されて送信されること（第三国への送信を含む）を理解し、同意する場合にのみ使用してください。

3. 次のコマンドを実行します：
   `setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <セットアップパラメータ>"`

ここで、<セットアップパラメータ> には、パラメータとその対応する値をスペースで区切って指定します（例：`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`）。Setup.exe ファイルは Server フォルダーにあり、これは Kaspersky Security Center 配布キットに含まれています。

管理サーバーをサイレントモードでインストールする時に使用できるパラメータの名前とその値を下の表に示します。

サイレントモードでの管理サーバーのインストールのパラメータ

パラメータ名	パラメータの説明	設定可能な値
EULA	使用許諾契約書の条項の同意。	• 1 – 使用許諾契約書の内容をすべて確認し、理解した上で条項に同 • その他の値または値なし – 使用許諾契約書に同意しません（イン
PRIVACYPOLICY	プライバシーポリシーの条項の同意。	• 1 – プライバシーポリシーに従ってデータが処理されて送信される理解しました。プライバシーポリシーの内容をすべて確認し、理 • その他の値または値なし – プライバシーポリシーの条項に同意しません）。
INSTALLATIONMODETYPE	管理サーバーのインストールの種別	• Standard – 標準インストール • Custom – カスタムインストール
INSTALLDIR	管理サーバーのインストールフォルダーへのパス	文字列値
ADDLOCAL	インストールする管理サーバーのコンポーネントのリスト（カンマで区切ります）	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86 管理サーバーの適切なインストールに最小限必要なコンポーネントは

		ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC100_CRT_x86
NETRANGETYPE	ネットワークの規模（ネットワーク上のデバイスの台数）	• NRT_1_100：デバイスが 1 ～ 100 台 • NRT_100_1000：デバイスが 101 ～ 1000 台 • NRT_GREATER_1000：デバイスが 1000 台以上
SRV_ACCOUNT_TYPE	管理サーバーをサービスとして実行するアカウントを指定するモード	• SrvAccountDefault – アカウントを自動的に作成する。 • SrvAccountUser – アカウントを手動で指定する。この場合は、S SERVERACCOUNTPWD パラメータの値を指定する必要があります。
SERVERACCOUNTNAME	管理サーバーをサービスとして実行するアカウントの名前。SRV_ACCOUNT_TYPE=SrvAccountUser の場合は、パラメータの値を指定する必要があります。	文字列値
SERVERACCOUNTPWD	サービスとして管理サーバーを開始する場合に使用するアカウントのパスワード。SRV_ACCOUNT_TYPE=SrvAccountUser の場合は、パラメータの値を指定する必要があります。	文字列値
SERVERCER	管理サーバー証明書の鍵のサイズ（ビット）	• 1 – 管理サーバー証明書の鍵のサイズは 2,048 ビット • 値なし – 管理サーバー証明書の鍵のサイズは 1024 ビット
DBTYPE	管理サーバーのデータベースを保管するために使用されるデータベースの種別 このパラメータは必須です。	• MySQL – MySQL データベースまたは MariaDB データベースを使 MYSQLSERVERNAME、 MYSQLSERVERPORT、 MYSQLDBNAME、 MYSQL MYSQLACCOUNTPWD パラメータの値を指定する必要があります。 • MSSQL – Microsoft SQL Server (SQL Express) データベースを使用 MSSQLSERVERNAME、 MSSQLDBNAME および MSSQLAUTHTYPE パラ す。 • POSTGRES – PostgreSQL または Postgres Pro データベースを使用 POSTGRESSERVERNAME、 POSTGRESSERVERPORT、 POSTGRESDBNA び POSTGRESACCOUNTPWD パラメータの値を指定する必要があり
MYSQLSERVERNAME	SQL サーバーの名前。DBTYPE=MySQL の場合は、パラメータの値を指定する必要があります。	文字列値
MYSQLSERVERPORT	SQL サーバーに接続するためのポートの番号。DBTYPE=MySQL の場合は、パラメータの値を指定する必要があります。	数値
MYSQLDBNAME	管理サーバーのデータを保管するために作成されるデータベースの名前。DBTYPE=MySQL の場合は、パラメータの値を指定する必要があります。	文字列値
MYSQLACCOUNTNAME	データベースに接続するためのアカウントの名前。DBTYPE=MySQL の場合は、パラメータの値を指定する必要があります。	文字列値
MYSQLACCOUNTPWD	データベースに接続するためのアカウントのパスワード。DBTYPE=MySQL の場合は、パラメータの値を指定する必要があります。	文字列値
MSSQLSERVERNAME	SQL サーバーの名前。DBTYPE=MSSQL の場合は、パラメータの値を指定する必要があります。	文字列値
MSSQLDBNAME	データベースの名前。DBTYPE=MSSQL の場合は、パラメータの値を指定する	文字列値

	必要があります。	
MSSQLAUTHTYPE	SQL サーバーへの接続時の認証方法。DBTYPE=MSSQL の場合は、パラメータの値を指定する必要があります。	• Windows – Microsoft Windows 認証モード。 • SQLServer – SQL サーバー認証モード。この場合は、MSSQLACCO MSSQLACCOUNTPWD パラメータの値を指定する必要があります。
MSSQLACCOUNTNAME	SQL サーバーに接続するためのアカウントの名前。MSSQLAUTHTYPE=SQLServer の場合は、パラメータの値を指定する必要があります。	文字列値
MSSQLACCOUNTPWD	SQL サーバーに接続するためのアカウントのパスワード。MSSQLAUTHTYPE=SQLServer の場合は、パラメータの値を指定する必要があります。	文字列値
CREATE_SHARE_TYPE	共有フォルダーを指定する方法	• Create – 新しい共有フォルダーを作成する。この場合は、SHARE SHAREFOLDERNAME パラメータの値を指定する必要があります。 • ChooseExisting – 既存のフォルダーを選択します。この場合は、タの値を指定する必要があります。
SHARELOCALPATH	ローカルフォルダーの完全パス。次の場合は、パラメータの値を指定する必要があります： CREATE_SHARE_TYPE=Create	文字列値
SHAREFOLDERNAME	共有フォルダーのネットワーク名。CREATE_SHARE_TYPE=Create の場合は、パラメータの値を指定する必要があります。	文字列値
EXISTSHAREFOLDERNAME	既存の共有フォルダーの完全パス。 CREATE_SHARE_TYPE=ChooseExisting の場合は、パラメータの値を指定する必要があります。	文字列値
SERVERPORT	管理サーバーに接続するためのポート番号	数値
SERVERSSLPORT	SSL プロトコルを使用した管理サーバーへの暗号化接続用ポートの番号。	数値
SERVERADDRESS	管理サーバーアドレス	文字列値
MOBILESERVERADDRESS	モバイルデバイスの接続に使用する管理サーバーのアドレス。	文字列値

管理サーバーのセットアップパラメータの詳細については、「カスタムインストール」セクションを参照してください。

管理者ワークステーションへの管理コンソールのインストール

管理コンソールは管理コンピューターに別途インストールし、このコンソールを使用してネットワーク上で管理サーバーを管理することもできます。

管理者ワークステーションに管理コンソールをインストールするには：

1. 実行ファイル setup.exe を実行します。
   ウィンドウが開き、インストールするカスペルスキー製品の選択を要求されます。

2. 製品を選択するウィンドウで、［**Kaspersky Security Center 管理コンソールのみのインストール**］をクリックし、管理コンソールのセットアップウィザードを開始します。ウィザードの指示に従ってください。

3. インストール先フォルダーを選択します。既定のインストール先は、<ドライブ名>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console です。このフォルダーがない場合は、インストール中に自動的に作成されます。インストール先フォルダーは、［**参照**］を使用して変更できます。

4. セットアップウィザードの最終ページで、［**インストール**］をクリックして管理コンソールのインストールを開始します。

ウィザードが完了すると、管理コンピューターに管理コンソールがインストールされます。

管理コンソールを管理者のワークステーションにサイレントモードでインストールするには：

1. 使用許諾契約書をお読みください。以下のコマンドは、使用許諾契約書の内容を理解して条項に同意する場合にのみ使用してください。

2. Kaspersky Security Center 配布キットの［`Distrib\Console`］フォルダーで、次のコマンドを使用して setup.exe ファイルを実行します：

   ```
   setup.exe /s /v"EULA=1"
   ```

   ［`Distrib\Console\Plugins`］フォルダーからすべての管理プラグインを管理コンソールとともにインストールする場合は、次のコマンドを実行します：

   ```
   setup.exe /s /v"EULA=1" /pALL
   ```

   ［`Distrib\Console\Plugins`］フォルダーから管理コンソールとともにインストールする管理プラグインを指定する場合は、「/p」キーの後にプラグインを指定し、セミコロンで区切ります：

   ```
   setup.exe /s /v"EULA=1" /pP1;P2;P3
   ```

   `P1`、`P2`、`P3` は、［`Distrib\Console\Plugins`］フォルダー内のプラグインフォルダー名に対応するプラグイン名です。例：

   ```
   setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
   ```

管理コンソールと管理プラグイン（存在する場合）が、管理者のワークステーションにインストールされます。

管理コンソールのインストール後に、管理サーバーに接続してください。接続するには、管理コンソールを起動します。起動後に開くウィンドウで、管理サーバーがインストールされたデバイスの名前または IP アドレスを指定します。また、接続に使用するアカウントも、このウィンドウで設定します。管理サーバーへの接続が確立されると、この管理コンソールを使用してアンチウイルスを管理できます。

管理コンソールは、標準の Microsoft Windows 削除 / 追加ツールで削除できます。

Kaspersky Security Center のインストール後のシステムの変更

管理コンソールのアイコン

管理コンソールがデバイスにインストールされると、アイコンが表示され、ここから管理コンソールを起動できるようになります。管理コンソールは［**スタート**］→［**プログラム**］→［**Kaspersky Security Center**］メニューにあります。

管理サーバーとネットワークエージェントのサービス

管理サーバーとネットワークエージェントは、次に示すプロパティを持つサービスとしてデバイスにインストールされます。この表には、管理サーバーインストール後にデバイスに適用される他のサービスの属性も示します。

Kaspersky Security Center のサービスのプロパティ

コンポーネント	サービス名	表示されるサービス名	アカウント
管理サーバー	kladminserver	Kaspersky Security Center 管理サーバー	インストール中に作成されたユーザー定義アカウントまたは KL-AK-* フォーマットの非特権専用アカウント
ネットワークエージェント	klnagent	Kaspersky Security Center ネットワークエージェント	ローカルシステム
Kaspersky Security Center Web コンソールにアクセスし、組織イントラネットを管理するための Web サーバー	klwebsrv	カスペルスキーの Web サーバー	特権のない専用の KlScSvc アカウント
アクティベーションプロキシサーバー	klactprx	カスペルスキーのアクティベーションプロキシサーバー	特権のない専用の KlScSvc アカウント
KSN プロキシサーバー	ksnproxy	Kaspersky Security Network プロキシサーバー	特権のない専用の KlScSvc アカウント

Kaspersky Security Center を Kaspersky Security Center のフェールオーバークラスターノードにインストールする時、「klfocsvc_klfoc」サービスが使用可能になります。「klnagent_klfoc」サービスと「klfocsvc_klfoc」サービスは、ローカルシステムアカウントで実行されます。「kladminserver_klfoc」サービスは「ksc」アカウントで実行する必要があり、他のサービスは「rightless」アカウントで実行する必要があります。「ksc」および「rightless」アカウントは、ローカル管理者権限を持つ「KLAdmins」グループに追加する必要があります。Kaspersky Security Center が正しく動作するには、サービスの実行に「ksc」アカウントと「rightless」アカウントのみを使用する必要があります。同じ権限を持つ他のアカウントを使用することは推奨しません。以下の表には、管理サーバーが Kaspersky Security Center のフェールオーバークラスターにインストールされた後にデバイスに適用されるサービスのプロパティが含まれています。

カスペルスキーのフェールオーバークラスターにインストールされている Kaspersky Security Center のサービスのプロパティ

コンポーネント	サービス名	表示されるサービス名	アカウント
管理サーバー	kladminserver_klfoc	Kaspersky Security Center 管理サーバー	ksc
ネットワークエージェント	klnagent_klfoc	Kaspersky Security Center ネットワークエージェント	ローカルシステム
Kaspersky Security Center Web コンソールにアクセスし、組織イントラネットを管理するための Web サーバー	klwebsrv_klfoc	カスペルスキーの Web サーバー	rightless
アクティベーションプロキシサーバー	klactprx_klfoc	カスペルスキーのアクティベーションプロキシサーバー	rightless
KSN プロキシサーバー	ksnproxy_klfoc	Kaspersky Security Network プロキシサーバー	rightless
カスペルスキーのフェールオーバークラスター	klfocsvc_klfoc	カスペルスキーのフェールオーバークラスター	ローカルシステム

Kaspersky Security Center Web コンソールサービス

Kaspersky Security Center Web コンソールをデバイスにインストールすると、次のサービスが導入されます（次の表を参照）：

Kaspersky Security Center Web コンソールサービス

表示されるサービス名	アカウント

Kaspersky Security Center サービス Web コンソール	NT Service/KSCSvcWebConsole
Kaspersky Security Center Web コンソール	ネットワークサービス
Kaspersky Security Center 製品プラグインサーバー	NT Service/KSCWebConsolePlugin
Kaspersky Security Center Web コンソール管理サービス	ローカルシステム
Kaspersky Security Center Web コンソールメッセージキュー	NT Service/KSCWebConsoleMessageQueue

ネットワークエージェントのサーバーのバージョン

サーバー向けネットワークエージェントは、管理サーバーとともにデバイスにインストールされます。サーバー向けネットワークエージェントは、管理サーバーの一部としてインストールされ、管理サーバーとともに削除されます。また、ローカルにインストールされた管理サーバーだけと連携します。ネットワークエージェントを管理サーバーに接続する設定は必要ありません。コンポーネントは同じデバイスにインストールされるので、設定はプログラムに実装されています。サーバー向けネットワークエージェントは、標準のネットワークエージェントと同じプロパティでインストールされ、同じアプリケーション管理機能を実行します。このネットワークエージェントは、管理サーバーのクライアントデバイスを含む管理グループのポリシーにより管理されます。ネットワークエージェントのサーバーバージョンでは、サーバー変更以外の全タスクは管理サーバー用タスク領域で作成されます。

既に管理サーバーがインストールされているデバイスには、ネットワークエージェントをインストールできません。

Microsoft Windows の標準管理ツール（コンピューターの管理 / サービス）を使用して、管理サーバーおよびネットワークエージェントの各サービスのプロパティの確認や動作の監視が可能です。管理サーバーのサービスの動作に関する情報は Microsoft Windows システムログに登録および保管されます。これは、管理サーバーがインストールされているデバイスのシステムログの中で、カスペルスキーのイベントログとは別の区分になります。

サービスの開始または停止を手動で行うことは避けてください。また、サービスの設定内のサービスアカウントはできるだけ変更しないでください。必要な場合、klsrvswch ユーティリティを使用して管理サーバーのサービスアカウントを編集できます。管理サーバーのインストールに使用した管理者権限を持つアカウントで、管理サーバーデバイス上で klsrvswch ユーティリティを起動する必要があることに注意してください。

ユーザーアカウントとセキュリティグループ

既定では、次のアカウントが管理サーバーのインストーラーによって作成されます：

- KL-AK-*：管理サーバーのサービスアカウント
- KlScSvc：管理サーバープールにある他のサービス用のアカウント
- KlPxeUser：オペレーティングシステムの導入用アカウント

インストーラーの実行中に、管理サーバーのサービスと他のサービス用に他のアカウントを選択した場合、指定されたアカウントが使用されます。

また、各グループの権限のセットと共に、KLAdmins および KLOperators というローカルセキュリティグループが管理サーバーがインストールされているデバイスに自動的に作成されます。

ドメインコントローラーへのインストールは推奨されません。ドメインコントローラーに管理サーバーをインストールする場合は、ドメイン管理者権限でインストーラーを起動する必要があります。この場合、インストーラーは KLAdmins と KLOperators という名前のドメインセキュリティグループを自動的に作成します。ドメインコントローラーではないコンピューターに管理サーバーをインストールする場合は、代わりにローカル管理者権限でインストーラーを起動する必要があります。この場合、インストーラーは KLAdmins と KLOperators という名前のローカルセキュリティグループを自動的に作成します。

メール通知の設定時に、メールサーバー上に ESMTP 認証目的のアカウントを作成する必要がある場合があります。

製品の削除

Kaspersky Security Center は、標準の Microsoft Windows 削除 / 追加ツールで削除できます。製品を削除するには、プラグインも含めてすべてのコンポーネントをデバイスから削除するウィザードを起動する必要があります。ウィザードにより、既定のブラウザーで Web ページが開かれ、Kaspersky Security Center の使用を停止した理由を項目から選択できます。ウィザードの操作中に共有フォルダー（Share）の削除をオンにしなかった場合は、関連するすべてのタスクの完了後に、手動で削除できます。

アプリケーションの削除後、そのアプリケーションのファイルのいくつかはシステムの一次フォルダーに残ることがあります。

製品の削除タスク作成ウィザードに、管理サーバーのバックアップコピーの保存を促すメッセージが表示されます。

アプリケーションを Microsoft Windows 7 および Microsoft Windows 2008 から削除すると、製品の削除タスク作成ウィザードが突然終了する場合があります。オペレーティングシステムのユーザーアカウント制御（UAC）を無効にして製品の削除を再開すると、この問題を回避できます。

Kaspersky Security Center のアップグレードについて

このセクションでは、以前のバージョンの Kaspersky Security Center をアップグレードする方法について説明します。Kaspersky Security Center がローカルにインストールされたか、Kaspersky Security Center のフェールオーバークラスターのノードにインストールされたかによって Kaspersky Security Center のアップグレード方法が異なります。

アップグレード中、管理サーバーと別のアプリケーションで同時に DBMS を使用することは厳重に禁じられています。

管理サーバーをバージョン 15.1 にアップグレードすると、ネットワークエージェントバージョン 15 以前の新しいインストールパッケージを作成できなくなることに注意してください。ただし、以前に作成されたインストールパッケージは利用できます。

Kaspersky Security Center を旧バージョンからアップグレードすると、サポート対象のカスペルスキー製品のインストール済みプラグインはすべて残ります。管理サーバープラグインとネットワークエージェントプラグインは自動的にアップグレードされます（管理コンソールおよび Kaspersky Security Center Web コンソール）。

以前のバージョンの Kaspersky Security Center からのアップグレード

次のトピックでは、アップグレードの推奨される準備手順について説明します：Kaspersky Security Center と管理対象セキュリティ製品のアップグレード.

管理サーバーのバージョン 15.1 をそれより前のバージョンの管理サーバー（バージョン 11（11.0.0.1131b）以降）がインストールされたデバイスにインストールすることができます。バージョン 15.1 にアップグレードすると、以前のバージョンの管理サーバーのデータと設定がすべて維持されます。

管理サーバーのインストール中に問題が発生した場合は、アップグレード操作の前に作成した管理サーバーデータのバックアップコピーを使用して管理サーバーを前のバージョンに戻すことが可能です。

ネットワーク上に少なくとも 1 つの新しいバージョンの管理サーバーがインストールされている場合は、その管理サーバーのインストールパッケージを使用するリモートインストールタスクを使用して、ネットワーク上の他の管理サーバーをアップグレードできます。

Kaspersky Security Center のフェールオーバークラスターを導入していた場合、ノード上の Kaspersky Security Center をアップグレードすることもできます。

旧バージョンの管理サーバーをバージョン 15.1 にアップグレードするには：

1. バージョン 15.1 向けの ksc_15.1_<ビルド番号>_full_<言語>.exe ファイルを実行します（このファイルはカスペルスキーの Web サイトからダウンロードできます）。

2. 製品を選択するウィンドウで、［**Kaspersky Security Center のインストール**］をクリックし、管理サーバーのセットアップウィザードを開始します。ウィザードの指示に従ってください。

3. 使用許諾契約書とプライバシーポリシーを読みます。使用許諾契約書とプライバシーポリシーのすべての条項に同意する場合、［**次の文書をすべて確認し、理解した上で条項に同意する**］セクションで、次のチェックボックスをオンにします：

   - **使用許諾契約書の諸条件**
   - **データの取り扱い方法を記載しているプライバシーポリシー**

   両方のチェックボックスをオンにすると、製品のデバイスへのインストールが続行されます。以前のバージョンの管理サーバーのデータのバックアップコピーの作成を促されます。

   Kaspersky Security Center は、旧バージョンを使用して作成した管理サーバーのバックアップコピーからのデータ復元をサポートします。

4. 管理サーバーのデータのバックアップを作成する場合は、表示される［**管理サーバーデータのバックアップ**］でデータを指定します。

   klbackup ユーティリティによりバックアップが作成されます。このユーティリティは配布キットに含まれており、Kaspersky Security Center インストールフォルダーのルートにあります。

5. セットアップウィザードに従って、バージョン 15.1 の管理サーバーをインストールします。

Kaspersky Security Center Web コンソールのサービスがビジー状態であるメッセージが表示された場合は、ウィザードで［**無視**］をクリックします。

セットアップウィザードは途中で終了しないことを推奨します。管理サーバーのインストールの途中でアップグレードを中止すると、アップグレードしたバージョンの Kaspersky Security Center が動作不能になる場合があります。

6. 旧バージョンのネットワークエージェントがインストールされているデバイスの場合は、新バージョンのネットワークエージェントのリモートインストールタスクを作成して実行します。

Network Agent for Linux を Kaspersky Security Center と同じバージョンにアップグレードすることを推奨します。

リモートインストールタスクが完了すると、ネットワークエージェントのバージョンがアップグレードされます。

Kaspersky Security Center のフェールオーバークラスターノードの Kaspersky Security Center のアップグレード

以前のバージョン（バージョン 13.2 以降）の管理サーバーがインストールされている Kaspersky Security Center のフェールオーバークラスターノードのすべてにバージョン 15.1 の管理サーバーをインストールすることができます。バージョン 15.1 にアップグレードすると、以前のバージョンの管理サーバーのデータと設定がすべて維持されます。

以前デバイスにローカルで Kaspersky Security Center をインストールしていた場合は、これらのデバイス上で Kaspersky Security Center をアップグレードすることができます。

Kaspersky Security Center のフェールオーバークラスターノードの Kaspersky Security Center をアップグレードするには：

1. クラスターのアクティブなノードで以下の操作を実行します：

   a. 実行ファイル ksc_15.1_<ビルド番号>_full_<ローカリゼーション言語>.exe を実行します。

   ウィンドウが開き、アップグレードするカスペルスキー製品の選択を要求されます。［**Kaspersky Security Center 管理サーバーをインストールします**］をクリックし、管理サーバーのセットアップウィザードを開始します。ウィザードの指示に従ってください。

   b. 使用許諾契約書とプライバシーポリシーを読みます。使用許諾契約書とプライバシーポリシーのすべての条項に同意する場合、［**次の文書をすべて確認し、理解した上で条項に同意する**］セクションで、次のチェックボックスをオンにします：

   - **使用許諾契約書の諸条件**
   - **データの取り扱い方法を記載しているプライバシーポリシー**

   インストールを続行するには、両方のチェックボックスをオンにします。

   使用許諾契約書またはプライバシーポリシーに同意しない場合は、［**キャンセル**］をクリックしてアップグレードをキャンセルします。

2. Kaspersky Security Center のフェールオーバークラスターのパッシブノードで、アクティブノードと同じ操作を実行します。

3. クラスターを開始します。

この結果、Kaspersky Security Center のフェールオーバークラスターのノードに最新版の管理サーバーがインストールされました。

Microsoft フェールオーバークラスターノードの Kaspersky Security Center のアップグレード

以前のバージョン（バージョン 13.2 以降）の管理サーバーがインストールされている Microsoft のフェールオーバークラスターノードのすべてにバージョン 15.1 の管理サーバーをアップグレードすることができます。バージョン 15.1 にアップグレードすると、以前のバージョンの管理サーバーのデータと設定がすべて維持されます。

Microsoft のフェールオーバークラスターノードの Kaspersky Security Center をアップグレードするには：

1. クラスターの任意のノードで以下の操作を実行します：

   a. 実行ファイル ksc_15.1_<ビルド番号>_full_<ローカリゼーション言語>.exe を実行します。

   ウィンドウが開き、アップグレードするカスペルスキー製品の選択を要求されます。［**Kaspersky Security Center 管理サーバーをインストールします**］をクリックし、管理サーバーのセットアップウィザードを開始します。ウィザードの指示に従ってください。

   b. 使用許諾契約書とプライバシーポリシーを読みます。使用許諾契約書とプライバシーポリシーのすべての条項に同意する場合、［**次の文書をすべて確認し、理解した上で条項に同意する**］セクションで、次のチェックボックスをオンにします：

   - **使用許諾契約書の諸条件**
   - **データの取り扱い方法を記載しているプライバシーポリシー**

   インストールを続行するには、両方のチェックボックスをオンにします。

   使用許諾契約書またはプライバシーポリシーに同意しない場合は、［**キャンセル**］をクリックしてアップグレードをキャンセルします。

   c. ［**クラスター上のインストール種別**］ウィンドウで、［**クラスター（すべてのクラスターノードにインストール）**］を選択します。

   次に、インストーラーはクラスターのすべてのノードで管理サーバーを構成し、アップグレードを完了します。アップグレード中は、管理サーバーの設定を変更できません。

2. クラスターを開始します。

この結果、Microsoft のフェールオーバークラスターのノードに最新版の管理サーバーがインストールされました。

Kaspersky Security Center の初期設定

このセクションでは Kaspersky Security Center のインストール後に初期セットアップを実行するために必要となる手順について説明します。

ハードニングガイド

このハードニングガイドは、Kaspersky Security Center のインストールおよび管理を行う専門家、ならびに Kaspersky Security Center を使用する組織にテクニカルサポートを提供する方を対象にしています。

ハードニングガイドでは、Kaspersky Security Center とそのコンポーネントの構成に関する推奨事項と機能について説明し、セキュリティ侵害のリスクを軽減することを目的としています。

設定する前に、管理サーバーデータのバックアップタスクまたはklbackupユーティリティを使用して、Kaspersky Security Center Administration Serverのバックアップコピーを作成し、安全な場所に保存してください。

ハードニングガイドには、次の情報が含まれています：

- 管理サーバーアーキテクチャの選択
- 管理サーバーへの安全な接続の設定
- 管理サーバーにアクセスするためのアカウントの設定
- 管理サーバーとクライアントデバイスの保護管理
- 管理対象アプリケーションの保護構成
- 管理サーバーのメンテナンス
- サードパーティ製品への情報の転送

管理サーバーでの作業を開始する前に、 Kaspersky Security Center からハードニングガイドの簡易版を読むように要求されます。

ハードニングガイドを読んだことを確認するまでは、管理サーバーを使用することができませんので、ご注意ください。

ハードニングガイドを読むには：

1. 管理コンソールまたは Kaspersky Security Center Web コンソールを開き、コンソールにログインします。
   コンソールは、現在のバージョンのハードニングガイドを読んだことを確認したかどうかを確認します。
   ハードニングガイドをまだ読んでいない場合は、ウィンドウが開き、ハードニングガイドの簡易版が表示されます。
2. 次のいずれかの手順を実行します：
   - ハードニングガイドの簡易版をテキストドキュメントとして表示したい場合は、［**新しいウィンドウで開く**］をクリックします。
   - ハードニングガイドの完全版を表示するには、［**オンラインヘルプでハードニングガイドを開く**］をクリックします。
3. ハードニングガイドを読んだ後、［**ハードニングガイドの内容をすべて確認し、理解した上で同意します**］をオンにし、［**同意**］をクリックします。

これで、管理サーバーを操作することができます。

ハードニングガイドの新しいバージョンが表示されると、Kaspersky Security Center はそれを読むように促します。

管理サーバークイックスタートウィザード

このセクションでは、管理サーバークイックスタートウィザードについて説明します。

クイックスタートウィザードの概要

このセクションでは、管理サーバークイックスタートウィザードについて説明します。

管理サーバークイックスタートウィザードを使用すると、最低限必要なタスクとポリシーを作成し、最小限の設定を行って、管理対象のカスペルスキー製品のプラグインをダウンロードしてインストールします。そして、管理対象のカスペルスキー製品のインストールパッケージを作成します。ウィザードの実行中、次の変更をアプリケーションに対して行うことができます：

- 管理対象アプリケーションのプラグインをダウンロードしてインストールします。クイックスタートウィザードが終了すると、インストールされている管理プラグインのリストが、管理サーバーのプロパティウィンドウの［**詳細**］→［**インストール済みアプリケーション管理プラグインの詳細情報**］セクションに表示されます。

- 管理対象のカスペルスキー製品のインストールパッケージを作成します。クイックスタートウィザードが終了すると、Windows 用のネットワークエージェントと管理対象のカスペルスキー製品のインストールパッケージが、［**管理サーバー**］→［**詳細設定**］→［**リモートインストール**］→［**インストールパッケージ**］のリストに表示されます。

- 管理グループ内のデバイスに自動配信可能なライセンス情報ファイルを追加するか、アクティベーションコードを入力します。クイックスタートウィザードが終了すると、ライセンスに関する情報が、［**管理サーバー**］→［**カスペルスキーのライセンス**］リストと管理サーバーのプロパティウィンドウの［**ライセンス**］セクションに表示されます。

- Kaspersky Security Network（KSN）との対話を設定します。

- 管理サーバーと管理対象アプリケーションの動作中に発生したイベントを通知するメール配信を設定します（通知が正しく送信されるようにするには、管理サーバーとすべての受信側デバイスで Messenger サービスが稼働している必要があります）。クイックスタートウィザードが終了すると、メール通知設定が、管理サーバーのプロパティウィンドウの［**通知**］セクションに表示されます。

- デバイスにインストールされたアプリケーションのアップデートの設定と脆弱性の修正設定を調整します。

- 管理対象デバイスの最上位階層で、ワークステーションとサーバーの保護ポリシー、およびマルウェアスキャンタスク、アップデートのダウンロードタスク、データバックアップタスクを作成します。クイックスタートウィザードが終了すると、作成されたタスクが、［**管理サーバー**］→［**タスク**］のリストに表示され、管理対象アプリケーションのプラグインに対応するポリシーが［**管理サーバー**］→［**ポリシー**］のリストに表示されます。

［**管理対象デバイス**］グループで既に該当するポリシーが作成されている場合を除き、クイックスタートウィザードでは Kaspersky Endpoint Security for Windows などの管理対象製品のポリシーが作成されます。クイックスタートウィザードでは、［**管理対象デバイス**］グループに同じ名前のタスクが作成されていない場合にタスクを作成します。

管理コンソールでは、Kaspersky Security Center に初めて接続すると、クイックスタートウィザードを実行することを指示するメッセージが自動的に表示されます。また、クイックスタートウィザードはいつでも手動で起動できます。

管理サーバークイックスタートウィザードの開始

管理サーバーのインストール後に初めて接続すると、クイックスタートウィザードを実行することを指示するメッセージが自動的に表示されます。また、クイックスタートウィザードはいつでも手動で起動できます。

クイックスタートウィザードを手動で起動するには：

1. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。
2. フォルダーのコンテキストメニューで、［**すべてのタスク**］→［**管理サークイックスタートウィザード**］の順に選択します。

   管理サーバーの初期設定を実行するように指示されます。ウィザードの指示に従ってください。

クイックスタートウィザードを再度起動した場合、ウィザードの前回の実行で作成されたタスクとポリシーをもう一度作成することはできません。

ステップ1：プロキシサーバーの設定

管理サーバーのインターネットアクセスを設定します。Kaspersky Security Network を使用し、Kaspersky Security Center 向けおよび管理対象カスペルスキー製品向けの定義データベースのアップデートをダウンロードするには、インターネットアクセスを設定する必要があります。

インターネットへの接続時にプロキシサーバーを使用する場合は、［**プロキシサーバーを使用する**］をオンにします。このオプションをオンにすると、設定を入力するフィールドが使用可能になります。プロキシサーバーの接続を次のように設定します：

- **アドレス**

  インターネットへの Kaspersky Security Center の接続に使用するプロキシサーバーのアドレス。

- **ポート番号**

  Kaspersky Security Center でプロキシサーバーへの接続を確立するポートの番号。

- **ローカルアドレスにプロキシサーバーを使用しない**

  ローカルネットワークのデバイスへの接続にプロキシサーバーを使用しません。

- **プロキシサーバー認証**

  このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。
  ［**プロキシサーバーを使用する**］をオンにすると、この入力フィールドが使用可能になります。

- **ユーザー名**

  プロキシサーバーへの接続の確立に使用されるユーザーアカウント（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

- **パスワード**

  プロキシサーバーへの接続の確立に使用されるアカウントのユーザーが設定したパスワード（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

  入力したパスワードを表示するには、確認する間だけ［**入力した文字を表示する**］をクリックしたままにします。

クイックスタートウィザードを使用せずに、後からインターネットアクセスを設定することもできます。

ステップ 2：アプリケーションのアクティベート方法の選択

Kaspersky Security Center のアクティベーションオプションのいずれかを選択します：

- **アクティベーションコードを挿入**

  *アクティベーションコード*は、英数字 20 文字の一意な並びで構成されます。アクティベーションコードを入力すると、Kaspersky Security Center をアクティベートするライセンス情報を追加することができます。アクティベーションコードは、Kaspersky Security Center を購入すると、指定したメールアドレスに届きます。

  アクティベーションコードを使用して製品をアクティベートするには、カスペルスキーのアクティベーションサーバーと接続を確立するためのインターネット接続が必要です。

  このアクティベーションオプションを選択すると、［**管理対象デバイスにライセンスを自動配信する**］を有効にできます。

  このオプションを有効にすると、ライセンスが管理対象デバイスに自動的に適用されます。

  このオプションが無効になっている場合、管理コンソールツリーの［**カスペルスキーのライセンス**］フォルダーで、後で管理対象デバイスにライセンスを適用できます。

  何らかの理由でアクティベーションコードを入力してもアクティベーションが成功しなかった場合は、ライセンス情報ファイルを指定してアプリケーションをアクティベートできます。

- **ライセンス情報ファイルを指定**

*ライセンス情報ファイル*は、拡張子「key」のファイルであり、カスペルスキーから提供されます。ライセンス情報ファイルを製品に追加し、製品をアクティベートする目的で作成されています。

ライセンス情報ファイルの取得方法については、次の［ライセンス情報ファイルについて］セクションで説明します。

ライセンス情報ファイルでのアクティベーション時には、カスペルスキーのアクティベーションサーバーへの接続は必要ありません。

このアクティベーションオプションを選択すると、［**管理対象デバイスにライセンスを自動配信する**］を有効にできます。

このオプションを有効にすると、ライセンスが管理対象デバイスに自動的に適用されます。

このオプションが無効になっている場合、管理コンソールツリーの［**カスペルスキーのライセンス**］フォルダーで、後で管理対象デバイスにライセンスを適用できます。

- **アプリケーションのアクティベーションを後で実行**

アプリケーションは基本機能のみが使用できる状態で動作し、モバイルデバイス管理および脆弱性とパッチ管理機能は利用できません。

アプリケーションのアクティベーションを延期する場合は、後でいつでもライセンスを追加できます。

ステップ 3：保護領域とオペレーティングシステムの選択

所属組織のネットワークで保護対象範囲とオペレーティングシステムを選択します。これらの項目を選択することによって、ネットワーク内のクライアントデバイスにインストールするためにカスペルスキーのサーバーからダウンロードできる管理プラグインと配布パッケージが絞り込まれます。オプションを選択します：

- **保護の対象**

次の保護領域を選択できます：

- **ワークステーション**：組織ネットワーク内のワークステーションを保護する場合はこのオプションをオンにします。既定では、［ワークステーション］はオンです。
- **ファイルサーバーおよびストレージ**：組織ネットワーク内のファイルサーバーを保護する場合はこのオプションをオンにします。
- **モバイルデバイス**：会社所有または従業員所有のモバイルデバイスを保護する場合はこのオプションをオンにします。モバイルデバイス管理機能をサポートするライセンスを追加していない状態でこのオプションを選択した場合、モバイルデバイス管理機能をサポートするライセンスを追加する必要性を通知するメッセージが表示されます。ライセンスを追加しない場合、モバイルデバイス機能を使用することはできません。
- **仮想化領域**。組織ネットワーク内の仮想マシンを保護する場合はこのオプションをオンにします。
- **Kaspersky Anti-Spam**：メールサーバーをスパムや詐欺、マルウェアから保護する場合はこのオプションを選択します。
- **組み込みシステム**。Automated Teller Machine（ATM）などの Windows ベースの組み込みシステムを保護する場合は、このオプションをオンにします。
- **産業ネットワーク**。産業用ネットワーク全体およびカスペルスキー製品によって保護されているネットワークエンドポイントからのセキュリティデータを監視する場合は、このオプションをオンにします。
- **産業エンドポイント**。産業用ネットワーク内の個々のノードを保護する場合は、このオプションをオンにします。

- **オペレーティングシステム**

次のプラットフォームを選択できます：

- Microsoft Windows
- Linux
- macOS
- Android
- その他

サポートされているオペレーティング システムについては、「ハードウェアおよびソフトウェア要件」を参照してください。

クイックスタートウィザードを使用せずに、後からカスペルスキー製品パッケージを使用可能なパッケージのリストから選択できます。必要なパッケージを検索しやすくするために、次の基準に従って使用可能なパッケージのリストをフィルタリングできます。

- 保護領域
- ダウンロードしたソフトウェアの種別（配布パッケージ、ユーティリティ、プラグイン、または Web プラグイン）

- カスペルスキー製品のバージョン
- カスペルスキー製品のローカリゼーション言語

ステップ 4：管理対象製品のプラグインの選択

インストールする管理対象製品のプラグインを選択します。カスペルスキーのサーバーから利用できるプラグインのリストが表示されます。リストは、ウィザードの前のステップで選択されたオプションに従ってフィルタリングされます。既定では、このリストではプラグインのすべての言語バージョンが表示されます。特定の言語バージョンのみを対象にプラグインのリストを表示するには、［**管理コンソールの言語または次の言語で表示**］で目的の言語を選択します。プラグインのリストには次の列が含まれます：

- **アプリケーション名**

  前のステップで選択した保護領域とプラットフォームに応じて、対応するプラグインが選択されています。

- **アプリケーションのバージョン**

  リストには、カスペルスキーのサーバーから利用できるすべてのバージョンのプラグインが含まれています。既定では、最新バージョンのプラグインが選択されています。

- **ローカリゼーション言語**

  既定では、インストール時に選択した Kaspersky Security Center の言語に応じてプラグインのローカリゼーション言語も選択されます。［**管理コンソールの言語または次の言語で表示**］ドロップダウンリストで、その他の言語を指定することもできます。

プラグインの選択が完了すると、別のウィンドウが開いてインストールが自動的に開始します。一部のプラグインのインストールでは使用許諾契約書に同意する必要があります。使用許諾契約書の内容を確認し、同意する場合は［**使用許諾契約書の条項に同意する**］をオンにして［**インストール**］をクリックします。使用許諾契約書の条項に同意しない場合、プラグインはインストールされません。

インストールが完了したら、インストールウィンドウを閉じます。

クイックスタートウィザードを使用せずに、後から管理プラグインを選択することもできます。

ステップ 5：配布パッケージのダウンロードとインストールパッケージの作成

Kaspersky Endpoint Security for Windows は、クライアントデバイスに保存されている情報を暗号化する機能を備えています。組織のニーズに合致した Kaspersky Endpoint Security for Windows の配布パッケージをダウンロードするには、組織内のクライアントデバイスの所在地における法令などを確認してください。

［**暗号化種別**］ウィンドウで、次のいずれかの暗号化種別を選択します：

- 高度な暗号化（AES256）：この暗号化種別では、256 ビットの鍵長が使用されます。
- 中程度の（AES56）：この暗号化種別では、56 ビットの鍵長が使用されます。

［**暗号化種別**］ウィンドウは、保護対象範囲として［**ワークステーション**］を、プラットフォームとして［**Microsoft Windows**］を選択した場合にのみ表示されます。

暗号化種別を選択すると、両方の暗号化種別のバージョンの配布パッケージのリストが表示されます。選択した暗号化種別の配布パッケージがリストで選択されています。配布パッケージの言語は Kaspersky Security Center の言語に対応するものが選択されます。Kaspersky Security Center の言語に対応する Kaspersky Endpoint Security for Windows の配布パッケージが存在しない場合、英語版の配布パッケージが選択されます。

リストでは、［**管理コンソールの言語または次の言語で表示**ドロップダウンリストを使用して、配布パッケージの言語を選択できます。

管理対象製品の配布パッケージには、Kaspersky Security Center の特定の最小バージョンをインストールする必要がある場合があります。

［**暗号化種別**］ウィンドウで選択した暗号化種別とは異なる暗号化種別の配布パッケージをリストで選択することもできます。Kaspersky Endpoint Security for Windows の配布パッケージの選択が完了すると、前のステップで指定した保護対象のネットワークの構成要素とプラットフォームに対応する配布パッケージのダウンロードが始まります。［**ダウンロード状況**］列でダウンロードの進捗を確認できます。クイックスタートウィザードが終了すると、Windows 用のネットワークエージェントと管理対象のカスペルスキー製品のインストールパッケージが、［**管理サーバー**］→［**詳細設定**］→［**リモートインストール**］→［**インストールパッケージ**］のリストに表示されます。

一部の配布パッケージのダウンロードを完了させるには、使用許諾契約書に同意する必要があります。［**同意する**］をクリックすると、使用許諾契約書の条項が表示されます。ウィザードの次のステップに進むには、使用許諾契約書の条項とカスペルスキーのプライバシーポリシーの条項に同意する必要があります。同意する場合、使用許諾契約書とカスペルスキーのプライバシーポリシーにそれぞれ対応するオプションを選択し、［**すべて同意する**］をクリックします。パッケージのダウンロードに必要な条項に同意しない場合、パッケージのダウンロードはキャンセルされます。

使用許諾契約書の条項とカスペルスキーのプライバシーポリシーの条項への同意が完了すると、配布パッケージのダウンロードが引き続き実行されます。ダウンロードが完了すると、［**インストールパッケージが作成されました**］ステータスが表示されます。インストールパッケージを使用して、後でカスペルスキー製品をクライアントデバイスに導入できます。

クイックスタートウィザードとは別に、インストールパッケージを手動で作成できます。管理コンソールツリーで、［**管理サーバー**］→［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］の順に移動します。

ステップ 6：Kaspersky Security Network の使用の設定

Kaspersky Security Network の評価データベースへのアクセス権を取得することで、脅威に対するカスペルスキー製品の対応を迅速化し、一部の保護コンポーネントの効果を高め、誤検知のリスクを低減することができます。

ウィンドウに表示される KSN に関する声明の内容を確認します。Kaspersky Security Center の動作に関する情報を Kaspersky Security Network ナレッジベースに転送する設定を指定します。次のいずれかのオプションをオンにします：

- **Kaspersky Security Network への参加に同意する**

Kaspersky Security Center とクライアントデバイスにインストールされている管理対象製品は、自動的に動作情報を Kaspersky Security Network に送信します。Kaspersky Security Network への参加により、ウイルスなどの脅威に関する情報を含んだデータベースのアップデートをより迅速に入手できるため、セキュリティへの緊急の脅威にすぐに対応できます。

- **Kaspersky Security Network への参加に同意しない**

  Kaspersky Security Center と管理対象製品は、Kaspersky Security Network に対して情報を提供しません。

  このオプションをオンにすると、Kaspersky Security Network の使用がオフになります。

Kaspersky Endpoint Security for Windows プラグインをダウンロードした場合、Kaspersky Security Center と Kaspersky Endpoint Security for Windows 両方の KSN に関する声明が表示されます。プラグインがダウンロードされた他の管理対象カスペルスキー製品の KSN 声明はそれぞれ別のウィンドウに表示され、声明ごとに同意または不同意を選択する必要があります。

後で、管理コンソールの管理サーバープロパティウィンドウから、Kaspersky Security Network（KSN）への管理サーバーアクセスを設定することもできます。

ステップ 7：メール通知の設定

管理対象デバイス上のカスペルスキー製品の実行中に登録されたイベントに関する通知の配信方法を設定します。この設定は、管理サーバーの既定の設定として使用されます。

カスペルスキー製品で発生したイベントに関する通知の配信を設定するには、次の設定を使用します：

- **受信者（メールアドレス）**

  通知が送られるユーザーのメールアドレスです。1つ以上のアドレスを入力できます。複数のアドレスを入力する場合はセミコロンで区切ってください。

- **SMTP サーバー**

  組織のメールサーバーのアドレスです。

  複数のアドレスを入力する場合はセミコロンで区切ってください。次の値を使用できます：

  - IPv4 / IPv6 アドレス
  - デバイスの Windows ネットワーク名（NetBIOS 名）
  - SMTP サーバーの DNS 名

- **SMTP サーバーのポート**

  SMTP サーバーの通信ポート番号。複数の SMTP サーバーを使用する場合、それらサーバーへの接続は指定された通信ポートを介して確立されます。既定のポート番号は 25 です。

- **ESMTP 認証を使用する**

ESMTP 認証のサポートを有効にします。チェックボックスをオンにすると、［**ユーザー名**］と［**パスワード**］で ESMTP 認証を設定できます。既定では、このチェックボックスはオフです。

- **設定**

次の設定を指定します：

- **件名**（メールの件名）
- **送信者のメールアドレス**
- **SMTPサーバーの TLS 設定**

SMTP サーバーの TLS 設定を指定できます：

TLS の使用を無効にしたり、SMTP サーバーがこのプロトコルをサポートしている場合に TLS を使用するように設定したり、TLS のみの使用を強制したりすることができます。TLS のみを使用する場合は、SMTP サーバーの認証用の証明書を指定し、TLS の任意のバージョンを介した通信を有効にするか、TLS 1.2 以降のバージョンのみを介した通信を有効にするかを選択します。また、TLS のみを使用する場合、SMTP サーバーのクライアント認証に使用する証明書を指定できます。

- SMTP サーバーの証明書ファイルを参照します：

信頼できる証明書認証局から証明書のリストを含むファイルを受け取り、ファイルを管理サーバーへアップロードできます。Kaspersky Security Center は、SMTP サーバーの証明書も信頼できる証明書認証局によって署名されているかどうかをチェックします。信頼できる証明書認証局から SMTP サーバーの証明書を受け取っていない場合、Kaspersky Security Center は SMTP サーバーに接続できません。

- クライアント証明書ファイルを参照します：

信頼できる認証局など、任意の発行元から受け取った証明書を使用できます。次のいずれかの証明書タイプを使用して、証明書とその秘密鍵を指定する必要があります：

- X-509証明書：

証明書を含むファイルと秘密鍵を含むファイルを指定します。これらのファイルは任意の順序でアップロードできます。両方のファイルをアップロードする際は、秘密鍵を復号化するためのパスワードを指定します。秘密鍵が暗号化されていない場合、パスワードの値は空である可能性があります。

- pkcs12 コンテナー：

証明書とその秘密鍵を含む単一のファイルをアップロードする必要があります。ファイルの読み込み時に、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

［**テストメッセージの送信**］をクリックして、新しいメール通知設定をテストできます。

クイックスタートウィザードを使用せずに、後からイベント通知を設定することもできます。

ステップ 8：アップデート管理の設定

クライアントデバイスにインストールされたアプリケーションのアップデートを管理するための設定を行います。

これらの設定は、脆弱性とパッチ管理機能を利用できるライセンスを適用している場合にのみ設定できます。

［**アップデートを検索してインストール**］セクションで、Kaspersky Security Center を検索してインストールする方法を選択できます。

- **必要なアップデートの検索**

  *脆弱性とアプリケーションのアップデートの検索*タスクがない場合は、自動的に作成されます。

  既定ではこのオプションが選択されます。

- **必要なアップデートの検索とインストール**

  ［*脆弱性とアプリケーションのアップデートの検索*］タスクと［*アップデートのインストールと脆弱性の修正*］タスクがまだ作成されていない場合は、自動的に作成されます。

［**Windows Server Update Services**］セクションで、アップデートの同期元を選択できます：

- **ドメインポリシーで定義されたアップデート元を使用する**

  クライアントデバイスは、ドメインポリシー設定に従って Windows Update 更新プログラムをダウンロードします。ネットワークエージェントポリシーがまだ作成されていない場合は、自動的に作成されます。

- **管理サーバーを WSUS サーバーとして使用する**

  クライアントデバイスは、管理サーバーから Windows Update 更新プログラムをダウンロードします。［*Windows Update の同期の実行*］タスクとネットワークエージェントポリシーがまだ作成されていない場合は、自動的に作成されます。

クイックスタートウィザードとは別に、［*脆弱性と必要な更新プログラムの検索*］および［*必要な更新プログラムのインストールと脆弱性の修正*］タスクを作成できます。管理サーバーを WSUS サーバーとして使用するには、［*Windows Update の同期の実行*］タスクを作成してから、ネットワークエージェントのポリシーで［**管理サーバーを WSUS サーバーとして使用する**］をオンにする必要があります。

ステップ 9：初期保護設定の作成

［**初期プロテクションの設定**］ウィンドウには、自動的に作成されたポリシーとタスクのリストが表示されます。次のポリシーとタスクが作成されます：

- Kaspersky Security Center ネットワークエージェントのポリシー
- 管理プラグインが以前にインストールされた管理対象カスペルスキー製品のポリシー
- 管理サーバーのメンテナンス タスク
- 管理サーバーデータのバックアップタスク
- 管理サーバーのリポジトリへのアップデートのダウンロードタスクの設定

- 脆弱性とアプリケーションのアップデートの検索タスク
- アップデートのインストールタスク

ポリシーとタスクの作成が完了してから、ウィザードの次のステップに進んでください。

Kaspersky Endpoint Security for Windows の 10 Service Pack 1 から 11.0.1 までの管理プラグインをダウンロードしてインストールしていた場合、ポリシーとタスクの作成中に Kaspersky Endpoint Security for Windows の信頼ゾーンの初期設定用のウィンドウが表示されます。カスペルスキーによって安全が確認された開発元を信頼リストに追加するようにメッセージで指示されます。これらの開発元の製品が誤ってブロックされないようスキャンから除外するためです。信頼するオブジェクトを今すぐ作成することも、信頼リストを後で作成することもできます。それには、コンソールツリーで、［**ポリシー**］→［Kaspersky Endpoint Security］のプロパティメニュー→［**先進の脅威対策**］→［**信頼ゾーン**］→［**設定**］→［**追加**］の順に選択します。信頼するオブジェクトのリストは、アプリケーションの使用時にいつでも編集できます。

信頼リストでの操作は、Kaspersky Endpoint Security for Windows により提供される専用ツールを使用して実行します。操作方法の詳細と暗号化関連機能の説明は、Kaspersky Endpoint Security for Windows のオンラインヘルプを参照してください。

信頼リストの初期設定を終了して、ウィザードに戻るには、［**OK**］をクリックします。

［**次へ**］をクリックします。必要なポリシーとタスクをすべて作成すると、このボタンが使用可能になります。

クイックスタートウィザードを使用せずに、必要なタスクとポリシーを後で作成することもできます。

ステップ 10：モバイルデバイスの接続

ウィザードの設定で［**モバイルデバイス**］の保護範囲を有効にするように設定済みの場合は、管理対象の組織内で企業用モバイルデバイスの接続設定を指定します。**モバイルデバイス**の保護対象範囲を有効にしていない場合は、このステップは省略します。

ウィザードのこのステップでは、次の操作を実行します：

- モバイルデバイスの接続用のポートを設定する
- 管理サーバーの認証を設定する
- 証明書の作成や管理を行う
- 一般的な証明書の発行、自動更新、暗号化を設定する
- モバイルデバイス用の移動ルールを作成する

モバイルデバイスの接続用のポートを設定するには：

1. ［**設定**］を［**モバイルデバイス接続**］フィールドの右でクリックします。
2. ドロップダウンリストで、［**ポートを設定する**］を選択します。
   ［管理サーバーのプロパティ］ウィンドウが開かれ、［**追加のポート**］セクションが表示されます。
3. ［**追加のポート**］セクションで、モバイルデバイス接続設定を指定できます：

- **アクティベーションプロキシサーバーの SSL ポート**

  Kaspersky Endpoint Security for Windows をカスペルスキーのアクティベーションサーバーに接続する SSL ポートの番号です。

  既定のポート番号は 17000 です。

- **モバイルデバイス用ポートを開く**

  モバイルデバイスをライセンス管理サーバーに接続するためのポートを開きます。その下のフィールドでポート番号とその他の設定を定義できます。

  既定では、このオプションはオンです。

- **モバイルデバイスとの同期用のポート**

  モバイルデバイスが管理サーバーに接続し、管理サーバーとデータをやり取りするために経由するポートの番号です。既定のポート番号は 13292 です。

  ポート 13292 が他の目的で使用されている場合は、別のポートを割り当てることができます。

- **モバイルデバイスのアクティベーション用のポート**

  Kaspersky Endpoint Security for Android をカスペルスキーのアクティベーションサーバーに接続するポートです。

  既定のポート番号は 17100 です。

- **UEFI 保護デバイスおよび KasperskyOS デバイス用のポートを開く**

  UEFI 保護デバイスを管理サーバーに接続できます。

- **UEFI 保護デバイスおよび KasperskyOS デバイス用のポート**

  ［**UEFI 保護デバイスおよび KasperskyOS デバイス用のポートを開く**］がオンの場合、ポート番号を変更できます。既定のポート番号は 13294 です。

- **Prometheus のポートを開く**

  Prometheus プルリクエスト用のポート。既定のポート番号は 13296 です。

4. ［**OK**］をクリックして変更内容を保存し、クイックスタートウィザードに戻ります。

モバイルデバイスによる管理サーバー認証および管理サーバーによるモバイルデバイス認証を設定する必要があります。必要に応じて、［クイックスタートウィザード］を使用せずに、後から認証の設定を行うこともできます。

モバイルデバイスによる管理サーバー認証を設定するには：

1. ［**設定**］を［**モバイルデバイス接続**］フィールドの右でクリックします。
2. ドロップダウンリストで、［**認証を設定する**］を選択します。

管理サーバーのプロパティウィンドウが開き、［**証明書**］セクションが表示されます。

3. ［**モバイルデバイスによる管理サーバー認証**］セクションでモバイルデバイス用の認証オプションを選択し、［**UEFI 保護デバイスによる管理サーバー認証**］セクションで UEFI 保護デバイス用の認証オプションを選択します。

   管理サーバーとクライアントデバイスのデータ交換時に、証明書を使用して認証が実行されます。

   既定では、管理サーバーは、管理サーバーのインストール中に作成された証明書を使用します。必要に応じて、新しい証明書を追加できます。

新しい証明書を追加するには（任意）：

1. ［**その他の証明書**］を選択します。

   ［**参照**］が表示されます。

2. ［**参照**］をクリックします。

3. 表示されたウィンドウで、証明書の設定を指定します。

   - **証明書の種別**

     このドロップダウンリストでは、証明書の種別を選択できます。

     - **X.509 証明書**：このオプションをオンにすると、証明書の秘密鍵および公開鍵証明書を指定する必要があります。
       - **秘密鍵 (.prk, .pem)**：このフィールドで、［**参照**］をクリックして PKCS #8 (*.prk) 形式で証明書の秘密鍵を指定します。
       - **公開鍵 (.cer)**：このフィールドで、［**参照**］をクリックして PEM (*.cer) 形式で公開鍵を指定します。
     - **PKCS #12 コンテナー**：このオプションをオンにすると、［**参照**］をクリックして［**証明書ファイル**］フィールドに入力することで P12 または PFX 形式で証明書を指定することができます。

   - アクティベーション時間

     - **即時**

       ［OK］をクリックすると、現在の証明書が新しい証明書に即座に置き換わります。
       以前接続していたモバイルデバイスは管理サーバーに接続できなくなります。

     - **次の日数経過後**

       このオプションをオンにすると、予備の証明書が生成されます。指定の日数が経過すると、現在の証明書は新しい証明書に置き換わります。予備の証明書の有効日付が［**証明書**］セクションに表示されます。

       事前に再発行を計画することを推奨します。指定された期間が終了する前に、予約証明書をモバイルデバイスにダウンロードする必要があります。現在の証明書が新しい証明書に置き換わると、予備の証明書がない以前接続していたモバイルデバイスは管理サーバーに接続できなくなります。

4. 選択した管理サーバー証明書の設定を確認するには、［**プロパティ**］をクリックします。

管理サーバーを使用して発行された証明書を再発行するには：

1. **管理サーバーを使用して発行された証明書**を選択します。
2. ［**再発行**］をクリックします。
3. 表示されたウィンドウで、次の設定を行います：
   - 接続アドレス：
     - **以前の接続アドレスを使用**

       モバイルデバイスの接続先管理サーバーのアドレスは変更されません。

       既定ではこのオプションが選択されます。

     - **接続アドレスを変更**

       モバイルデバイスを別のアドレスに接続するには、このフィールドで該当するアドレスを指定します。

       モバイルデバイス接続用のアドレスの変更が完了すると、新しい証明書が発行されます。接続されているすべてのモバイルデバイスで古い証明書は無効になります。以前接続していたデバイスは管理サーバーに接続できなくなるので、非管理対象になります。

   - アクティベーション時間
     - **即時**

       ［OK］をクリックすると、現在の証明書が新しい証明書に即座に置き換わります。

       以前接続していたモバイルデバイスは管理サーバーに接続できなくなります。

     - **次の日数経過後**

       このオプションをオンにすると、予備の証明書が生成されます。指定の日数が経過すると、現在の証明書は新しい証明書に置き換わります。予備の証明書の有効日付が［**証明書**］セクションに表示されます。

       事前に再発行を計画することを推奨します。指定された期間が終了する前に、予約証明書をモバイルデバイスにダウンロードする必要があります。現在の証明書が新しい証明書に置き換わると、予備の証明書がない以前接続していたモバイルデバイスは管理サーバーに接続できなくなります。

4. ［OK］をクリックして変更内容を保存し、［**証明書**］ウィンドウに戻ります。
5. ［OK］をクリックして変更内容を保存し、クイックスタートウィザードに戻ります。

管理サーバーによるモバイルデバイス識別の一般的な証明書の発行、自動更新、暗号化を設定するには：

1. ［**設定**］を［**モバイルデバイスの認証**］フィールドの右でクリックします。
   ［**証明書発行ルール**］ウィンドウが開き、［**モバイル証明書の発行**］セクションが表示されます。

2. 必要に応じて、［**発行の設定**］セクションで次を設定します：

- **証明書の有効期間**

  証明書の有効期間（日数）です。証明書の既定の有効期間は 365 日です。この有効期間を過ぎると、モバイルデバイスは管理サーバーに接続できなくなります。

- **証明書ソース**

  モバイルデバイスの一般的な証明書のソースを選択します。証明書は管理サーバーによって発行されるか、手動で指定します。

  公開鍵基盤（PKI）との統合が［**PKI（公開鍵基盤）の統合**］セクションで設定されている場合は、証明書テンプレートを変更できます。その場合、次のテンプレート選択フィールドを使用できます：

- **既定のテンプレート**

  外部証明書ソース（Certification Center）によって発行された証明書を既定のテンプレートで使用します。

  既定では、このオプションがオンです。

- **他のテンプレート**

  証明書の発行に使用するテンプレートを選択します。ドメインで証明書のテンプレートを指定できます。［**リストの更新**］をクリックすると、証明書のテンプレートのリストが更新されます。

3. 必要に応じて、［**自動更新設定**］セクションで証明書の自動発行について次の設定を指定します：

- **証明書の有効期間の残りが次の日数になったら更新**

  現在の証明書の有効期限が切れるまでの残りの日数の中で、管理サーバーによって新しい証明書が発行されます。たとえば、このフィールドの値が 4 の場合、現在の証明書の有効期限が切れる 4 日前に、管理サーバーによって新しい証明書が発行されます。既定値は 7 です。

- **可能であれば証明書を自動で再発行**

  このオプションをオンにすると、［**証明書の有効期間の残りが次の日数になったら更新**］フィールドで指定された日数の間、証明書が自動的に再発行されます。証明書を手動で定義した場合、証明書を自動的に更新することはできず、有効化したオプションは機能しません。

  既定では、このオプションはオフです。

  証明書は認証局によって自動的に再発行されます。

4. 必要に応じて、インストール時に［**パスワードによる保護**］セクションで証明書の復号化設定を指定します。

   ［**証明書のインストール時にパスワードを要求する**］をオンにすると、証明書がモバイルデバイスにインストールされる時に、パスワードの入力が要求されます。パスワードは、モバイルデバイスに証明書をインストールする際に 1 度だけ使用されます。

パスワードは管理サーバーによって自動的に生成され、ユーザーの指定したメールアドレスに送信されます。ユーザーのメールアドレスを指定できます。あるいは、別の方法でユーザーにパスワードを送信する場合は自身のメールアドレスを指定できます。

スライダーを使用して、証明書復号化のパスワードの文字数を指定できます。

たとえば、スタンドアロンの Kaspersky Endpoint Security for Android インストールパッケージの共有証明書を保護するには、パスワード入力ウィンドウのオプションが必要です。Kaspersky Security Center Web サーバーからスタンドアロンインストールパッケージが窃取されても、パスワードの保護を使用することで、侵入者による共有証明書へのアクセス権の取得が阻止されます。

このオプションをオフにすると、証明書はインストール中に自動的に復号化され、ユーザーにパスワードを要求することはありません。既定では、このオプションはオフです。

5. ［**OK**］をクリックして変更内容を保存し、クイックスタートウィザードのウィンドウに戻ります。

［**キャンセル**］をクリックすると、変更が保存されないまま、クイックスタートウィザードに戻ります。

選択した管理グループにモバイルデバイスを移動する機能を有効にするには：

［**モバイルデバイスの自動移動**］フィールドで、［**モバイルデバイスの移動ルールを作成**］をオンにします。

［**モバイルデバイスの移動ルールを作成**］をオンにすると、Android と iOS を実行しているデバイスを［**管理対象デバイス**］グループに移動するルールが自動的に作成されます。

- Kaspersky Endpoint Security for Android と証明書がインストールされている Android オペレーティングシステムを対象
- iOS MDM プロファイルと証明書がインストールされている iOS オペレーティングシステムを対象

そのようなルールが既に存在する場合、ルールは新しく作成されません。

既定では、このオプションはオフです。

Kaspersky Safe Browser のサポートは終了しました。

ステップ 11：アップデートのダウンロード

Kaspersky Security Center とカスペルスキー製品とで使用する定義データベースのアップデートが自動的にダウンロードされます。アップデートはカスペルスキーのサーバーからダウンロードされます。

クイックスタートウィザードを使用せずにアップデートをダウンロードするには、*管理サーバーのリポジトリへのアップデートのダウンロード*タスクを作成して設定します。

ステップ 12：デバイスの検索

［**ネットワークポーリング**］ウィンドウには、管理サーバーによって実行されたネットワークポーリングのステータスに関する情報が表示されます。

［**デバイスの検索**］ウィンドウの下部にあるリンクをクリックすると、管理サーバーによって検出されたネットワークデバイスが表示され、［ネットワークポーリング］ウィンドウの操作方法に関するヘルプを参照できます。

クイックスタートウィザードを使用せずに、後からネットワークのポーリングを行うこともできます。管理コンソールを使用して、 Windows ドメイン、 Active Directory、 IP 範囲、および IPv6 ネットワークのポーリングを構成します。

ステップ 13：クイックスタートウィザードの終了

ネットワーク上のデバイスへのアンチウイルス製品またはネットワークエージェントの自動インストールを開始する場合は、クイックスタートウィザードの完了ウィンドウで［**リモートインストールウィザードの実行**］をオンにします。

ウィザードを終了するには、［**終了**］をクリックします。

管理コンソールから管理サーバーへの接続の設定

管理コンソールは、SSL ポート TCP 13291 を介して管理サーバーに接続されます。同じポートを klakaut 自動化オブジェクトも使用できます。

ポート TCP 14000 は、管理コンソール、ディストリビューションポイント、セカンダリ管理サーバー、klakaut 自動化オブジェクトへの接続とクライアントデバイスからのデータの受信に使用されます。

通常、SSL ポート TCP 13000 は、DMZ 内にあるネットワークエージェント、セカンダリ管理サーバー、プライマリ管理サーバーのみが使用できます。次の場合は、管理コンソールを SSL ポート 13000 で接続する必要があります：

- 管理コンソールと他の動作（クライアントデバイスからのデータの取得、ディストリビューションポイントへの接続、セカンダリ管理サーバーへの接続）の両方で 1 つの SSL ポートを使用する可能性がある場合
- klakaut 自動化オブジェクトが管理サーバーに直接ではなく DMZ 内のディストリビューションポイントを介して接続される場合

管理コンソールをポート 13000 で接続できるようにするには：

1. 管理サーバーがインストールされたデバイスのシステムレジストリを開きます（たとえば、ローカルで［**スタート**］→［**ファイル名を指定して実行**］で regedit コマンドを使用します）。
2. 次のレジストリエントリに移動します：
   - 32 ビットシステム：

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - 64 ビットシステム：

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. LP_ConsoleMustUsePort13291 （DWORD）キーの値を 00000000 に設定します。

   このキーの既定値は 1 です。
4. 管理サーバーサービスを再起動します。

これにより、管理コンソールをポート 13000 で管理サーバーに接続できます。

管理サーバーのインターネットアクセスを設定します

Kaspersky Security Network を使用し、Kaspersky Security Center 向けおよび管理対象カスペルスキー製品向けの定義データベースのアップデートをダウンロードするには、インターネットアクセスを設定する必要があります。

管理サーバーのインターネットアクセスを指定するには：

1. コンソールツリーで、［**管理サーバー %s**］ノードを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウで、［**詳細**］→［**インターネットアクセスの設定**］の順に移動します。
4. インターネットへの接続時にプロキシサーバーを使用する場合は、［**プロキシサーバーを使用する**］をオンにします。このオプションをオンにすると、設定を入力するフィールドが使用可能になります。プロキシサーバーの接続を次のように設定します：

   - **アドレス**

     インターネットへの Kaspersky Security Center の接続に使用するプロキシサーバーのアドレス。

   - **ポート番号**

     Kaspersky Security Center でプロキシサーバーへの接続を確立するポートの番号。

   - **ローカルアドレスにプロキシサーバーを使用しない**

     ローカルネットワークのデバイスへの接続にプロキシサーバーを使用しません。

   - **プロキシサーバー認証**

     このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。
     ［**プロキシサーバーを使用する**］をオンにすると、この入力フィールドが使用可能になります。

   - **ユーザー名**

     プロキシサーバーへの接続の確立に使用されるユーザーアカウント（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

   - **パスワード**

プロキシサーバーへの接続の確立に使用されるアカウントのユーザーが設定したパスワード（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

入力したパスワードを表示するには、確認する間だけ［**入力した文字を表示する**］をクリックしたままにします。

クイックスタートウィザードを使用して、インターネットアクセスを構成することもできます。

モバイルユーザーデバイスの接続

このセクションでは、モバイルユーザーデバイス（メインネットワークの外部にある管理対象デバイス）を管理サーバーに接続する方法について説明します。

シナリオ：接続ゲートウェイを使用したモバイルユーザーデバイスの接続

このシナリオでは、メインネットワークの外部にある管理対象デバイスを管理サーバーに接続する方法について説明します。

必須条件

シナリオには次の前提条件があります：

- 非武装地帯（DMZ）が組織のネットワークに編成されていること。
- Kaspersky Security Center 管理サーバーが企業ネットワークに導入されていること。

実行するステップ

このシナリオは段階的に進行します：

1. **DMZ 内のクライアントデバイスの選択**

   このデバイスは接続ゲートウェイとして使用されます。選択するデバイスは、接続ゲートウェイの要件を満たしている必要があります。

2. **接続ゲートウェイのロールへのネットワークエージェントのインストール**

   ローカルインストールを使用して、選択したデバイスにネットワークエージェントをインストールすることを推奨します。

   既定では、インストールファイルは次の場所にあります：\\<サーバー名>\KLSHARE\PkgInst\NetAgent_<バージョン番号>

   ネットワークエージェントのセットアップウィザードの［**接続ゲートウェイ**］ウィンドウで、［**DMZ 内でネットワークエージェントを接続ゲートウェイとして使用する**］を選択します。このモードは同時に接続ゲートウェイのロールをアクティブにし、管理サーバーからの接続を待機するようにネットワークエージェントに指示します。管理サーバーへの接続の確立は指示しません。

または、Linux デバイスにネットワークエージェントをインストールし、ネットワークエージェントを接続ゲートウェイとして動作するように設定することも可能です。ただし、Linux デバイスで実行されるネットワークエージェントの制限事項のリストを確認しておく必要があります。

3 接続ゲートウェイのファイアウォールにおける接続の許可

管理サーバーが実際に DMZ の接続ゲートウェイに接続できることを確認するには、管理サーバーと接続ゲートウェイの間のすべてのファイアウォールで TCP ポート 13000 への接続を許可します。

接続ゲートウェイがインターネット上に実際の IP アドレスを持たず、ネットワークアドレス変換（NAT）を使用している場合は、NAT を介して接続を転送するルールを設定します。

4 外部デバイスの管理グループの作成

管理対象デバイスグループの下に新しいグループを作成します。この新しいグループには、外部の管理対象デバイスを含めます。

5 接続ゲートウェイの管理サーバーへの接続

設定した接続ゲートウェイは、管理サーバーからの接続を待機しています。ただし、管理サーバーは、管理対象デバイス間の接続ゲートウェイを使用するデバイスを一覧表示しません。これは、接続ゲートウェイが管理サーバーへの接続確立を試行していないためです。したがって、管理サーバーが接続ゲートウェイへの接続を開始するようにするには、特別な手順が必要です。

次の手順に従います：

1. 接続ゲートウェイをディストリビューションポイントとして追加します。
2. 接続ゲートウェイを**未割り当てデバイス**グループから、外部デバイス用に作成したグループに移動します。

接続ゲートウェイが接続および設定されます。

6 管理サーバーへの外部デスクトップコンピューターの接続

通常、外部デスクトップコンピューターは境界の内側に移動されません。したがって、ネットワークエージェントのインストール時に、ゲートウェイを介して管理サーバーに接続するように設定する必要があります。

7 外部デスクトップコンピューターのアップデートの設定

セキュリティ製品のアップデートが管理サーバーからダウンロードされるように設定されている場合、外部コンピューターは接続ゲートウェイを介してアップデートをダウンロードします。この方法には、2 つの欠点があります：

- これは不要なトラフィックであり、会社のインターネット通信チャネルの帯域幅を占有します。
- この方法により、アップデートの取得が必ずしも最速になるとは限りません。外部コンピューターがカスペルスキーのアップデートサーバーからアップデートを取得する方が、低コストで高速である可能性があります。

次の手順に従います：

1. 前の手順で作成した別の管理グループにすべての外部コンピューターを移動します。
2. 外部デバイスを含むグループをアップデートタスクから除外します。
3. 外部デバイスを含むグループ用に個別のアップデートタスクを作成します。

8 移動中のノート PC の管理サーバーへの接続

移動中のノート PC は、ネットワーク内に存在する場合もあれば、ネットワーク外に存在する場合もあります。効果的に管理するには、場所に応じて異なる方法で管理サーバーに接続する必要があります。トラフィックを効率的に使用するには、場所に応じて異なるアップデート元からアップデートを受信することも必要です。

次のモバイルユーザー向けのルールを設定する必要があります：接続プロファイルとネットワークロケーション記述。各ルールは、移動するノート PC が場所に応じて接続する必要がある管理サーバーのインスタンスと、アップデートの受信元とする必要がある管理サーバーのインスタンスを定義します。

シナリオ：DMZ 内のセカンダリ管理サーバーを介した社外デバイスの接続

メインネットワークの外側にある管理対象デバイスを管理サーバーに接続する場合は、非武装地帯（DMZ）にあるセカンダリ管理サーバーを使用して接続できます。

必須条件

導入を開始する前に、次が完了していることを確認してください：

- DMZ が組織内のネットワークに編成されていること。
- Kaspersky Security Center 管理サーバーが組織の内部ネットワークに導入されていること。

実行するステップ

このシナリオは段階的に進行します：

1. **DMZ 内のクライアントデバイスの選択**

   DMZ で、セカンダリ管理サーバーとして使用されるクライアントデバイスを選択します。

2. **Kaspersky Security Center 管理サーバーのインストール**

   Kaspersky Security Center 管理サーバーをクライアントデバイスにインストールします。

3. **管理サーバーの階層の作成**

   セカンダリ管理サーバーを DMZ に配置する場合、セカンダリ管理サーバーはプライマリ管理サーバーからの接続を受け取る必要があります。新規管理サーバーをセカンダリとして追加し、プライマリ管理サーバーからセカンダリ管理サーバーへポート 13000 で接続できます。2 つの管理サーバーを 1 つの階層内で組み合わせる時は、ポート 13291 が両方の管理サーバーで開放されていることを確認してください。管理コンソールは、ポート 13291 を介して管理サーバーに接続します。

4. **社外の管理対象デバイスをセカンダリ管理サーバーに接続します**

   管理サーバーとメインネットワークにある管理対象デバイスとの間で接続を確立するのと同じ方法で、社外のデバイスを DMZ 内の管理サーバーに接続できます。社外の管理対象デバイスは、ポート 13000 を通じて接続を開始します。

モバイルユーザーデバイスの接続

一部の管理対象デバイスは、常にメインネットワークの外部に配置されています（たとえば、会社の支社にあるコンピューター、売店、ATM、様々な販売拠点に設置されている端末、従業員のホームオフィスにあるコンピューターなど）。また、一部のデバイスは、ネットワークの外部を不定期に移動しています（たとえば、支社や顧客オフィスを訪問するユーザーのノート PC など）。

モバイルユーザーデバイスの保護について、引き続き監視および管理する必要があります。保護ステータスに関する実際の情報を受け取り、デバイスのセキュリティ製品を最新の状態に保ちます。たとえば、そのようなデバイスがメインネットワークから離れている際にセキュリティ侵害を受けた場合、メインネットワークに接続するとすぐに脅威を伝播するプラットフォームになる可能性があるため、これは必要です。モバイルユーザーデバイスを管理サーバーへ接続する方法は、次の 2 つがあります：

- 非武装地帯（DMZ）にある接続ゲートウェイ

  データトラフィックのスキーム：LAN 上の管理サーバー、インターネット上の管理対象デバイス、使用中の接続ゲートウェイ

- DMZ 内の管理サーバー

  データトラフィックのスキーム：DMZ 内の管理サーバー、インターネット上の管理対象デバイス

DMZ 内の接続ゲートウェイ

モバイルユーザーデバイスから管理サーバーへの接続で推奨される方法は、DMZ を組織内に構築し、接続ゲートウェイを DMZ 内に実装することです。外部デバイスは接続ゲートウェイに接続し、ネットワーク内の管理サーバーは接続ゲートウェイを介してデバイスへの接続を開始します。

その他の方法と比較すると、この方法はより安全です。

- ネットワーク外部からの管理サーバーへのアクセスを許可する必要がありません。
- 接続ゲートウェイが攻撃された場合でも、ネットワーク上のデバイスに深刻な危険が及ぶ可能性がありません。接続ゲートウェイ自身は実際は何も管理しておらず、接続を確立することもありません。

また、接続ゲートウェイに必要なハードウェアリソースも少量です。

ただし、この方法には複雑な設定編集の手順が必要です：

- デバイスを DMZ 内で接続ゲートウェイとして動作するように設定するには、ネットワークエージェントのインストールと管理サーバーへの接続を、特定の方法で実行する必要があります。
- 同一のアドレスを、管理サーバーへの接続用に使用することができません。ネットワーク境界の外部から、異なるアドレス（接続ゲートウェイアドレス）を使用するだけでなく、接続方法も変更する必要があります：接続ゲートウェイを介した方法。
- 異なる場所にあるノート PC 用に、別の接続設定を指定する必要もあります。

以前に構成したネットワークに接続ゲートウェイを追加するには、次の手順を実行します：

1. ネットワークエージェントを接続ゲートウェイモードでインストールします。
2. 新しく追加した接続ゲートウェイに接続するデバイスにネットワークエージェントを再インストールします。

DMZ 内の管理サーバー

もう 1 つの方法は、単一の管理サーバーの DMZ 内へのインストールです。

前述の方法よりも、設定の安全性が低くなります。この方法で外部のノート PC を管理するには、インターネット上の任意のアドレスからの接続を管理サーバーが許可する必要があります。内部ネットワークのデバイスをすべて管理することも可能ですが、DMZ からの管理となります。したがって、発生の可能性は低いと言えますが、サーバーが攻撃された場合、結果として甚大な被害が発生する可能性があります。

DMZ 内の管理サーバーが内部ネットワークのデバイスを管理しない場合、この危険性は大幅に低減されます。この設定は、たとえば、顧客デバイスを管理するサービスプロバイダーなどが使用する可能性があります。

この方法の使用が検討されるのは、次のような場合があります：

- 管理サーバーのインストールと設定を熟知しており、接続ゲートウェイを別の方法でインストール、設定したくない場合。
- 管理対象デバイスの数が多い場合。管理サーバーで管理可能な台数は 100,000 台、接続ゲートウェイは 10,000 台です。

この方法には、次の欠点もあります：

- 管理サーバーに必要なハードウェアリソースが増大し、データベースも 1 個追加する必要があります。
- デバイスに関する情報が、互いに関連付けられていない 2 つのデータベースに保管されるので（ネットワーク内の管理サーバーと DMZ）、監視が困難になります。
- デバイスをすべて管理するには、管理サーバーが階層構造に属する必要があります。これにより、監視と管理の両方が複雑化されます。セカンダリ管理サーバーのインスタンスがある場合、管理グループで構築可能な構造が制限されます。タスクとポリシーを選択し、セカンダリ管理サーバーのインスタンスへの導入方法を決定する必要があります。
- DMZ 内の管理サーバーを外部から使用し、プライマリ管理サーバーを内部で使用するように外部デバイスを設定するのは、接続ゲートウェイへの接続条件を満たして使用するように設定するよりも難易度が高くなります。
- セキュリティ上の高い危険性。管理サーバーのインスタンスが攻撃されると、管理対象のノート PC をより簡単に攻撃できるようになります。この攻撃が発生すると、ノート PC のうち 1 台が企業ネットワーク内に復帰するまで待機するだけで、ローカルエリアネットワークへの攻撃を継続することが可能になります。

管理サーバーへの外部デスクトップコンピューターの接続

常にメインネットワークの外部にあるデスクトップコンピューター（たとえば、会社の支社にあるコンピューター、売店、ATM、様々な販売拠点に設置されている端末、従業員のホームオフィスにあるコンピューター）は、管理サーバーに直接接続できません。非武装地帯（DMZ）にインストールされている接続ゲートウェイを介して管理サーバーに接続する必要があります。この設定は、これらのコンピューターにネットワークエージェントをインストールする時に行われます。

外部デスクトップコンピューターを管理サーバーに接続するには：

1. ネットワークエージェントの新規インストールパッケージを作成します。
2. 作成したインストールパッケージのプロパティを開き、［**詳細**］セクションに移動して、［**接続ゲートウェイを使用して管理サーバーに接続する**］をオンにします。

［**接続ゲートウェイを使用して管理サーバーに接続する**］設定は［**DMZ 内でネットワークエージェントを接続ゲートウェイとして使用する**］設定と互換性がありません。これらの設定の両方を同時に有効にすることはできません。

3. ［**接続ゲートウェイアドレス**］で、接続ゲートウェイのパブリックアドレスを指定します。

   接続ゲートウェイがネットワークアドレス変換（NAT）の背後にあり、独自のパブリックアドレスがない場合は、接続をパブリックアドレスから接続ゲートウェイの内部アドレスに転送するための NAT ゲートウェイルールを設定します。

4. 作成したインストールパッケージに基づいて、スタンドアロンインストールパッケージを作成します。

5. スタンドアロンインストールパッケージを電子送信により、またはリムーバブルドライブによりターゲットコンピューターに配信します。

6. スタンドアロンパッケージからネットワークエージェントをインストールします。

外部デスクトップコンピューターが管理サーバーに接続されます。

モバイルユーザー用の接続プロファイルの概要

モバイルユーザー用のノート PC（以降「デバイス」とも表記）では、企業ネットワーク内でのデバイスの現在位置によっては、管理サーバーへの接続方法を変更する、または管理サーバーを切り替える必要があります。

接続プロファイルは、Windows および macOS を実行しているデバイスでのみサポートされます。

単一の管理サーバーに対する異なるアドレスの使用

ネットワークエージェントがインストールされたデバイスは、組織の社内ネットワークかイントラネット経由で管理サーバーに接続できます。そのため、ネットワークエージェントは異なるアドレスを使用して管理サーバーに接続することが必要になる場合があります。つまり、インターネット経由で接続された場合は外部管理サーバーアドレス、社内ネットワーク経由で接続された場合は内部管理サーバーアドレスが使用されます。

これを行うには、（インターネット経由で管理サーバーに接続するための）プロファイルを、ネットワークエージェントポリシーに追加する必要があります。ポリシープロパティでプロファイルを追加します（［**接続**］セクション、［**接続プロファイル**］サブセクション）。次に、プロファイル作成ウィンドウで、［**アップデートの受信にのみ使用する**］をオフにし、［**このプロファイルで指定された管理サーバー設定と接続設定を同期する**］をオンにします。接続ゲートウェイを使用して管理サーバーにアクセスする場合（たとえば、「インターネットアクセス：DMZ 内でネットワークエージェントを接続ゲートウェイとして使用する」で説明されているような Kaspersky Security Center の設定の場合）、接続プロファイルの該当フィールドで、接続ゲートウェイのアドレスを指定する必要があります。

現在のネットワークに応じた管理サーバーの切り替え

企業に、異なる管理サーバーを使用する複数のオフィスがあり、ネットワークエージェントがインストールされた一部のデバイスが管理サーバー間を移動している場合、現在のデバイスがあるオフィスのローカルネットワークの管理サーバーに、ネットワークエージェントを接続する必要があります。

この場合、各オフィスにおいて、ネットワークエージェントのポリシーのプロパティに、管理サーバーへの接続用プロファイルを作成する必要があります。ただし、独自のホーム管理サーバーがあるホームオフィスは除きます。接続プロファイルで管理サーバーのアドレスを指定し、次のように、［**アップデートの受信にのみ使用する**］をオンまたはオフにする必要があります：

- ローカルサーバーをアップデートのダウンロードのためだけに使用する間、ネットワークエージェントをホーム管理サーバーと同期する必要がある場合は、このオプションをオンにします。
- ネットワークエージェントをローカル管理サーバーで完全に管理する必要がある場合は、このオプションをオフにします。

その後、新たに作成したプロファイルに切り替える条件を設定します。ホームオフィスを除いて、オフィスごとに少なくとも1つの条件を設定する必要があります。各条件は、オフィスのネットワーク環境特有の項目を検出することを目的とします。条件が真の場合、対応するプロファイルがアクティブになります。いずれの条件も真でない場合、ネットワークエージェントはホーム管理サーバーに切り替わります。

モバイルユーザー用の接続プロファイルの作成

管理サーバーの接続プロファイルは、Windows および macOS を実行しているデバイスでのみ使用できます。

ネットワークエージェントのモバイルユーザー用管理サーバー接続プロファイルを作成するには：

1. コンソールツリーから、ネットワークエージェントを管理サーバーに接続するためのプロファイルを作成するクライアントデバイスが属する管理グループを選択します。
2. 次のいずれかの手順を実行します：
   - グループに属するすべてのデバイスの接続プロファイルを作成する場合は、グループの作業領域の［**ポリシー**］タブでネットワークエージェントポリシーを選択します。選択したポリシーのプロパティウィンドウを開きます。
   - グループ内の1台のデバイスの接続プロファイルを作成する場合は、グループの作業領域の［**デバイス**］タブでデバイスを選択し、次の手順を実行します：
     a. 選択したデバイスのプロパティウィンドウを開きます。
     b. デバイスのプロパティウィンドウの［**アプリケーション**］セクションで、ネットワークエージェントを選択します。
     c. ネットワークエージェントのプロパティウィンドウを開きます。
3. プロパティウィンドウの［**接続**］セクションで、［**接続プロファイル**］サブセクションを選択します。
4. ［**管理サーバー接続プロファイル**］設定グループで、［**追加**］をクリックします。

   既定では、接続プロファイルのリストには <オフラインモード> プロファイルと <ホーム管理サーバー> プロファイルが含まれています。プロファイルの編集や削除はできません。

   <オフラインモード> プロファイルでは接続するサーバーが指定されていません。したがって、このプロファイルに切り替わると、クライアントデバイスにインストールされたアプリケーションがモバイルユーザーポリシー下で実行されている場合、ネットワークエージェントは管理サーバーへの接続を行いません。<オフラインモード> プロファイルは、デバイスがネットワークから切断された場合に使用できます。

<ホーム管理サーバー> プロファイルは、ネットワークエージェントのインストール中に選択された管理サーバーの接続を指定します。<ホーム管理サーバー> プロファイルは、しばらく外部ネットワークで動作していたデバイスが、ホーム管理サーバーに再接続された時に適用されます。

5. ［**新規プロファイル**］ウィンドウが開いたら、接続プロファイルを設定します：

- **プロファイル名**

  この入力フィールドでは、接続プロファイル名を表示または変更できます。

- **管理サーバー**

  プロファイルの有効化時にクライアントデバイスが接続する管理サーバーのアドレス。

- **ポート**

  接続に使用されるポート番号。

- **SSL ポート**

  SSL プロトコルを使用する接続のポート番号。

- **SSL を使用する**

  このオプションをオンにすると、SSL プロトコルを使用してセキュアなポート経由で接続が確立されます。

  既定では、このオプションはオンです。セキュアな接続を保つために、このオプションを無効にしないことを推奨します。

- ［**プロキシサーバー接続設定**］をクリックして、プロキシサーバー経由の接続を設定します。インターネットへの接続時にプロキシサーバーを使用する場合は、［**プロキシサーバーを使用する**］をオンにします。このオプションをオンにすると、設定を入力するフィールドが使用可能になります。プロキシサーバーの接続を次のように設定します：

  - **プロキシサーバーアドレス**

    インターネットへの Kaspersky Security Center の接続に使用するプロキシサーバーのアドレス。

  - **ポート番号**

    Kaspersky Security Center でプロキシサーバーへの接続を確立するポートの番号。

  - **プロキシサーバー認証**

    このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。

    ［**プロキシサーバーを使用する**］をオンにすると、この入力フィールドが使用可能になります。

- **ユーザー名**（［**プロキシサーバー認証**］をオンにすると有効になります）

  プロキシサーバーへの接続の確立に使用されるユーザーアカウント（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

- **パスワード**（［**プロキシサーバー認証**］をオンにした場合に有効になります）

  プロキシサーバーへの接続の確立に使用されるアカウントのユーザーが設定したパスワード（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

  入力したパスワードを表示するには、確認する間だけ［**入力した文字を表示する**］をクリックしたままにします。

- **接続ゲートウェイの設定**

  クライアントデバイスが管理サーバーに接続する場合に使用するゲートウェイのアドレス。

- **モバイルユーザーモードを有効にする**

  このオプションを有効にすると、このプロファイルで接続しているクライアントデバイスにインストールされているアプリケーションは、モバイルユーザーモードおよびモバイルユーザーポリシーを使用します。モバイルユーザーポリシーがアプリケーションに対して定義されていない場合は、アクティブポリシーが使用されます。

  このオプションを無効にすると、アプリケーションはアクティブポリシーを使用します。

  既定では、このオプションはオフです。

- **アップデートの受信にのみ使用する**

  このオプションをオンにすると、クライアントデバイスにインストールされているアプリケーションによってアップデートがダウンロードされる場合にのみプロファイルが使用されます。その他の処理では、ネットワークエージェントのインストール時に定義された初期接続設定で管理サーバーへの接続が確立されます。

  既定では、このオプションはオンです。

- **このプロファイルで指定された管理サーバー設定と接続設定を同期する**

  このオプションをオンにすると、ネットワークエージェントはプロファイルのプロパティで指定された設定を使用して管理サーバーに接続します。

  このオプションをオフにすると、ネットワークエージェントはインストール時に指定された元の設定を使用して管理サーバーに接続します。

  このオプションは、［**アップデートの受信にのみ使用する**］を無効にすると使用可能になります。

  既定では、このオプションはオフです。

6. ［**管理サーバーが使用できない時にモバイルユーザーモードを有効にする**］をオンにすると、クライアントデバイスにインストールされているアプリケーションは、管理サーバーが使用できない場合の接続試行で、モバイルユーザーモードのデバイス向けのポリシーのプロファイル、およびモバイルユーザー用ポリシーを使用できます。モバイルユーザーポリシーがアプリケーションに対して定義されていない場合は、アクティブポリシーが使用されます。

ネットワークエージェントを管理サーバーに接続する、モバイルユーザー用のプロファイルが作成されます。ネットワークエージェントがこのプロファイルを使用して管理サーバーに接続すると、クライアントデバイスにインストールされたアプリケーションは、モバイルユーザーモードのデバイス用のポリシーまたはモバイルユーザーポリシーを使用します。

ネットワークエージェントの別の管理サーバーへの切り替えについて

ネットワークエージェントから管理サーバーへの接続の既定の設定は、ネットワークエージェントのインストール時に定義されます。ネットワークエージェントを他の管理サーバーに切り替えるには、切り替えルールを使用できます。この機能は、Windows または macOS を実行しているデバイスにインストールされているネットワークエージェントでのみサポートされます。

スイッチングルールは、次のネットワークパラメータの変更時にトリガーできます。

- デフォルトゲートウェイアドレス。
- DHCP（Dynamic Host Configuration Protocol）サーバーの IP アドレス。
- サブネットの DNS サフィックス。
- ネットワーク DNS サーバーの IP アドレス。
- Windows ドメインのアクセシビリティ。このパラメータは Windows を実行しているデバイスでのみ使用可能です。
- サブネットアドレスとマスク。
- ネットワーク WINS サーバーの IP アドレス。このパラメータは Windows を実行しているデバイスでのみ使用可能です。
- クライアントデバイスの DNS または NetBIOS 名。
- SSL 接続アドレスのアクセシビリティ。

ネットワークエージェントを他の管理サーバーに切り替えるルールが作成されると、次のようにネットワークエージェントがネットワークパラメータの変更に対応します：

- 作成されたルールの 1 つをネットワーク設定が満たす場合、ネットワークエージェントはそのルールで指定された管理サーバーに接続します。クライアントデバイスにインストールされたアプリケーションは、モバイルユーザーポリシーへの切り替えがルールで認められている場合、モバイルユーザーポリシーに切り替わります。
- どのルールも満たされなくなった場合、ネットワークエージェントはインストール時に指定された管理サーバーへの既定の接続設定に戻します。クライアントデバイスにインストールされたアプリケーションは、アクティブポリシーに戻ります。
- 管理サーバーに接続できない場合、ネットワークエージェントはモバイルユーザーポリシーを使用します。

ネットワークエージェントがモバイルユーザーポリシーに切り替わるのは、［**管理サーバーが使用できない時にモバイルユーザーモードを有効にする**］がネットワークエージェントのポリシー設定でオンになっている場合のみです。

ネットワークエージェントの管理サーバーへの接続設定は接続プロファイルに保存されます。接続プロファイルでは、クライアントデバイスをモバイルユーザーポリシーに切り替えるルールを作成したり、プロファイルをアップデートのダウンロード専用に設定したりすることができます。

ネットワークの場所によるネットワークエージェント切り替えルールの作成

ネットワークロケーションに基づくネットワークエージェント切り替えは、Windows または macOS を実行しているデバイスでのみ使用できます。

ネットワーク設定が変更された場合に、ある管理サーバーから別の管理サーバーにネットワークエージェントを切り替えるルールを作成するには：

1. コンソールツリーで、ネットワークエージェント切り替えルールをネットワークロケーション別に作成するデバイスの管理グループを選択します。
2. 次のいずれかの手順を実行します：
   - グループの全デバイスの切り替えルールを作成する場合は、グループの作業領域に移動し、［**ポリシー**］タブでネットワークエージェントポリシーを選択します。選択したポリシーのプロパティウィンドウを開きます。
   - グループ内の1台のデバイスの切り替えルールを作成する場合は、グループの作業領域に移動して［**デバイス**］タブでデバイスを選択し、次の手順を実行します：
     a. 選択したデバイスのプロパティウィンドウを開きます。
     b. デバイスのプロパティウィンドウの［**アプリケーション**］セクションで、ネットワークエージェントを選択します。
     c. ネットワークエージェントのプロパティウィンドウを開きます。
3. ［**プロパティ**］ウィンドウが開いたら、［**接続**］セクションで［**接続プロファイル**］サブセクションを選択します。
4. ［**ネットワークロケーションの設定**］セクションで、［**追加**］をクリックします。
5. ［**新しい記述**］ウィンドウが開いたら、ネットワークロケーションの説明と切り替えルールを設定します。次のネットワークロケーションの説明に関する設定を指定します：
   - **ネットワークロケーションの説明の名前**

     ネットワークロケーションの説明の名前は 255 字以内とし、特殊文字（例："*<>?\/:|）を含むことはできません。

   - **接続プロファイルの使用**

このドロップダウンリストで、ネットワークエージェントが管理サーバーへの接続に使用する接続プロファイルを指定できます。ネットワークロケーションの説明の条件が一致すると、このプロファイルが使用されます。この接続プロファイルには、ネットワークエージェントから管理サーバーへの接続に関する設定が含まれ、クライアントデバイスがモバイルユーザーポリシーに切り替える条件も定義されています。このプロファイルは、アップデートをダウンロードする場合にのみ使用されます。

6. ［**条件の変更**］セクションの［**追加**］をクリックして、ネットワークロケーションの説明の条件リストを作成します。

   ルールに複数の条件がある場合、論理演算子「AND」を使用して組み合わせられます。ネットワークロケーションの記述により切り替えルールを適合させるには、すべてのルール切り替え条件を満たす必要があります。

7. このドロップダウンリストで、クライアントデバイスが接続されるネットワークの特性の変化に対応する値を選択できます：

   - **デフォルト接続ゲートウェイアドレス** – メインネットワークゲートウェイのアドレスが変更された場合。
   - **DHCP サーバーアドレス** – ネットワークの DHCP（Dynamic Host Configuration Protocol）サーバーの IP アドレスが変更された場合。
   - **DNS ドメイン** – サブネットの DNS サフィックスが変更された場合。
   - **DNS サーバーアドレス** – ネットワークの DNS サーバーの IP アドレスが変更された場合。
   - **Windows ドメインアクセスの可否（Windows のみ）** – クライアントデバイスが接続している Windows ドメインのステータスが変更された場合。この設定は Windows を実行しているデバイスにのみ使用してください。
   - **サブネット** – サブネットアドレスとマスクが変更された場合。
   - **WINS サーバーアドレス（Windows のみ）** – ネットワークの WINS サーバーの IP アドレスが変更された場合。この設定は Windows を実行しているデバイスにのみ使用してください。
   - **名前解決** - クライアントデバイスの DNS または NetBIOS 名が変更された場合。
   - **SSL 接続アドレスのアクセス可否** - クライアントデバイスは、（選択したオプションによって）指定されたサーバー（name：port）との SSL 接続を確立できる場合とできない場合があります。サーバーごとに、SSL 証明書を追加で指定できます。この場合、ネットワークエージェントは、SSL 接続の機能をチェックすることに加えて、サーバー証明書を検証します。証明書が一致しない場合、接続は失敗します。

8. ウィンドウが開いたら、ネットワークエージェントを別の管理サーバーに切り替える条件を指定します。ウィンドウ名は、前の手順で選択した値によって異なります。次の切り替え条件の設定を指定します：

   - **値**

     このフィールドでは、作成した条件に対して、1つ以上の値を追加することができます。

   - **リストにある値のいずれかと一致する**

このオプションをオンにすると、［**値**］リストで指定された値のいずれかが一致した場合に条件が満たされます。

既定では、このオプションがオンです。

- **リストにある値のいずれとも一致しない**

  このオプションをオンにすると、条件の値が［**値**］リストに存在しない場合に条件が満たされます。

9. ［**新しい記述**］ウィンドウで［**記述を有効にする**］をオンにして、新しいネットワークロケーションの説明の使用を有効にします。

ネットワークロケーションの記述ごとに新しい切り替えルールが作成されます。ルールの条件が満たされるたびに、ネットワークエージェントはルールで指定された接続プロファイルを使用して管理サーバーに接続します。

ネットワークロケーションの説明はリストの表示順で、ネットワークレイアウトに一致しているかどうか確認されます。ネットワークが複数の説明と一致する場合は、最初のルールが使用されます。［**上へ**］（）と［**下へ**］（）を使用して、リストのルールの順序を変更できます。

イベント通知

このセクションでは、クライアントデバイスのイベントに関して管理者への通知方法を選択する方法、およびイベントの通知設定を設定する方法について説明します。

また、Eicar テストウイルスを使用したイベント通知の配信をテストする方法についても説明します。

イベント通知の設定

Kaspersky Security Center では、クライアントデバイスで発生したイベントについて管理者に通知するように設定し、その通知方法を選択することができます：

- メール：イベントが発生すると、指定されたメールアドレスに通知を送信します。この通知のテキストを編集することができます。
- SMS：イベントが発生すると、指定された電話番号に通知を送信します。メールゲートウェイを使用して SMS 通知を送信するよう設定できます。
- 実行ファイル：デバイスでイベントが発生すると、管理コンピューターで実行ファイルが起動されます。管理者は、実行ファイルを使用して、発生した任意のイベントのパラメータを受信できます。

クライアントデバイスで発生したイベントの通知を設定するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**イベント**］タブを選択します。

3. ［**通知とイベントのエクスポートの設定**］をクリックして、ドロップダウンリストから［**通知の設定**］を選択します。

   ［**プロパティ：イベント**］ウィンドウが表示されます。

4. ［**通知**］セクションで、通知の方法（メール、SMS、ファイルの実行）を選択して通知の設定を定義することができます。

   - **メール**

［**メール**］タブで、イベントのメール通知を設定できます。

［**受信者（メールアドレス）**］に、通知の送信先となるメールアドレスを指定します。このフィールドでは、複数のアドレスをセミコロンで区切って指定することができます。

［**SMTP サーバー**］に、メールサーバーのアドレスをセミコロンで区切って指定します。次の値を使用できます：

- IPv4 / IPv6 アドレス
- デバイスの Windows ネットワーク名（NetBIOS 名）
- SMTP サーバーの DNS 名

［**SMTP サーバーのポート**］に、SMTP サーバーの通信ポート番号を指定します。既定のポート番号は 25 です。

［**DNS MX ルックアップを使用**］を有効にすると、IP アドレスの複数の MX レコードを、SMTP サーバーの同一の DNS 名に使用できます。同一 DNS 名に複数の MX レコードが存在し、各レコードのメール受信の優先度の値が異なる場合があります。管理サーバーは SMTP サーバーへのメール通知の 送信を、MX レコードの優先度の昇順に試行します。既定では、このオプションはオフです。

［**DNS MX ルックアップを使用**］を有効にし、TLS 設定の使用は有効にしない場合、メール通知を保護する追加の方法として、サーバーデバイスで DNSSEC 設定を使用することを推奨します。

［**設定**］をクリックし、通知の詳細設定を指定します：

- 件名（メールの件名）
- 送信者のメールアドレス
- ESMTP 認証設定

SMTP サーバーの ESMTP 認証オプションを有効にする場合、SMTP サーバーの認証用アカウントを指定する必要があります。

- SMTPサーバーの TLS 設定：
  - **TLS を使用しない**

    メールの暗号化を無効にする場合に、このオプションを選択できます。
  - **TLS を使用する（SMTP サーバーがサポートする場合）**

    SMTP サーバーに TLS 接続を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは TLS を使用せずに SMTP サーバーへ接続します。
  - **常に TLS を使用し、サーバー証明書の有効性をチェックする**

    TLS 認証設定を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは SMTP サーバーへ接続できません。

SMTP サーバーの接続の保護をより強化する目的で、このオプションを使用することを推奨します。このオプションを選択すると、TLS 接続の認証設定を指定できます。

［**常に TLS を使用し、サーバー証明書の有効性をチェックする**］を選択した場合は、SMTP サーバーの認証用の証明書を指定し、TLS の任意のバージョンを介した通信を有効にするか、TLS 1.2 以降のバージョンのみを介した通信を有効にするかを選択できます。また、SMTP サーバーでクライアント認証に使用する証明書を指定することもできます。

SMTP サーバーの TLS 設定を指定できます：

- SMTP サーバーの証明書ファイルを参照します：

信頼できる証明書認証局から証明書のリストを含むファイルを受け取り、ファイルを管理サーバーへアップロードできます。Kaspersky Security Center は、SMTP サーバーの証明書も信頼できる証明書認証局によって署名されているかどうかをチェックします。信頼できる証明書認証局から SMTP サーバーの証明書を受け取っていない場合、Kaspersky Security Center は SMTP サーバーに接続できません。

- クライアント証明書ファイルを参照します：

信頼できる認証局など、任意の発行元から受け取った証明書を使用できます。次のいずれかの証明書タイプを使用して、証明書とその秘密鍵を指定する必要があります：

- X-509証明書：

証明書を含むファイルと秘密鍵を含むファイルを指定する必要があります。両方のファイルは相互に依存せず、ファイルを読み込む順序は重要ではありません。両方のファイルを読み込む時は、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

- pkcs12 コンテナー：

証明書とその秘密鍵を含む単一のファイルをアップロードする必要があります。ファイルの読み込み時に、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

［**通知メッセージ**］には、イベント発生時に送信される、イベントに関する情報を含む標準的なメッセージが表示されます。このメッセージには、イベント名、デバイス名、ドメイン名といった代替パラメータが含まれます。イベントに関連する詳細情報の代替パラメータを追加して、メッセージを編集できます。代替パラメータのリストは、このフィールドの右側にあるボタンをクリックすると表示されます。

通知テキストにパーセント記号「%」が含まれる場合、メッセージを送信するには 2 つ続けて入力する必要があります。たとえば、「CPU の負荷 100%%」のように入力します。

［**通知数の上限を設定する**］をクリックし、指定した時間内に送信できる最大通知数を指定します。

［**テストメッセージの送信**］をクリックし、通知の設定が適切かどうかをチェックします。指定したメールアドレスに、テストの通知が送信されます。

- SMS

［**SMS**］タブでは、携帯電話へ送信する様々なイベントの SMS 通知を設定できます。SMS メッセージはメールゲートウェイを通して送信されます。

［**宛先（メールアドレス）**］に、通知の送信先となるメールアドレスを指定します。このフィールドでは、複数のアドレスをセミコロンで区切って指定することができます。通知は、指定したメールアドレスに関連付けられている電話番号に送信されます。

［**SMTP サーバー**］に、メールサーバーのアドレスをセミコロンで区切って指定します。次の値を使用できます：

- IPv4 / IPv6 アドレス
- デバイスの Windows ネットワーク名（NetBIOS 名）
- SMTP サーバーの DNS 名

［**SMTP サーバーのポート**］に、SMTP サーバーの通信ポート番号を指定します。既定のポート番号は 25 です。

［**設定**］をクリックし、通知の詳細設定を指定します：

- 件名（メールの件名）
- 送信者のメールアドレス
- ESMTP 認証設定

必要に応じて、SMTP サーバーの ESMTP 認証オプションを有効にする場合、SMTP サーバーの認証用アカウントを指定できます。

- SMTPサーバーの TLS 設定

TLS の使用を無効にしたり、SMTP サーバーがこのプロトコルをサポートしている場合に TLS を使用するように設定したり、TLS のみの使用を強制したりすることができます。TLS のみを使用する場合は、SMTP サーバーの認証用の証明書を指定し、TLS の任意のバージョンを介した通信を有効にするか、TLS 1.2 以降のバージョンのみを介した通信を有効にするかを選択できます。また、TLS のみを使用する場合、SMTP サーバーのクライアント認証に使用する証明書を指定できます。

- SMTP サーバーの証明書ファイルを参照します

信頼できる証明書認証局から証明書のリストを含むファイルを受け取り、ファイルを Kaspersky Security Center にアップロードできます。Kaspersky Security Center は、SMTP サーバーの証明書も信頼できる証明書認証局によって署名されているかどうかをチェックします。信頼できる証明書認証局から SMTP サーバーの証明書を受け取っていない場合、Kaspersky Security Center は SMTP サーバーに接続できません。

証明書とその秘密鍵を含む単一のファイルをアップロードする必要があります。ファイルの読み込み時に、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。［**通知メッセージ**］には、イベント発生時に送信される、イベントに関する情報を含む標準的なメッセージが表示されます。このメッセージには、イベント名、デバイス名、ドメイン名といった代替パラメータが含まれます。イベントに関連する詳細情報の代替パラメータを追加して、メッセージを編集できます。代替パラメータのリストは、このフィールドの右側にあるボタンをクリックすると表示されます。

通知テキストにパーセント記号「%」が含まれる場合、メッセージを送信するには 2 つ続けて入力する必要があります。たとえば、「CPU の負荷 100%%」のように入力します。

［**通知数の上限を設定する**］をクリックし、指定した時間内に送信できる最大通知数を指定します。

［**テストメッセージの送信**］をクリックし、通知が正しく設定されているかチェックします。指定した受信者に、テストの通知が送信されます。

- 実行ファイル

この通知方法を選択すると、イベントの発生時に起動するアプリケーションを入力フィールドで選択できます。

［**通知数の上限を設定する**］をクリックすると、指定した時間内に送信できる最大通知数を指定できます。

［**テストメッセージの送信**］をクリックすると、通知が正しく設定されているか確認することができます。指定したメールアドレスにテスト通知が送信されます。

5. ［**通知メッセージ**］で、イベント発生時にアプリケーションが送信するテキストを入力します。

   テキストフィールドの右にあるドロップダウンリストを使用して、イベントの詳細（イベントの説明や発生時刻など）に置換される文字列を追加できます。

   通知テキストにパーセント記号（%）が含まれる場合、メッセージが送信されるようにするには、この記号を 2 回続けて入力する必要があります。たとえば、「CPU の負荷 100%%」のように入力します。

6. ［**テストメッセージの送信**］をクリックして、通知が正しく設定されたかどうかを確認します。

   指定されたユーザーにテストの通知が送信されます。

7. ［**OK**］をクリックして変更内容を保存します。

クライアントデバイスで発生するすべてのイベントに、再調整された通知設定が適用されます。

管理サーバーの設定、ポリシーの設定、またはアプリケーションの設定で、［**イベントの設定**］で指定された設定を特定のイベントについて上書きできます。

テストの通知

イベント通知が送信されているかどうかを確認するには、クライアントデバイスで EICAR テスト「ウイルス」を検知したことの通知を使用します。

イベント通知の送信を検証するには：

1. クライアントデバイスでファイルシステムのリアルタイム保護タスクを停止し、EICAR テスト「ウイルス」をクライアントデバイスにコピーします。ファイルシステムのリアルタイム保護タスクを再び有効にします。

2. EICAR「ウイルス」があるクライアントデバイスを含む管理グループまたはそのデバイスに対してスキャンタスクを実行します。

   スキャンタスクが正しく設定されていれば、テスト「ウイルス」が検知されます。通知が正しく設定されていれば、ウイルスが検知されたと通知されます。

   ［**管理サーバー**］フォルダーの作業領域で、［**イベント**］タブの［**最近のイベント**］を選択すると、「ウイルス」を検知した記録が表示されます。

EICAR テスト「ウイルス」には、デバイスに損害を与えるコードは含まれていません。ただし、ほとんどの製造元のセキュリティ製品で、このファイルはウイルスと判断されます。このテスト「ウイルス」は、EICAR の公式 Web サイトからダウンロードできます。

実行ファイルの起動により表示されるイベント通知

Kaspersky Security Center は、実行ファイルを起動することにより、クライアントデバイスでのイベントについて管理者に通知できます。この実行ファイルには、管理者にリレーするイベントのプレースホルダーを持つ別の実行ファイルを含める必要があります（下表参照）。

イベントを説明するためのプレースホルダー

プレースホルダー	プレースホルダーの説明
%SEVERITY%	イベントの重要度。指定可能な値： • **情報** • **警告** • **エラー** • **緊急**
%COMPUTER%	イベントが発生したデバイスの名前。 デバイス名の最大長は 256 文字です。
%DOMAIN%	イベントが発生したデバイスのドメイン名。
%EVENT%	イベントタイプの名前。 イベントタイプ名の最大長は 50 文字です。
%DESCR%	イベントの説明。 説明の最大長は 1000 文字です。
%RISE_TIME%	イベント作成時間。
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	タスク名。 タスク名の最大長は 100 文字です。
%KL_PRODUCT%	製品名。
%KL_VERSION%	製品のバージョン番号。
%KLCSAK_EVENT_SEVERITY_NUM%	イベントの重要度番号。指定可能な値： • 1 – **情報** • 2 – **警告** • 3 – **エラー** • 4 – **緊急**
%HOST_IP%	イベントが発生したデバイスの IP アドレス。
%HOST_CONN_IP%	イベントが発生したデバイスの接続 IP アドレス。

例：
イベント通知は、%COMPUTER% プレースホルダーを持つ実行ファイル（script2.bat など）を内部で起動する別の実行ファイル（script1.bat など）によって送信されます。イベントが発生すると、管理者のデバイスでファイル script1.bat が起動され、それが %COMPUTER% プレースホルダーを持つファイル script2.bat を起動します。次に管理者は、イベントが発生したデバイスの名前を受信します。

TLS による通信の暗号化

社内の企業ネットワークの脆弱性を修正するために、TLS プロトコルを使用したトラフィックの暗号化を有効にすることができます。管理サーバーと iOS MDM サーバーで TLS 暗号化プロトコルとサポートされている暗号スイートを有効にすることができます。Kaspersky Security Center は、TLS プロトコルのバージョン 1.0、1.1、1.2 および 1.3 をサポートしています。必要な暗号化プロトコルと暗号化スイートを選択できます。

Kaspersky Security Center は、自己署名証明書を使用します。iOS デバイスの追加構成は必要ありません。証明書を自分で用意して使用することもできます。信頼できる証明機関から発行された証明書を使用することを推奨します。

管理サーバー

管理サーバーで許可される暗号化プロトコルと暗号化スイートを設定するには、次の手順に従います：

1. Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

2. SrvUseStrictSslSettings フラグを使用し、管理サーバーで許可される暗号化プロトコルと暗号化スイートを指定します。次のコマンドを入力します：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <値> -t d
   ```

   SrvUseStrictSslSettings フラグの <値> パラメータを指定します：

   - 4—TLS 1.2 および TLS 1.3 プロトコルのみが有効になります。また、TLS_RSA_WITH_AES_256_GCM_SHA384 の暗号スイートも有効になります（この暗号スイートは、Kaspersky Security Center との下位互換性のために必要です）。これは既定値です。

     TLS 1.2 プロトコルでサポートされる暗号スイート：

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384（TLS_RSA_WITH_AES_256_GCM_SHA384 を使用した暗号スイート）
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     TLS 1.3 プロトコルでサポートされる暗号スイート：

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - 5—TLS 1.2 および TLS 1.3 プロトコルのみが有効になります。TLS 1.2 および TLS 1.3 プロトコルの場合、以下にリストされている特定の暗号スイートがサポートされています。

     TLS 1.2 プロトコルでサポートされる暗号スイート：

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

TLS 1.3 プロトコルでサポートされる暗号スイート：

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

SrvUseStrictSslSettings フラグのパラメータ値として 0、1、2、または 3 を使用することは推奨しません。これらのパラメータ値は、セキュアでない TLS プロトコルバージョン（TLS 1.0 および TLS 1.1 プロトコル）およびセキュアでない暗号スイートに対応しており、以前の Kaspersky Security Center バージョンとの下位互換性のためにのみ使用されます。

3. 次の Kaspersky Security Center15.1 サービスを再起動します：
   - 管理サーバー
   - Web サーバー
   - アクティベーションプロキシ

TLS プロトコルを使用したトラフィック暗号化が有効になります。

KLTR_TLS12_ENABLED フラグおよび KLTR_TLS13_ENABLED フラグを使用して、それぞれ TLS 1.2 および TLS 1.3 プロトコルのサポートを有効にすることができます。これらのフラグは既定で有効になっています。

TLS 1.2 および TLS 1.3 プロトコルのサポートを有効または無効にするには：

1. klscflag ユーティリティを実行します。

   Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

2. 管理者権限を使用し、Windows コマンドプロンプトで以下のいずれかのコマンドを入力します：
   - 次のコマンドを使用して、TLS 1.2 プロトコルのサポートを有効または無効にします：

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <値> -t d
     ```

   - 次のコマンドを使用して、TLS 1.3 プロトコルのサポートを有効または無効にします：

```
klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <値> -
t d
```

フラグの <値> パラメータを指定します：

- `1`—TLS プロトコルのサポートを有効にします。
- `0`—TLS プロトコルのサポートを無効にします。

iOS MDM サーバー

iOS デバイスと iOS MDM サーバー間の接続は既定で暗号化されます。

iOS MDM サーバーで許可される暗号化プロトコルと暗号化スイートを指定するには：

1. iOS MDM サーバーがインストールされたクライアントデバイスのシステムレジストリを開きます（たとえば、ローカルで［**スタート**］→［**ファイル名を指定して実行**］で regedit コマンドを使用します）。
2. 次のレジストリエントリに移動します：
   - 32 ビットシステム：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor
   - 64 ビットシステム：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSM
3. `StrictSslSettings` という名前のキーを作成します。
4. キーの種別に `DWORD` を指定します。
5. 次のようにキーの値を設定します：
   - 2 - TLS 1.0、TLS 1.1、および TLS 1.2 プロトコルが有効になります。
   - 3 - TLS 1.2 プロトコルのみが有効になります（既定値）。
6. Kaspersky Security Center iOS MDM サーバーサービスを再起動します。

インターフェイスの設定

Kaspersky Security Center のインターフェイスを設定することができます：

- 使用している機能に応じて、コンソールツリー、作業領域、およびオブジェクト（フォルダーやセクション）のプロパティウィンドウのオブジェクトの表示 / 非表示を切り替えられます。
- メインウィンドウの要素（コンソールツリーや、［**操作**］および［**表示**］などの標準的なメニュー）の表示 / 非表示を切り替えられます。

現在使用している機能に基づいて Kaspersky Security Center のインターフェイスを設定するには：

1. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。

2. メインウィンドウのメニューバーで［**表示**］→［**インターフェイスの設定**］の順に選択します。

3. ［**インターフェイスの設定**］ウィンドウが開いたら、インターフェイス要素を表示する方法を次のチェックボックスを使用して設定します：

- **脆弱性とパッチ管理の表示**

  このオプションをオンにすると、［**リモートインストール**］フォルダーの［**デバイスイメージの導入**］サブフォルダーが表示され、［**リポジトリ**］フォルダーに［**ハードウェア**］サブフォルダーが表示されます。

  クイックスタートウィザードが終了していない場合、このチェックボックスは既定で有効です。クイックスタートウィザードが終了している場合、このチェックボックスは既定でオフです。

  このオプションを有効にしない場合、システム管理ライセンスを持っている場合でも、メニュー項目の［**RDP セッションの作成**］および［**Windows デスクトップ共有**］は使用できません。

- **データ暗号化と保護機能の表示**

  このオプションをオンにすると、コンソールツリーに［**データ暗号化と保護機能**］フォルダーが表示されます。

  既定では、このオプションはオンです。

- **エンドポイントコントロール設定の表示**

  このオプションをオンにすると、Kaspersky Endpoint Security for Windows ポリシーのプロパティウィンドウの［**セキュリティコントロール**］セクションに、次のサブセクションが表示されます：

  - **アプリケーションコントロール**
  - **デバイスコントロール**
  - **ウェブコントロール**
  - **アダプティブアノマリーコントロール**

  このオプションをオフにすると、上記のサブセクションは［**セキュリティコントロール**］セクションに表示されません。

  既定では、このオプションはオンです。

- **モバイルデバイス管理の表示**

  このオプションをオフにすると、**モバイルデバイス管理**機能が使用可能になります。アプリケーションを再起動した後、コンソールツリーに［**モバイルデバイス**］フォルダーが表示されます。

  既定では、このオプションはオンです。

- **セカンダリ管理サーバーの表示**

このチェックボックスをオンにすると、管理コンソールツリーに、管理グループに含まれるセカンダリ管理サーバーおよび仮想管理サーバーのフォルダーが表示されます。これにより、セカンダリ管理サーバーおよび仮想管理サーバーに関連する機能（セカンダリ管理サーバーへのアプリケーションをリモートインストールするタスクの作成など）が使用可能になります。

既定では、このチェックボックスはオフです。

- **セキュリティ設定タブの表示**

  このオプションをオンにすると、管理サーバー、管理グループおよびその他オブジェクトのプロパティウィンドウに［**セキュリティ**］セクションが表示されます。このオプションにより、オブジェクトを扱うカスタム権限をユーザーおよびユーザーグループに付与できます。

  既定では、このオプションはオフです。

4. ［OK］をクリックします。

いくつかの変更は、適用するためにメインウィンドウを一旦閉じて再度開く必要があります。

メインウィンドウ内の要素の表示を設定するには：

1. メインウィンドウのメニューバーで［**表示**］→［**設定**］の順に選択します。
2. 開かれる［**表示のカスタマイズ**］ウィンドウで、チェックボックスを使用してメインウィンドウの要素の表示方法を設定します。
3. ［OK］をクリックします。

ネットワーク接続されたデバイスの検出

このセクションでは Kaspersky Security Center のインストール後に必要となる手順について説明します。

ネットワーク接続されたデバイスの検出シナリオ

セキュリティ製品のインストール前にデバイスの検索を実行する必要があります。管理サーバーは、検出されたデバイスに関する情報を受け取り、ポリシーを通じてデバイスを管理することができるようにします。ネットワークで使用可能なデバイスのリストを更新するには、定期的なネットワークポーリングが必要です。

ネットワークポーリングを開始する前に、SMB プロトコルが有効になっていることを確認してください。有効でない場合、Kaspersky Security Center はポーリングされたネットワークでデバイスを検出できません。SMB プロトコルを有効にするには、オペレーティングシステムの指示に従ってください。

ネットワーク接続されたデバイスの検出は、次の手順で進行します：

1. **デバイスの検出**

クイックスタートウィザードの説明に従って最初のデバイス検出を実行すると、コンピューター、タブレット、スマートフォンなどのネットワーク接続されたデバイスが検出されます。デバイスの検出は手動でも実行できます。

2. **ポーリングスケジュールを設定**

   どのポーリングタイプを定期的に使用するかを決定します。目的のタイプを有効にして、ポーリングスケジュールを自由に設定することができます。「ネットワークポーリングの頻度に関する推奨事項」を参照してください。

3. **検出されたデバイスを管理グループに追加するルールの設定（任意）**

   ネットワーク内に新しいデバイスが追加された場合、これらのデバイスは定期的なポーリング中に検出され、［**未割り当てデバイス**］グループに含まれます。デバイスの移動ルールを設定することで、［**管理対象デバイス**グループへのデバイスの割り当てを自動化することができます。また、［保持ルール］を確立することもできます。

   手順 3 をスキップすると、新しく検出されたデバイスは［**未割り当てデバイス**］グループに割り当てられます。必要に応じて、これらのデバイスを［**管理対象デバイス**］グループに手動で移動できます。デバイスを［**管理対象デバイス**］グループに手動で移動する場合、各デバイスの情報を分析し、管理グループに移動するかどうかや具体的にどの管理グループに移動するかを決定することができます。

結果

これらのステップがすべて完了すると、次の状態を実現できます：

- Kaspersky Security Center 管理サーバーがネットワーク内のデバイスを検出し、その情報を利用できるようになります。
- ポーリングのスケジュールが設定され、指定したスケジュールに従ってポーリングが実行されます。
- 新しく検出されたデバイスは、設定されたルールに従って配置されます（または、ルールが設定されていない場合、デバイスは［**未割り当てデバイス**］グループに割り当てられたままになります）。

未割り当てデバイス

このセクションでは、企業ネットワークの管理グループに含まれていないデバイスの管理について説明します。

デバイスの検索

Kaspersky Security Center で利用できるデバイスの検索方法の種別と、それぞれの方法の使用方法を説明しています。

管理サーバーは、ネットワークの構造およびネットワーク上のデバイスに関する情報を定期的なポーリングによって取得します。情報は管理サーバーのデータベースに保存されます。管理サーバーが実行可能なポーリングの種類は、次の通りです：

- **Windows ネットワークのポーリング**：管理サーバーでは、簡易ポーリングと完全ポーリングの 2 種類の Windows ネットワークポーリングを実行できます。簡易ポーリングでは管理サーバーが、すべてのネットワークドメインとワークグループ内のデバイスの NetBIOS 名リストの情報のみ取得します。完全ポーリングでは、各クライアントデバイスに対して、オペレーティングシステムの名前、IP アドレス、DNS 名、NetBIOS 名などより詳細な情報が要求されます。既定では、簡易ポーリングと完全ポーリングの両方がオ

ンです。Windows ネットワークのポーリングでは、一部の状況（例：UDP 137、UDP 138、TCP 139 ポートがルーターまたはファイアウォールで閉じている）ではデバイスの検出に失敗する場合があります。

- **Active Directory のポーリング**：管理サーバーでは、Active Directory の単位構造と Active Directory グループ内のデバイスの DNS 名に関する情報が取得されます。既定では、この種別のポーリングはオンです。Active Directory のポーリングは、Active Directory を使用している場合に推奨されます。Active Directory を使用していない場合は、管理サーバーでデバイスは検出されません。Active Directory を使用していてもネットワークデバイスの一部が Active Directory のメンバーとしてリストに含まれていない場合、これらのデバイスは Active Directory のポーリングで検出できません。

- **IP アドレス範囲のポーリング**：管理サーバーが ICMP パケットまたは NBNS プロトコルを使用して指定の IP アドレス範囲をポーリングし、IP アドレス範囲内にあるデバイスの完全なデータを作成します。既定では、この種別のポーリングはオフです。Windows ネットワークのポーリングや Active Directory のポーリングを使用する場合は、この種別のポーリングの使用は推奨されません。

- **Zeroconf ポーリング**：ゼロコンフィギュレーションネットワーキング（zero-configuration networking）（「*Zeroconf*」とも表記）を使用して IPv6 ネットワークを検索するディストリビューションポイント。既定では、この種別のポーリングはオフです。ディストリビューションポイントが Linux を実行している場合は Zeroconf ポーリングを使用できます。

デバイス移動ルールを設定しオンにしている場合、新たに検出されたデバイスは自動的に**管理対象デバイス**グループに含まれます。移動ルールがオンでない場合、新たに検出されたデバイスは自動的に**未割り当てデバイス**グループに含まれます。

デバイスの検索の各種別に対して設定を編集できます。たとえば、ポーリングのスケジュールや、ポーリングの対象をドメインフォレストとするか特定のドメインのみにするかなどの設定が可能です。

ネットワークポーリングを開始する前に、SMB プロトコルが有効になっていることを確認してください。有効でない場合、Kaspersky Security Center はポーリングされたネットワークでデバイスを検出できません。SMB プロトコルを有効にするには、オペレーティングシステムの指示に従ってください。

Windows ネットワークのポーリング

Windows ネットワークのポーリングの概要

簡易ポーリングでは管理サーバーが、すべてのネットワークドメインとワークグループ内のデバイスの NetBIOS 名リストの情報のみ取得します。完全ポーリングでは、各クライアントデバイスに対して次の情報が要求されます：

- オペレーティングシステムの名前
- IP アドレス
- DNS 名
- NetBIOS 名

簡易ポーリングと完全ポーリングの両方で次の要件を満たす必要があります：

- UDP 137/138、TCP 139、UDP 445、TCP 445 ポートをネットワーク内で利用できる必要があります。
- SMB プロトコルが有効になっています。

- Microsoft のコンピューターブラウザーサービスを使用し、管理サーバー上でプライマリブラウザーコンピューターが有効である必要があります。
- Microsoft のコンピューターブラウザーサービスを必ず使用し、クライアントデバイス上でプライマリブラウザーコンピューターが有効であり、かつ次の条件を満たす必要があります：
  - ネットワークデバイスが 32 台以内の場合、1 台以上のデバイスで実行する
  - ネットワークデバイス 32 台につき、1 台以上のデバイスで

完全ポーリングは簡易ポーリングを 1 回以上実行している場合にのみ実行できます。

Windows ネットワークのポーリング設定の表示と変更

Windows ネットワークのポーリング設定を変更するには：

1. コンソールツリーで、［**デバイスの検索**］フォルダーの［**ドメイン**］サブフォルダーを選択します。

   ［**今すぐポーリング**］をクリックすると、［**未割り当てデバイス**］フォルダーから［**デバイスの検索**］フォルダーに進むことができます。

   ［**ドメイン**］サブフォルダーの作業領域で、デバイスのリストが表示されます。

2. ［**今すぐポーリング**］をクリックします。

   ドメインのプロパティウィンドウが開きます。必要に応じて、Windows ネットワークのポーリング設定を編集します：

   - **Windows ネットワークのポーリングを有効にする**

     既定ではこのオプションが選択されます。Windows ネットワークのポーリングを実行する必要がない場合（例：Active Directory のポーリングで十分だと考えられる場合）、このオプションをオフにできます。

   - **簡易ポーリングのスケジュールを設定する**

既定の時間は 15 分です。

簡易ポーリングでは管理サーバーが、すべてのネットワークドメインとワークグループ内のデバイスの NetBIOS 名リストの情報のみ取得します。

古いデータは次回のポーリングで取得されたデータで置換されます。

ポーリングスケジュールには次のオプションがあります：

- **N 日ごと**

  指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。
  既定では、現在のシステム日時から、1 日ごとにポーリングが実行されます。

- **N 分ごと**

  指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。
  既定では、現在のシステム時刻から、5 分ごとにポーリングが実行されます。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。
  既定では、毎週金曜日の午後 6 時にポーリングが実行されます。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。
  既定では、月内のいかなる日付も選択されておらず、開始時刻は午後 6 時です。

- **未実行のタスクを実行する**

  ポーリングの実行がスケジュールされていた時刻に管理サーバーがオフまたは接続できなかった場合は、管理サーバーがオンになった時に即座にポーリングを実行させるか、ポーリングの次回のスケジュールまで待機するかを選択できます。

  このオプションをオンにすると、管理サーバーがオンになるとすぐにポーリングを開始します。

  このオプションをオフにすると、管理サーバーはポーリングの次回のスケジュールまでポーリングの実行を待機します。

  既定では、このオプションはオンです。

- **完全ポーリングのスケジュールを設定する**

既定では、時間は1時間です。古いデータは次回のポーリングで取得されたデータで置換されます。
ポーリングスケジュールには次のオプションがあります：

- **N日ごと**

  指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。
  既定では、現在のシステム日時から、1日ごとにポーリングが実行されます。

- **N分ごと**

  指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。
  既定では、現在のシステム時刻から、5分ごとにポーリングが実行されます。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。
  既定では、毎週金曜日の午後6時にポーリングが実行されます。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。
  既定では、月内のいかなる日付も選択されておらず、開始時刻は午後6時です。

- **未実行のタスクを実行する**

  ポーリングの実行がスケジュールされていた時刻に管理サーバーがオフまたは接続できなかった場合は、管理サーバーがオンになった時に即座にポーリングを実行させるか、ポーリングの次回のスケジュールまで待機するかを選択できます。
  このオプションをオンにすると、管理サーバーがオンになるとすぐにポーリングを開始します。
  このオプションをオフにすると、管理サーバーはポーリングの次回のスケジュールまでポーリングの実行を待機します。
  既定では、このオプションはオンです。

すぐにポーリングを実行するには、［**今すぐポーリング**］をクリックします。両方の種別のポーリングが開始されます。

仮想管理サーバーでは、ディストリビューションポイントのプロパティウィンドウの［**デバイスの検索**］セクションで、Windowsネットワークの検索設定を表示および編集できます。

Active Directoryのポーリング

Active Directory のポーリングは、Active Directory を使用している場合に利用してください。Active Directory を使用していない場合は、その他の種別のポーリングの利用を推奨します。Active Directory を使用していてもネットワークデバイスの一部が Active Directory のメンバーとしてリストに含まれていない場合、これらのデバイスは Active Directory のポーリングで検出できません。

ネットワークポーリングを開始する前に、SMB プロトコルが有効になっていることを確認してください。有効でない場合、Kaspersky Security Center はポーリングされたネットワークでデバイスを検出できません。SMB プロトコルを有効にするには、オペレーティングシステムの指示に従ってください。

Active Directory のポーリング設定の表示と変更

Active Directory グループのポーリング設定の表示と変更を行うには：

1. コンソールツリーで、［**デバイスの検索**］フォルダーの［**Active Directory**］サブフォルダーを選択します。

   または、［**今すぐポーリング**］をクリックすると、［**未割り当てデバイス**］フォルダーから［**デバイスの検索**］フォルダーに進むことができます。

2. ［**ポーリングの設定**］をクリックします。

   Active Directory のプロパティウィンドウが開きます。必要に応じて、Active Directory のポーリング設定を編集します：

   - **Active Directory のポーリングを有効にする**

     既定ではこのオプションが選択されます。ただし、Active Directory を使用していない場合は、ポーリングの結果として取得される情報はありません。この場合、オプションをオフにできます。

   - **ポーリングのスケジュールを設定する**

既定では、時間は1時間です。古いデータは次回のポーリングで取得されたデータで置換されます。
ポーリングスケジュールには次のオプションがあります：

- **N 日ごと**

  指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。
  既定では、現在のシステム日時から、1日ごとにポーリングが実行されます。

- **N 分ごと**

  指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。
  既定では、現在のシステム時刻から、5分ごとにポーリングが実行されます。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。
  既定では、毎週金曜日の午後6時にポーリングが実行されます。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。
  既定では、月内のいかなる日付も選択されておらず、開始時刻は午後6時です。

- **未実行のタスクを実行する**

  ポーリングの実行がスケジュールされていた時刻に管理サーバーがオフまたは接続できなかった場合は、管理サーバーがオンになった時に即座にポーリングを実行させるか、ポーリングの次回のスケジュールまで待機するかを選択できます。

  このオプションをオンにすると、管理サーバーがオンになるとすぐにポーリングを開始します。

  このオプションをオフにすると、管理サーバーはポーリングの次回のスケジュールまでポーリングの実行を待機します。

  既定では、このオプションはオンです。

- **詳細**

どの Active Directory ドメインでポーリングを実行するか選択できます：

- Kaspersky Security Center が属している Active Directory ドメイン
- Kaspersky Security Center が属しているドメインフォレスト
- Active Directory ドメインを指定したリスト

  このオプションを選択した場合、ポーリングの範囲にドメインを追加できます。

  - ［**追加**］をクリックします。
  - それぞれのフィールドで、ドメインコントローラーのアドレス、アクセスに必要なアカウントの名前とパスワードを指定します。
  - ［OK］をクリックして、変更内容を保存します。

  リストに含まれているドメインコントローラーのアドレスを変更または削除するには、［**変更**］または［**削除**］をクリックします。

- ［OK］をクリックして、変更内容を保存します。

すぐにポーリングを実行するには、［**今すぐポーリング**］をクリックします。

仮想管理サーバーでは、ディストリビューションポイントのプロパティウィンドウの［**デバイスの検索**］セクションで、Active Directory グループのポーリング設定を表示および編集できます。

IP アドレス範囲のポーリング

管理サーバーが ICMP パケットまたは NBNS プロトコルを使用して指定の IP アドレス範囲をポーリングし、IP アドレス範囲内にあるデバイスの完全なデータを作成します。既定では、この種別のポーリングはオフです。Windows ネットワークのポーリングや Active Directory のポーリングを使用する場合は、この種別のポーリングの使用は推奨されません。

ネットワークポーリングを開始する前に、SMB プロトコルが有効になっていることを確認してください。有効でない場合、Kaspersky Security Center はポーリングされたネットワークでデバイスを検出できません。SMB プロトコルを有効にするには、オペレーティングシステムの指示に従ってください。

IP アドレス範囲のポーリング設定の表示と変更

IP アドレス範囲のポーリング設定の表示と変更を行うには：

1. コンソールツリーで、［**デバイスの検索**］フォルダーの［**IP アドレス範囲**］サブフォルダーを選択します。

   ［**今すぐポーリング**］をクリックすると、［**未割り当てデバイス**］フォルダーから［**デバイスの検索**］フォルダーに進むことができます。

2. 必要に応じて、［**IP アドレス範囲**］サブフォルダーで［**サブネットの追加**］をクリックしてポーリング対象の IP アドレス範囲を追加し、［OK］をクリックします。

3. ［**ポーリングの設定**］をクリックします。

IP アドレス範囲のプロパティウィンドウが開きます。必要に応じて、IP アドレス範囲のポーリング設定を編集できます：

- **IP アドレス範囲のポーリングを有効にする**

  既定では、このオプションはオフです。Windows ネットワークのポーリングや Active Directory のポーリングを使用する場合は、この種別のポーリングの使用は推奨されません。

- **ポーリングのスケジュールを設定する**

  既定では、時間は 420 分です。古いデータは次回のポーリングで取得されたデータで置換されます。

  ポーリングスケジュールには次のオプションがあります：

  - **N 日ごと**

    指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。

    既定では、現在のシステム日時から、1 日ごとにポーリングが実行されます。

  - **N 分ごと**

    指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。

    既定では、現在のシステム時刻から、5 分ごとにポーリングが実行されます。

  - **曜日ごと**

    指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。

    既定では、毎週金曜日の午後 6 時にポーリングが実行されます。

  - **毎月、選択した週の指定日**

    毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。

    既定では、月内のいかなる日付も選択されておらず、開始時刻は午後 6 時です。

  - **未実行のタスクを実行する**

    ポーリングの実行がスケジュールされていた時刻に管理サーバーがオフまたは接続できなかった場合は、管理サーバーがオンになった時に即座にポーリングを実行させるか、ポーリングの次回のスケジュールまで待機するかを選択できます。

    このオプションをオンにすると、管理サーバーがオンになるとすぐにポーリングを開始します。

    このオプションをオフにすると、管理サーバーはポーリングの次回のスケジュールまでポーリングの実行を待機します。

    既定では、このオプションはオンです。

すぐにポーリングを実行するには、［**今すぐポーリング**］をクリックします。このボタンは、［**IP アドレス範囲のポーリングを有効にする**］をオンにすると使用可能になります。

仮想管理サーバーでは、ディストリビューションポイントのプロパティウィンドウの［**デバイスの検索**］セクションで、IP アドレス範囲ポーリングの設定を表示および編集できます。IP アドレス範囲のポーリング中に検出されたクライアントデバイスは、仮想管理サーバーの［**ドメイン**］フォルダーに表示されます。

Zeroconf ポーリング

この検索方法は Linux ベースのディストリビューションポイントでのみサポートされます。

ディストリビューションポイントは IPv6 アドレスのデバイスを持つネットワークを検索できます。この場合、IP 範囲は指定されず、ディストリビューションポイントはネットワーク全体をゼロコンフィギュレーションネットワーキング（「*Zeroconf*」とも表記）を使用して検索します。Zeroconf の使用を開始するには、ディストリビューションポイントで avahi-browse ユーティリティをインストールする必要があります。

Zeroconf ポーリングを有効にするには：

1. コンソールツリーで、［**デバイスの検索**］フォルダーの［**IP アドレス範囲**］サブフォルダーを選択します。
   ［**今すぐポーリング**］をクリックすると、［**未割り当てデバイス**］フォルダーから［**デバイスの検索**］フォルダーに進むことができます。
2. ［**ポーリングの設定**］をクリックします。
3. 表示されるIP アドレス範囲のプロパティウィンドウで、**[Zeroconf 技術を使用したポーリングを有効にする]**を選択します。

その後、ディストリビューションポイントはネットワークの検索を開始します。この場合、指定された IP 範囲は無視されます。

Windows ドメインの操作：ドメイン設定の表示と変更

ドメイン設定を変更するには：

1. コンソールツリーで、［**デバイスの検索**］フォルダーの［**ドメイン**］サブフォルダーを選択します。
2. ドメインを選択し、次のいずれかの方法でそのドメインのプロパティウィンドウを開きます：
   - ドメインのコンテキストメニューで［**プロパティ**］を選択します。
   - ［**グループのプロパティの表示**］をクリックします。

［**プロパティ：<ドメイン名>**］ウィンドウが開き、選択したドメインのプロパティを設定できます。

未割り当てデバイスの保持ルールの設定

Windows のネットワークポーリングの完了後、検出されたデバイスは［未割り当てデバイス］管理グループのサブグループに配置されます。［**詳細**］→［**デバイスの検索**］→［**ドメイン**］の順に選択するとこの管理グループが見つかります。［**ドメイン**］フォルダーが親グループです。この親グループ内に、ネットワークポーリングで検出された対応ドメインとワークグループに基づいて命名された子グループが含まれています。親グループにはモバイルデバイスの管理グループが含まれる場合もあります。親グループとそれぞれの子グループで、未割り当てデバイスの保持ルールを設定できます。保持ルールはネットワークポーリングの設定には依存せず、ネットワークポーリングが無効な場合でも機能します。

未割り当てデバイスの保持ルールを設定するには：

1. コンソールツリーの［**デバイスの検索**］フォルダーで次の操作のいずれかを実行します：

   - 親グループの設定を編集するには、［**ドメイン**］サブフォルダーを右クリックし、［**プロパティ**］を選択します。

     親グループのプロパティウィンドウが開きます。

   - 子グループの設定を編集するには、目的の子グループの名前を右クリックし、［**プロパティ**］を選択します。

     子グループのプロパティウィンドウが開きます。

2. ［**デバイス**］セクションで、次の設定を指定します：

   - **次の期間デバイスが不可視の場合グループから削除（日）**

     このオプションをオンにすると、デバイスをグループから自動的に削除するまでの期間を指定できます。既定では、この設定が子グループにも反映されます。既定の期間は 7 日です。

     既定では、このオプションはオンです。

   - **親グループから継承する**

     このオプションをオンにすると、デバイスの保持期間が設定が親グループから現在のグループに継承され、変更することはできません。

     このオプションは子グループでのみ利用できます。

     既定では、このオプションはオンです。

   - **子グループへ強制的に継承する**

     設定値が子グループに配信され、子グループのプロパティではそれらの設定がロックされます。

     既定では、このオプションはオフです。

変更内容が保存され、適用されます。

IP アドレス範囲の指定

既存の IP アドレス範囲をカスタマイズし、新しい IP アドレス範囲を作成できます。

IP アドレス範囲の作成

IP アドレス範囲を作成するには：

1. コンソールツリーで、［**デバイスの検索**］フォルダーの［**IP アドレス範囲**］サブフォルダーを選択します。
2. フォルダーのコンテキストメニューで、［**新規作成**］→［**IP アドレス範囲**］の順に選択します。
3. ［**新規 IP アドレス範囲**］ウィンドウが表示されたら、新しい IP アドレス範囲を設定します。

新しい IP アドレス範囲は、［**IP アドレス範囲**］フォルダーに表示されます。

IP アドレス範囲の設定の表示と変更

IP アドレス範囲の設定を変更するには：

1. コンソールツリーで、［**デバイスの検索**］フォルダーの［**IP アドレス範囲**］サブフォルダーを選択します。
2. IP アドレス範囲を選択し、次のいずれかの方法でそのプロパティウィンドウを開きます：
   - IP アドレス範囲のコンテキストメニューで［**プロパティ**］を選択する。
   - ［**グループのプロパティの表示**］をクリックします。

［**プロパティ：<IP アドレス範囲名>**］ウィンドウが開き、選択した IP アドレス範囲のプロパティを設定できます。

Active Directory グループの操作：グループ設定の表示と変更

Active Directory グループの設定を変更するには：

1. コンソールツリーで、［**デバイスの検索**］フォルダーの［**Active Directory**］サブフォルダーを選択します。
2. Active Directory グループを選択し、次のいずれかの方法でそのグループのプロパティウィンドウを開きます：
   - IP アドレス範囲のコンテキストメニューで［**プロパティ**］を選択する。
   - ［**グループのプロパティの表示**］をクリックします。

［**プロパティ：<Active Directory グループ名>**］ウィンドウが開き、選択した Active Directory グループを設定できます。

デバイスを管理グループに自動的に移動するルールの作成

企業ネットワークのポーリングで検出されたデバイスを自動的に管理グループに移動するように設定できます。

デバイスを管理グループに自動的に移動するルールを設定するには：

1. コンソールツリーで、［**未割り当てデバイス**］フォルダーを選択します。
2. フォルダーの作業領域で［**ルールの設定**］をクリックします。

   ［**プロパティ：未割り当てデバイス**］ウィンドウが表示されます。［**デバイスの移動**］セクションで、デバイスを管理グループに自動的に移動するルールを設定します。

リスト内の最初の適用可能なルール（上から下）がデバイスに適用されます。

VDI 向け動的モードのクライアントデバイスでの使用

一時的な仮想マシンを使用して、企業ネットワークに仮想インフラストラクチャを導入できます。Kaspersky Security Center は一時的な仮想マシンを検出し、それらに関する情報を管理サーバーのデータベースに追加します。一時的な仮想マシンの使用を終了した後、このマシンは仮想インフラストラクチャから削除されます。ただし、削除された仮想マシンに関する記録は、管理サーバーのデータベースに保存可能です。また、存在しない仮想マシンを管理コンソールに表示することもできます。

存在しない仮想マシンに関する情報が保存されるのを防ぐため、Kaspersky Security Center は仮想デスクトップインフラストラクチャ（VDI）向け動的モードをサポートしています。管理者は、一時的な仮想マシンにインストールされるネットワークエージェントのインストールパッケージのプロパティで、VDI 向け動的モードのサポートを有効にできます。

一時的な仮想マシンが無効になっている場合、ネットワークエージェントは管理サーバーに仮想マシンが無効化されていることを通知します。仮想マシンが正常に無効化されると、その仮想マシンは管理サーバーに接続されているデバイスのリストから削除されます。仮想マシンの無効化でエラーが発生し、無効化された仮想マシンに関する通知をネットワークエージェントが管理サーバーに送信しない場合、バックアップシナリオが使用されます。このシナリオでの仮想マシンは、管理サーバーとの同期に 3 回失敗すると、管理サーバーに接続されているデバイスのリストから削除されます。

ネットワークエージェントインストールパッケージのプロパティでの VDI 向け動的モードの有効化

VDI 向け動的モードを有効にするには：

1. コンソールツリーの［**リモートインストール**］フォルダーで、［**インストールパッケージ**］サブフォルダーを選択します。
2. ネットワークエージェントのインストールパッケージのコンテキストメニューで［**プロパティ**］を選択します。

   ［**プロパティ：Kaspersky Security Center ネットワークエージェント**］ウィンドウが表示されます。

3. ［**プロパティ：Kaspersky Security Center ネットワークエージェント**］ウィンドウで、［**詳細**］セクションを選択します。

4. ［**詳細**］セクションで、［**VDI 向け動的モードを有効にする**］を選択します。

ネットワークエージェントがインストールされるデバイスが VDI の一部になります。

VDI を構成するデバイスの検索

VDI を構成する未割り当てデバイスを検索するには：

1. ［**未割り当てデバイス**］フォルダーのコンテキストメニューから［**検索**］を選択します。

仮想デスクトップインフラストラクチャに含まれるすべてのデバイスのリストを表示するには、［**管理サーバー**］フォルダーのコンテキストメニューから［**検索**］を選択します。

2. ［**検索**］ウィンドウの［**仮想マシン**］タブで、［**仮想デスクトップインフラストラクチャの一部**］グループで［**はい**］を選択します。

3. ［**今すぐ検索**］をクリックします。

仮想デスクトップインフラストラクチャの一部である未割り当てデバイスのリストが表示されます。

VDI から管理グループへのデバイスの移動

VDI を構成するデバイスを管理グループへ移動するには：

1. ［**未割り当てデバイス**］フォルダーの作業領域で［**ルールの設定**］をクリックします。

［**未割り当てデバイス**］フォルダーのプロパティウィンドウが開きます。

2. ［**未割り当てデバイス**］フォルダーのプロパティウィンドウで、［**デバイスの移動**］セクションの［**追加**］をクリックします。

［**新規ルール**］ウィンドウが表示されます。

3. ［**新規ルール**］ウィンドウで、［**仮想マシン**］セクションを選択します。

4. ［**仮想マシン**］ドロップダウンリストで、［**はい**］を選択します。

管理グループへデバイスを移動するルールが作成されます。

機器のインベントリ

機器の在庫管理に使用するハードウェアリスト（［**リポジトリ**］→［**ハードウェア**］）は、自動と手動の 2 つの方法で追加されます。各ネットワークポーリングの後、検出されたすべてのコンピューターが自動的にリストに追加されます。ただし、ネットワークをポーリングしない場合は、コンピューターを手動で追加することもできます。ルーター、プリンター、コンピューターハードウェアなど、他のデバイスを手動でリストに追加できます。

デバイスの詳細情報の確認と編集は、デバイスのプロパティで行うことができます。

ハードウェアリストには、次の種別のデバイスが含まれます：

- コンピューター
- モバイルデバイス
- ネットワークデバイス
- 仮想デバイス
- OEM コンポーネント
- コンピューター周辺機器
- 接続されているデバイス
- VoIP 電話
- ネットワークリポジトリ

管理者は、検出されたデバイスに*企業用*属性を割り当てることができます。この属性は、デバイスのプロパティで手動で割り当てることができます。また、この属性を自動的に割り当てる基準を管理者が指定することもできます。この場合、*企業用*属性はデバイスの種類に応じて割り当てられます。

Kaspersky Security Center では、機器を抹消することができます。デバイスを抹消するには、そのデバイスのプロパティで［**抹消済みデバイス**］をオンにします。抹消済みデバイスは機器リストに表示されません。

管理者は［**ハードウェア**］フォルダー内のプログラマブルロジックコントローラー（PLC）のリストを管理することができます。PLC リストの管理方法の詳細については、『*Kaspersky Industrial CyberSecurity for Nodes User Guide*』に記載されています。

新しいデバイスに関する情報の追加

ネットワーク上の新しいデバイスに関する情報を追加するには：

1. コンソールツリーの［**リポジトリ**］フォルダーで、［**ハードウェア**］サブフォルダーを選択します。
2. ［**ハードウェア**］フォルダーの作業領域で［**デバイスの追加**］をクリックして［**新しいデバイス**］ウィンドウを表示します。

   ［**新しいデバイス**］ウィンドウが表示されます。
3. ［**新しいデバイス**］ウィンドウの［**種別**］から、追加したいデバイス種別を選択します。
4. ［**OK**］をクリックします。

   デバイスのプロパティウィンドウの［**全般**］セクションが表示されます。
5. ［**全般**］セクションの各フィールドにデバイスに関する情報を入力します。［**全般**］セクションには、次の設定項目があります：

   - **企業用デバイス**：デバイスに*企業用*属性を割り当てたい場合は、チェックボックスをオンにします。この属性を使用して、［**ハードウェア**］フォルダーでデバイスを検索できます。

- **抹消済みデバイス**：［**ハードウェア**］フォルダーのデバイスのリストにデバイスが表示されないようにする場合は、このチェックボックスをオンにします。

6. ［**適用**］をクリックします。

［**ハードウェア**］フォルダーの作業領域に新しいデバイスが表示されます。

企業用デバイスの定義に使用する基準の設定

企業用デバイスの検出基準を設定するには：

1. コンソールツリーの［**リポジトリ**］フォルダーで、［**ハードウェア**］サブフォルダーを選択します。
2. ［**ハードウェア**］フォルダーの作業領域で、［**その他の操作**］をクリックし、ドロップダウンリストから［**企業用デバイスのルールの設定**］を選択します。
   ハードウェアのプロパティウィンドウが開きます。
3. ハードウェアのプロパティウィンドウの［**企業用デバイス**］セクションで、*企業用*属性をデバイスに割り当てる方法を選択します：
   - **デバイスに企業用デバイス属性を手動で設定**：デバイスのプロパティウィンドウの［**全般**］セクションで*企業用ハードウェア*属性をデバイスに手動で割り当てます。
   - **デバイスに企業用デバイス属性を自動で設定**：［**デバイス種別**］で、*企業用*属性を自動的に割り当てるデバイス種別を指定します。

     このオプションは、ネットワークポーリングによって追加されたデバイスにのみ影響します。手動で追加したデバイスの場合は、*企業*属性を手動で設定してください。

4. ［**OK**］をクリックします。

企業用デバイスの検出条件が設定されました。

カスタムフィールドの設定

デバイスのカスタムフィールドを設定するには：

1. コンソールツリーの［**リポジトリ**］フォルダーで、［**ハードウェア**］サブフォルダーを選択します。
2. ［**ハードウェア**］フォルダーの作業領域で、［ **その他の操作**］をクリックし、ドロップダウンリストから［**カスタムデータフィールドの設定**］を選択します。
   ハードウェアのプロパティウィンドウが開きます。
3. ハードウェアのプロパティウィンドウで、［**カスタムフィールド**］セクションを選択し、［**追加**］をクリックします。
   ［**フィールド追加**］ウィンドウが表示されます。

4. ［**フィールド追加**］ウィンドウで、ハードウェアのプロパティに表示されるカスタムフィールドの名前を指定します。

   異なる名前の複数のカスタムフィールドを作成できます。

5. ［**OK**］をクリックします。

追加されたカスタムフィールドが、ハードウェアのプロパティの［**カスタムフィールド**］セクションに表示されます。カスタムフィールドを使用して、デバイスの特定の情報を指定できます。たとえば、ハードウェア購入時の注文番号にすることができます。

ライセンス

このセクションでは、Kaspersky Security Center 15.1 のライセンス付与に関係する一般的な概念に関する情報を提供します。

ライセンス制限超過のイベント

Kaspersky Security Center には、クライアントデバイスにインストールされたカスペルスキー製品がライセンスによる制限を超過した時のイベントに関する情報が表示されます。

ライセンス管理の制限を超過した時のイベントの重要度は、次のルールに従って決定されます：

- 単一のライセンスが現在適用されている台数が、そのライセンスが対応している合計台数の 90 ～ 100% である場合、重要度が「**情報**」のイベントが発生します。
- 単一のライセンスが現在適用されている台数が、そのライセンスが対応している合計台数の 100 ～ 110% である場合、重要度が「**警告**」のイベントが発生します。
- If the number of currently used units covered by a single license exceeds 110% of the total number of units covered by the license, the event is published with the **Critical event** importance level.

ライセンスについて

このセクションでは Kaspersky Security Center 経由で管理されているカスペルスキー製品のライセンスに関する情報について説明します。

ライセンスについて

*ライセンス*は、署名されたライセンス契約（使用許諾契約書）の条件に基づいて提供される、Kaspersky Security Center を使用する期限付きの権利です。

サービスの範囲と有効期間は、アプリケーションが使用されるライセンスによって異なります。

次のライセンス種別があります：

- *試用版*

  製品の試用を目的とした無償ライセンス。試用版ライセンスは通常、有効期間が短く設定されています。

  試用版ライセンスの有効期間が終了すると、Kaspersky Security Center のすべての機能が無効になります。製品の使用を継続するには、製品版ライセンスを購入する必要があります。

  試用ライセンスに基づいてアプリケーションを使用できるのは、1回の試用期間のみです。

- *製品版*

  有料ライセンス。

  製品版ライセンスの有効期限が切れると、本製品の主要な機能が無効になります。Kaspersky Security Center の使用を継続するには、製品版ライセンスを更新する必要があります。商用ライセンスの有効期限が切れると、アプリケーションを引き続き使用できなくなり、デバイスから削除する必要があります。

  有効期間が終了する前、すべてのセキュリティ脅威から継続的に保護された環境を維持できるようにライセンスを更新することを推奨します。

使用許諾契約書について

*使用許諾契約書*は、ユーザーと AO Kaspersky Lab との間で交わされる契約であり、製品の使用条件が定められています。

製品の使用を開始する前に、使用許諾契約書の条項をよく読んでください。

Kaspersky Security Center とそのコンポーネント（ネットワークエージェントなど）にはそれぞれ個別の使用許諾契約書があります。

Kaspersky Security Center の使用許諾契約書の条項は、次の方法で確認できます：

- Kaspersky Security Center のインストール中に確認する。
- Kaspersky Security Center の配布キットに含まれている license.txt を参照する。
- Kaspersky Security Center のインストールフォルダーにある license.txt を参照する。
- カスペルスキーの Web サイトから ファイル license.txt をダウンロードする。

Windows、Mac、Linux の各 OS 向けのネットワークエージェントの使用許諾契約書の条項は、次の方法で確認できます：

- カスペルスキーの Web サーバーからのネットワークエージェント配布パッケージのダウンロード時に確認する。
- Windows 用、Mac 用または Linux 用ネットワークエージェントのインストール中に確認する。
- Windows 用、Mac 用または Linux 用ネットワークエージェント配布パッケージに含まれている license.txt ドキュメントを参照する。
- Windows 用、Mac 用または Linux 用ネットワークエージェントのインストールフォルダーにある license.txt ドキュメントを参照する。
- カスペルスキーの Web サイトから ファイル license.txt をダウンロードする。

製品のインストール時に使用許諾契約書に同意することにより、使用許諾契約書の条項を受諾したものと判断されます。使用許諾契約書の条項に同意しない場合は、製品のインストールを中止し、使用しないようにする必要があります。

ライセンス証書について

*ライセンス証書*とは、ライセンス情報ファイルまたはアクティベーションコードに付随して受け取る文書です。

ライセンス証書には、提供されたライセンスに関する次の情報が含まれています：

- ライセンス情報の数値または注文番号
- ライセンスが適用されるユーザーの情報
- 提供されたライセンスを使用したアクティベーションが可能である製品の情報
- ライセンスの上限（提供されたライセンスで使用可能な製品が使用できるデバイスの台数など）
- ライセンスの有効期間の開始日
- ライセンスの有効期間または有効期間の終了日
- ライセンス種別

ライセンス情報について

*ライセンス情報*とは、使用許諾契約書の条項に基づいてアクティベーションを適用して製品を使用できる数値の並びです。ライセンス情報は、カスペルスキーによって生成されます。

製品にライセンス情報を追加するには、*ライセンス情報ファイル*を適用するか、*アクティベーションコード*を入力します。ライセンス情報は、製品に追加した後、インターフェイスに一意の英数字の並びで表示されます。

使用許諾契約書の条項に違反した場合、カスペルスキーがライセンス情報をブロックします。ライセンス情報がブロックされた際に、製品を使用したい場合は、別のライセンス情報を追加する必要があります。

ライセンスには、現在のライセンスまたは予備のライセンスがあります。

現在のライセンス：アプリケーションによって現在使用されているライセンス。現在のライセンスは、試用版または製品版のライセンス情報として追加できます。製品に指定できる現在のライセンスは1つのみで、2つ以上の現在のライセンスを指定することはできません。

予備のライセンス：アプリケーションを使用する権限をユーザーに付与する、現在使用されていないライセンス。予備のライセンスは、現在のライセンスの有効期間が終了すると、自動的に適用されます。予備のライセンスは、現在のライセンスが追加済みである場合にのみ、追加できます。

試用版のライセンスは、現在のライセンスとしてのみ追加できます。試用版のライセンスを予備のライセンスとして追加することはできません。

ライセンス情報ファイルについて

*ライセンス情報ファイル*は、拡張子が「key」のファイルで、カスペルスキーから提供されます。ライセンス情報ファイルは、製品のアクティベーションに使用します。

ライセンス情報ファイルは、Kaspersky Security Center を購入すると提供されます。

ライセンス情報ファイルでのアクティベーション時には、カスペルスキーのアクティベーションサーバーへの接続は必要ありません。

製品のインストール後にライセンス情報ファイルを紛失した場合は、再入手できます。ライセンス情報ファイルは、カスペルスキーカンパニーアカウントへの登録時などに必要となる場合があります。

ライセンス情報ファイルを再入手するには次の方法があります：

- ご購入元の販売代理店へ問い合わせる。
- カスペルスキーの Web サイトで、使用可能なアクティベーションコードを使用してライセンス情報ファイルを取得する。
- 他の管理サーバーからライセンス情報ファイルをエクスポートします。

定額制サービスについて

*Kaspersky Security Center の定額制サービス*とは、選択した設定（有効期限、保護されるデバイスの台数）でのアプリケーションの使用を注文することです。Kaspersky Security Center の定額制サービスをサービスプロバイダー（インターネットプロバイダーなど）に登録できます。定額制サービスは手動および自動で更新することができ、キャンセルすることもできます。

定額制サービスの期間は制限する（1 年間など）ことも、無制限にすることもできます。制限された定額制サービスの期限を過ぎて Kaspersky Security Center を利用するには、更新する必要があります。サービスプロバイダーによって期限までに支払いが行われた場合、無制限の定額制サービスは自動的に更新されます。

制限された定額制サービスの期限が過ぎた場合は、更新するまでの猶予期間が与えられ、その期間はアプリケーションが機能し続けます。猶予期間の長さや利用できる機能はサービスプロバイダーによって定義されます。

Kaspersky Security Center を定額制サービスの形式で利用するには、サービスプロバイダーが提供するアクティベーションコードを適用する必要があります。

異なる Kaspersky Security Center のアクティベーションコードを適用できるのは、定額制サービスの期限の経過後か、定額制サービスをキャンセルした時のみです。

サービスプロバイダーによっては、定額制サービスの管理に伴う操作が異なる可能性があります。サービスプロバイダーが定額制サービスの更新のための猶予期間を設定しないこともあり、その場合はアプリケーションを利用できなくなります。

定額制サービスの形式で利用する目的で購入されたアクティベーションコードで Kaspersky Security Center の旧バージョンをアクティベートすることはできません。

定額制サービスのもとアプリケーションを使用している場合、Kaspersky Security Center は、定額制サービスの有効期間が切れるまで、指定された間隔でアクティベーションサーバーへの接続を自動的に試みます。これにより、サブスクリプションに関する情報がアクティベーションサーバーと確実に同期されます。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。定額制サービスは、サービスプロバイダーの Web サイトで更新することができます。

Kaspersky Security Center がアクティベーションサーバーにアクセスするのを待たずに、サブスクリプションに関する情報を手動で更新できます。たとえば、これはサブスクリプション設定を変更する場合に役立つ場合があります。

サブスクリプションに関する情報を手動で更新するには：

1. コンソールツリーで、［**カスペルスキーのライセンス**］フォルダーを選択します。
2. ［**追加のアクション**］をクリックし、ドロップダウンリストから［**サブスクリプション設定をライセンス管理サーバーと同期する**］を選択します。

   サブスクリプションに関する情報はアクティベーションサーバー上で更新されます。

アクティベーションコードについて

*アクティベーションコード*は、英数字 20 文字の一意な並びで構成されます。アクティベーションコードを入力すると、Kaspersky Security Center をアクティベートするライセンスを追加することができます。アクティベーションコードは、Kaspersky Security Center を購入すると提供されます。

アクティベーションコードを使用して製品をアクティベートするには、カスペルスキーのアクティベーションサーバーと接続を確立するためのインターネット接続が必要です。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。

アクティベーションコードを使用して製品をアクティベートした後、ライセンスの現在のステータスを確認するリクエストが、製品からカスペルスキーのアクティベーションサーバーに定期的に送信される場合があります。アプリケーションからリクエストを送信するには、インターネット接続が必要です。

アプリケーションのインストール後にアクティベーションコードを紛失した場合は、ライセンスを購入したカスペルスキーのパートナー企業に連絡してください。

管理対象アプリケーションのアクティベーションにライセンス情報ファイルは使用できません。アクティベーションコードのみ使用できます。

使用許諾契約書による同意の取り消し

クライアントデバイスの保護を停止する場合は、管理対象のカスペルスキー製品をアンインストールして、それらの製品の使用許諾契約書（EULA）を取り消すことができます。

管理対象のカスペルスキー製品の EULA を取り消すには：

1. コンソールツリーで、［**管理サーバー**］→［**詳細設定**］→［**同意した EULA**］の順に選択します。

   インストールパッケージの作成時、アップデートのシームレスインストール時、または Kaspersky Security for Mobile の導入時に同意した EULA のリストが表示されます。
2. リストから、同意を取り消す EULA を選択します。

   EULA の以下のプロパティを確認できます：

   - EULA に同意した日付。
   - EULA に同意したユーザーの名前。

- EULA の条項へのリンク。
- EULA に接続されているオブジェクトのリスト：インストールパッケージ名、シームレスアップデート名、モバイルアプリ名。

3. ［**EULA の取り消し**］をクリックします。

   表示されたウィンドウで、この EULA に対応するカスペルスキー製品のアンインストールが必要であることが示されます。

4. ボタンをクリックして取り消しを確定します。

   Kaspersky Security Center は、インストールパッケージ（EULA を取り消す管理対象のカスペルスキー製品に対応するもの）が削除されたかどうかをチェックします。

   インストールパッケージが削除されている管理対象のカスペルスキー製品のみを取り消すことができます。

これで EULA が取り消されました。この EULA は、［**管理サーバー**］→［**詳細設定**］→［**同意した EULA**］セクションの EULA のリストに表示されません。EULA を取り消したカスペルスキー製品を使用するクライアントデバイスを保護することはできません。

データ提供について

サードパーティに送信されるデータ

製品のモバイルデバイス管理機能を使用する場合、プッシュ通知のメカニズムによって Android オペレーティングシステムを実行するデバイスにコマンドをタイムリーに配信する目的で、Google Firebase Cloud Messaging サービスが使用されます。ユーザーが Google Firebase Cloud Messaging サービスの使用を設定した場合、ユーザーは、プッシュ通知を送信する必要がある Kaspersky Endpoint Security for Android アプリケーションのインストール ID に関する情報を Google Firebase Cloud Messaging サービスに自動モードで送信することに同意したものとします。

Google Firebase Cloud Messaging サービスとの情報の交換をブロックするには、ユーザーが Google Firebase Cloud Messaging サービスの使用設定を出荷時の設定にロールバックする必要があります。

製品のモバイルデバイス管理機能を使用する場合、プッシュ通知のメカニズムによって iOS オペレーティングシステムを実行するデバイスにコマンドをタイムリーに配信する目的で、Apple Push Notification Service（APNs）サービスが使用されます。ユーザーが iOS MDM サーバーに APNs 証明書をインストールし、iOS モバイルデバイスを製品に接続するために iOS MDM プロファイルを作成して一連の設定を行い、このプロファイルをモバイルデバイスにインストールした場合、そのユーザーは次の情報を APNs に自動モードで提供することに同意したものとします：

- トークン - デバイスのプッシュトークン。サーバーはデバイスにプッシュ通知を送信する時に、このトークンを使用します。
- PushMagic - プッシュ通知に含まれる必要のある文字列。この文字列の値はデバイスによって生成されます。

ローカル環境で処理されるデータ

Kaspersky Security Center は、組織のネットワークの基本的な管理と保守の一元化を目的として設計されています。管理者は組織のネットワークのセキュリティレベルに関する詳細情報にアクセスし、カスペルスキー製品を使用して構築された保護システムのすべてのコンポーネントを設定できるようになります。Kaspersky Security Center が実行する主要な機能は次の通りです：

- 組織のネットワーク内のデバイスおよびそのユーザーの検出
- デバイス管理用の管理グループ階層の作成
- デバイスへのカスペルスキー製品のインストール
- インストールされた製品の設定およびタスクの管理
- カスペルスキー製品およびサードパーティ製品のアップデートの管理、および脆弱性の検知と修正
- デバイス上でのカスペルスキー製品のアクティベーション
- ユーザーアカウントの管理
- デバイス上でのカスペルスキー製品の動作に関する情報の表示
- レポートの表示

主要な機能を実行するために、Kaspersky Security Center は次の情報を取得し、保存し、処理することができます：

- Windows ドメイン、Active Directory または Samba ドメインコントローラーのスキャン、または IP レンジのスキャンを通じて受信した、組織のネットワーク上のデバイスに関する情報。管理サーバーは、独自にデータを取得するか、ディストリビューションポイントとして機能するネットワークエージェントからデータを受信します。
- 組織単位、ドメイン、ユーザー、およびグループに関する Active Directory および Samba からの情報。管理サーバーは、独自にデータを取得するか、ディストリビューションポイントとして機能するネットワークエージェントからデータを受信します。
- 管理対象デバイスの詳細情報。ネットワークエージェントによって、次に記載されたデータがデバイスから管理サーバーに送信されます。ユーザーはデバイスの表示名と説明を管理コンソールのインターフェイスまたは Kaspersky Security Center Web コンソールのインターフェイスに入力します：
  - デバイスの識別に必要な管理対象デバイスとそのコンポーネントの技術的な仕様情報：デバイスの表示名と説明、Windows ドメイン名と種別、Windows 環境におけるデバイス名、DNS ドメインと DNS 名、IPv4 アドレス、IPv6 アドレス、ネットワークロケーション、MAC アドレス、シリアル番号、オペレーティングシステムの種別、デバイスが仮想マシンかどうかの情報とハイパーバイザーの種別、およびデバイスが VDI の一部としての動的仮想マシンかどうかの情報。
  - 管理対象デバイスの監査および特定のパッチやアップデートが適用可能かどうかの判断に必要となる、管理対象デバイスとそのコンポーネントのその他の仕様情報：Windows Update エージェント（WUA）のステータス、オペレーティングシステムのアーキテクチャ、オペレーティングシステムの製造元、オペレーティングシステムのビルド番号、オペレーティングシステムのリリース ID、オペレーティングシステムのロケーションフォルダー、デバイスが仮想マシンかどうかの情報とその仮想マシンの種別、デバイスを管理する仮想管理サーバー名、クラウドのデバイスデータ（クラウドの地域、VPC、クラウドのアベイラビリティゾーン、クラウドのサブネット、クラウドの配置ゾーン）。
  - 管理対象デバイス上の処理の詳細情報：前回のアップデートの日時、デバイスが前回ネットワークで検出された日時、再起動の待機ステータス、デバイスの電源を投入した日時。
  - デバイスのユーザーアカウントとその作業セッションの詳細情報。

- 管理対象デバイスでリモート診断を実行することによって受信したデータ：トレースファイル、システム情報、デバイスにインストールされているカスペルスキーアプリケーションの詳細、ダンプファイル、イベントログ、カスペルスキーテクニカルサポートから受信した診断スクリプトの実行結果。

- デバイスがディストリビューションポイントである場合、ディストリビューションポイントの動作統計情報。ネットワークエージェントによってデータがデバイスから管理サーバーに送信されます。

- ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールに入力したディストリビューションポイントの設定。

- 管理サーバーへのモバイルデバイスの接続に必要なデータ：証明書、モバイル接続ポート、管理サーバーの接続アドレス。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールでデータを入力します。

- iOS MDM プロトコル経由で送信されるモバイルデバイスの詳細情報。次に記載されたデータがモバイルデバイスから管理サーバーに送信されます：

  - デバイスの識別に必要なモバイルデバイスとそのコンポーネントの技術的な仕様情報：デバイス名、機種、オペレーティングシステムの名前とビルド番号、デバイスの機種番号、IMEI 番号、UDID、MEID、シリアル番号、ストレージ容量、モデムファームウェアのバージョン、Bluetooth の MAC アドレス、Wi-Fi の MAC アドレス、SIM カードの詳細情報（SIM カードの識別子の一部としての ICCID）。

  - 管理対象デバイスで使用されるモバイルネットワークの詳細情報：モバイルネットワークの種別、現在使用されているモバイルネットワークの名前、ホームモバイルネットワーク名、通信事業者の設定のバージョン、音声ローミングとデータローミングのステータス、ホームネットワークの国コード、居住国コード、現在使用されているネットワークの国コード、暗号化レベル。

  - モバイルデバイスのセキュリティ設定：パスワードの使用とポリシー設定への準拠の状況、サードパーティ製品のインストールに使用される設定ファイルとプロビジョニングプロファイルのリスト。

  - 管理サーバーとの前回の同期の日付とデバイスの管理ステータス。

- デバイスにインストールされたカスペルスキー製品の詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます：

  - 管理対象デバイスにインストールされているカスペルスキー製品の設定：カスペルスキー製品の名前とバージョン、ステータス、リアルタイム保護のステータス、前回のデバイススキャンの日時、検知された脅威の数、駆除に失敗したオブジェクトの数、製品コンポーネントの使用可否の情報とそのステータス、定義データベースの前回のアップデート日時とバージョン、カスペルスキー製品の設定およびタスクの詳細情報、現在のライセンスと予備のライセンスに関する情報、製品のインストールの日付と ID。

  - 製品動作の統計情報：管理対象デバイス上のカスペルスキー製品コンポーネントのステータス変化および製品コンポーネントによって開始されたタスクのパフォーマンスに関係するイベント。

  - カスペルスキー製品によって定義されたデバイスのステータス。

  - カスペルスキー製品によって割り当てられたタグ。

  - カスペルスキー製品のインストール済みのアップデートおよび適用可能なアップデート。

- Kaspersky Security Center のコンポーネントおよび管理対象のカスペルスキー製品からのイベントに含まれるデータ。ネットワークエージェントによってデータがデバイスから管理サーバーに送信されます。

- Kaspersky Security Center と、イベントをエクスポートする SIEM システムとの統合に必要なデータ。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールでデータを入力します。

- Kaspersky Security Center のコンポーネント、およびポリシーとポリシーのプロファイルに示される管理対象のカスペルスキー製品の設定。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールのインターフェイスでデータを入力します。

- Kaspersky Security Center のコンポーネントおよび管理対象のカスペルスキー製品のタスク設定。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールのインターフェイスでデータを入力します。

- 脆弱性とパッチ管理機能によってデータが処理されます。ネットワークエージェントによって、次に記載されたデータがデバイスから管理サーバーに送信されます：

  - 管理対象デバイスにインストールされているアプリケーションおよびパッチの詳細情報（アプリケーションのレジストリ）。

  - 管理対象デバイスで検出されたハードウェアに関する情報（ハードウェアのレジストリ）。

  - 管理対象デバイスで検出されたサードパーティ製品の脆弱性に関する詳細情報。

  - 管理対象デバイスにインストールされているサードパーティ製品で利用できるアップデートの詳細情報。

  - WSUS 機能によって検出された Microsoft の更新プログラムの詳細情報。

  - デバイスにインストールする必要のある、WSUS 機能によって検出された Microsoft の更新プログラムのリスト。

- 管理対象デバイスのサードパーティ製品の脆弱性を修正するため、分離された管理サーバー上のアップデートをダウンロードするために必要なデータ。ユーザーは管理サーバーの klscflag ユーティリティを使用してデータを入力および送信します。

- Kaspersky Security Center とクラウド環境（Amazon Web Services、Microsoft Azure、Google Cloud、Yandex Cloud）での作業に必要なデータ。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールでデータを入力します。

- アプリケーションのユーザーカテゴリ。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールのインターフェイスでデータを入力します。

- アプリケーションコントロール機能を使用して管理対象デバイスで検出された実行ファイルの詳細。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールのインターフェイスでデータを入力します。データ一覧については、該当する製品のヘルプファイルに記載されています。

- バックアップされたファイルの詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 隔離されたファイルの詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 詳細分析のためにカスペルスキーの担当者から提出を依頼されたファイルの詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- アダプティブアノマリーコントロールルールのステータスとトリガーの詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- デバイスコントロール機能によって検出された、管理対象デバイスに搭載されているデバイスまたは管理対象デバイスに接続している外部デバイス（メモリユニット、情報転送ツール、情報ハードコピーツール、接続バス）の詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 暗号化されたデバイスと暗号化のステータスに関する情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。

- カスペルスキー製品のデータ暗号化機能を使用してデバイス上で実行されたデータ暗号化のエラーの詳細情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 管理対象のプログラマブルロジックコントローラー（PLC）のリスト。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 脅威開発チェーンの作成に必要なデータ。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- 組織の従業員によるクラウドサービスへのアクセス試行に関する情報。管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。データ一覧については、該当する製品のヘルプファイルに記載されています。

- Kaspersky Security Center と Kaspersky Managed Detection and Response サービスの統合に必要なデータ（Kaspersky Security Center Web コンソールには専用プラグインをインストールする必要があります）：統合開始トークン、統合トークン、およびユーザーセッショントークン。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールで統合開始トークンを入力します。Kaspersky MDR サービスは、専用プラグインを介して統合トークンとユーザーセッショントークンを転送します。

- 入力されたアクティベーションコードまたは指定されたライセンス情報ファイルの詳細。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールのインターフェイスでデータを入力します。

- ユーザーアカウント：名前、説明、氏名、メールアドレス、メインの電話番号、パスワード、管理サーバーによって生成された秘密鍵、および二段階認証用のワンタイムパスワード。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールのインターフェイスでデータを入力します。

- IAM が一元化された認証および Kaspersky Security Center と連携するカスペルスキー製品間でシングルサインオン（SSO）の提供に必要とするデータ：IAM のインストールおよび構成設定、IAM ユーザーセッション、IAM トークン、クライアントアプリケーションのステータスおよびリソースサーバーのステータス。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールのインターフェイスでデータを入力します。

- 管理オブジェクトの変更履歴。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールのインターフェイスでデータを入力します。

- ユーザーがリビジョンを作成したデバイスの IP アドレス。IP アドレスは管理サーバーによって自動的に定義されます。

- 削除された管理オブジェクトのレジストリ。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールのインターフェイスでデータを入力します。

- ファイルから作成されたインストールパッケージとインストール設定。ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールのインターフェイスでデータを入力します。

- Kaspersky Security Center Web コンソールでのカスペルスキーからの告知表示に必要なデータ。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- Kaspersky Security Center Web コンソールで管理対象アプリケーションのプラグインが機能するために必要なデータおよび日常の作業中に管理サーバーのデータベースにプラグインによって保存されるデータ。データの説明および提供方法については、対応するアプリケーションのヘルプファイルで説明されています。

- Kaspersky Security Center Web コンソールのユーザー設定：ローカリゼーション言語とインターフェイスのテーマ、監視パネルの表示設定、通知のステータスに関する情報（確認済みまたは未確認）、スプレッドシートの列のステータス（表示または非表示）、トレーニングモードの進捗状況。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- Kaspersky Security Center のコンポーネントおよび管理対象のカスペルスキー製品に関する Kaspersky イベントログ。Kaspersky イベントログは各デバイスに保存され、管理サーバーに送信されることはありません。

- 管理対象デバイスから Kaspersky Security Center コンポーネントへのセキュアな接続を確立するための証明書。ユーザーは、管理サーバーの klsetsrvcert ユーティリティを使用してデータを入力します。

- 組織の内部 Web リソースへの信頼を確立するための証明書。ユーザーが Kaspersky Security Center Web コンソールでデータを入力します。

- Amazon Web Services（AWS）、Microsoft Azure、Google Cloud、Yandex.Cloud などのクラウド環境での Kaspersky Security Center の運用に必要なデータ。管理サーバーは、それが実行されている仮想マシンからデータを受信します。

- カスペルスキーとの法的契約の条項に対するユーザーの同意に関する情報。

- 次のコンポーネントでユーザーが入力する管理サーバーのデータ：

  - 管理コンソール

  - Kaspersky Security Center Web コンソール

  - Klscflag ユーティリティ使用中のコマンドラインターミナル

  - Klakaut 自動化オブジェクトおよび Kaspersky Security Center OpenAPI 経由で連携するコンポーネント

- ユーザーが管理コンソールまたは Kaspersky Security Center Web コンソールで入力したあらゆるデータ。

上記のデータは、次の方法のいずれかが適用された場合に Kaspersky Security Center に表示される場合があります：

- ユーザーは次のコンポーネントのインターフェイスでデータを入力します：

  - 管理コンソール

  - Kaspersky Security Center Web コンソール

  - Klscflag ユーティリティ使用中のコマンドラインターミナル

  - Klakaut 自動化オブジェクトおよび Kaspersky Security Center OpenAPI 経由で連携するコンポーネント

- ネットワークエージェントが自動的にデータをデバイスから受信して、管理サーバーに送信します。

- ネットワークエージェントが、管理対象のカスペルスキー製品によって取得されたデータを受信して、管理サーバーに送信する。管理対象のカスペルスキー製品によって処理されるデーター覧については、該当する製品のヘルプファイルに記載されています。

- 管理サーバーは、ネットワークに接続されたデバイスに関する情報を独自に取得するか、ディストリビューションポイントとして機能するネットワークエージェントから情報を受信します。
- iOS MDM プロトコルを使用して、データがモバイルデバイスから管理サーバーに送信されます。

これらのデータは管理サーバーのデータベースに保存されます。ユーザー名とパスワードは暗号化された形式で保存されます。

上記のデータはすべて、ダンプファイル、トレースファイル、または Kaspersky Security Center のコンポーネントのログファイル（インストーラーやユーティリティによって作成されたログファイルを含む）としてのみカスペルスキーに送信されます。

ダンプファイル、トレースファイル、および Kaspersky Security Center のコンポーネントのログファイルには、管理サーバー、ネットワークエージェント、管理コンソール、iOS MDM サーバーおよび Kaspersky Security Center Web コンソールから取得したデータがランダムに含まれています。これらのファイルには、個人のデータや機密データが含まれている場合がありますダンプファイル、トレースファイル、およびログファイルは、デバイス上で暗号化されずに保存されます。ダンプファイル、トレースファイル、およびログファイルがカスペルスキーに自動的に送信されることはありません。ただし、Kaspersky Security Center の使用時に発生した問題を解決するために、テクニカルサポートの担当者の依頼に応じて、管理者がカスペルスキーに手動でデータを送信する場合があります。

管理コンソールまたは Kaspersky Security Center Web コンソールのリンクを使用することで、ユーザーは次のデータが自動的に送信されることに同意したものとします：

- Kaspersky Security Center のコード
- Kaspersky Security Center のバージョン
- Kaspersky Security Center の言語
- ライセンス識別子
- ライセンス種別
- ライセンスが代理店経由で購入されたかどうか

リンクの目的や位置によってリンク経由で提供されたデータのリスト。

カスペルスキーでは、取得したデータはすべて匿名形式で、また一般的な統計情報としてのみ使用します。統計情報のサマリーが最初に取得した情報から自動的に生成されますが、そのサマリーには個人情報などの機密情報は含まれていません。新しい情報が蓄積された後、以前のデータは即座に破棄されます（年に1回）。統計情報のサマリーは、無期限に保管されます。

カスペルスキーは、受け取ったすべての情報を法律およびカスペルスキーの内規に基づいて保護します。データはセキュアな接続で送信されます。

Kaspersky Security Center のライセンスオプション

Kaspersky Security Center は次のモードで動作します：

- **ライセンスなし（基本機能）**

  Kaspersky Security Center は、アプリケーションがアクティベートされる前、または製品版ライセンスの有効期限が切れた後、このモードで動作します。Kaspersky Security Center と管理コンソールの基本機能は、企業ネットワークを保護するカスペルスキー製品の一部として提供されます。カスペルスキーの Web サイトからもダウンロードできます。

- **製品版ライセンス**

  管理コンソールの基本機能に含まれていない追加機能が必要な場合は、製品版ライセンスを購入する必要があります。

  管理サーバーのプロパティウィンドウでライセンスキーを追加する時は、Kaspersky Security Center を使用できるようにするライセンスキーを必ず追加してください。この情報は、カスペルスキーの Web サイトにあります。各ソリューションの Web ページには、ソリューションに含まれるアプリケーションのリストが記載されています。管理サーバーは、サポートされていないライセンス（たとえば、Kaspersky Endpoint Security Cloud のライセンス）を受け入れる場合がありますが、そのようなライセンスは、管理コンソールの基本機能に加えて新しい機能を提供しません。

機能またはプロパティ	Kaspersky Security Center 操作モード	
	ライセンスなし	製品版ライセンス
管理コンソールの基本機能 次の機能を使用できます： • リモートオフィスまたはクライアント組織のネットワークを管理する仮想管理サーバーの作成 • 特定のデバイスをまとめて管理する管理グループの階層の作成 • アプリケーションのリモートインストール • クライアントデバイスにインストールされたアプリケーションの一元的設定 • 組織のアンチウイルスセキュリティステータスの管理 • ユーザーロールの管理 • アプリケーションの動作に関する統計、レポートの検索、および緊急イベントの通知 • 隔離フォルダーまたはバックアップフォルダーに移動されたファイルおよび処理が延期されたファイルの一元的管理 • 暗号化とデータ保護の管理 • 既存のライセンス認証済みアプリケーションのグループの表示と編集 • ネットワークポーリングによって検出されたハードウェアのリストの表示と手動編集 • リモートインストールに使用できるオペレーティングシステムイメージのリストの表示	✓	✓
脆弱性とパッチ管理：基本機能	✓	✓

次のタスクに商用ライセンスは必要ありません： • *脆弱性とアプリケーションのアップデートの検索タスク* このタスクを使用して、Kaspersky Security Center は管理対象デバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。 • ［*Windows Update 更新プログラムのインストール*］タスク このタスクは、Windows Update 更新プログラムのインストールにのみ使用できます。このタスクを使用するには、タスク設定で必要なアップデートを手動で指定する必要があります。 • ［*脆弱性の修正*］タスク ［*脆弱性の修正*］タスクでは、Microsoft 製品に対しては推奨される修正を、その他のサードパーティ製ソフトウェアに対してはユーザー修正をインストールして脆弱性を修正します。このタスクを使用するには、タスクの設定で、脆弱性を修正するために使用するユーザー修正を手動で指定する必要があります。		
脆弱性とパッチ管理：高度な機能 次の機能を使用できます： • 定義したルールに従って、ソフトウェアのアップデートのリモートインストールと脆弱性の修正が自動的に行われます • 管理サーバーを Windows Server Update Services（WSUS）サーバーとして使用し、一元管理モードで設定された頻度でデバイス上の Windows 更新プログラムサービスにアップデートを提供します	–	✓
MMC ベースの管理コンソールのモバイルデバイス管理機能	–	✓（ライセンスを管理サーバーのプロパティに追加する必要があります。）

モバイルデバイス管理機能は、iOS MDM および Android モバイルデバイスを管理するために使用されます。 iOS MDM デバイス向けには、次の機能を使用できます： • Kaspersky Security Center の管理下に新しいデバイスを追加します • 設定プロファイルの作成と編集、モバイルデバイスでの設定プロファイルのインストール • App Store® 経由、マニフェストファイル（.plist）またはモバイルインストールパッケージ（.ipa）を使用して、モバイルデバイスにアプリケーションをインストールします • モバイルデバイスのロック、モバイルデバイスのパスワードのリセット、モバイルデバイスからのすべてのデータの削除など、iOS MDM デバイス上でのコマンドの実行 Android デバイス向けには、次の機能を使用できます： • Kaspersky Security Center の管理下に新しいデバイスを追加します • ポリシーによる Kaspersky Endpoint Security for Android の管理 • デバイス上でコマンドを実行します モバイルデバイス管理機能の管理単位はモバイルデバイスです。モバイルデバイスはモバイルデバイスサーバーに接続した時点から管理対象と判断されます。		
Kaspersky Security Center Web コンソールでのモバイルデバイス保護 Kaspersky Security Center Web コンソールには、 Android および iOS モバイルデバイスを管理するための次の機能が用意されています： • Kaspersky Security Center の管理下に新しいデバイスを追加します • ポリシーにより、Kaspersky Endpoint Security for Android および Kaspersky Security for iOS を管理します • 関連するプロトコル経由でモバイルデバイスにコマンドを送信し、コマンドを実行します	–	✓（ライセンスは各モバイルデバイスに追加する必要があります。）
システム管理	–	✓

次の機能を使用できます： • オペレーティングシステムとアプリケーションのインストール。 Kaspersky Security Center では、オペレーティングシステムイメージを作成し、それをネットワーク上のクライアントデバイスに導入できます。また、カスペルスキー製品や他の製造元のアプリケーションのリモートインストールを行うこともできます。Kaspersky Security Center は、デバイスからオペレーティングシステムイメージを取得し、管理サーバーに転送できます。そのようなオペレーティングシステムイメージは管理サーバー上の専用フォルダーに格納されます。基準となるデバイスのオペレーティングシステムイメージの取得と作成は、インストールパッケージ作成タスクにより行われます。イメージを使用して、オペレーティングシステムがまだインストールされていない新しくネットワーク接続されたデバイスにオペレーティングシステムを導入できます。この場合、Preboot eXecution Environment（PXE）というテクノロジーが使用されます。 • ライセンス認証済みアプリケーショングループの管理 • リモートデスクトップ接続という名前の Microsoft® Windows® コンポーネントによるクライアントデバイスへのリモート接続権限 • Windows デスクトップ共有によるクライアントデバイスへのリモート接続 • ［**Kaspersky リモートデスクトップ接続ビューア**］を介したリモート接続。		
クラウド環境との統合 Kaspersky Security Center はオンプレミスのデバイスに対して使用できるだけでなく、クラウド環境設定ウィザードなど、クラウド環境で使用できる特別な機能を備えています。Kaspersky Security Center は次の仮想マシンと連携します： • Amazon EC2 インスタンス • Microsoft Azure 仮想マシン • Google Cloud 仮想マシンインスタンス • Yandex.Cloud 仮想マシン	–	✓
イベントを SIEM システムへエクスポートする方法：Syslog プロトコルを使用します Syslog プロトコルを使用すると、Kaspersky Security Center 管理サーバーおよび管理対象デバイスにインストールされたカスペルスキー製品で発生したイベントはすべてリレーできます。Syslog プロトコルは、標準メッセージロギングプロトコルです。任意の SIEM システムへのイベントのエクスポートに使用可能です。	✓	✓

Kaspersky Security Center および管理対象アプリケーションのライセンス管理

管理サーバーと管理対象アプリケーションのライセンス管理には、次の方法があります：

- 脆弱性とパッチ管理、モバイルデバイス管理、または SIEM システムとの連携機能をアクティベートする場合には、ライセンス情報または有効なアクティベーションコードを管理サーバーに追加できます。Kaspersky Security Center の一部の機能は、管理サーバーに追加した有効なライセンス情報ファイルまたはアクティベーションコードに応じてアクセスできるかどうかが決まります。

- 管理対象アプリケーション向けには、複数のアクティベーションコードまたはライセンス情報ファイルを管理サーバーのリポジトリに追加できます。

Kaspersky Security Center のライセンス管理について

ライセンスが必要な機能のいずれか（例：モバイルデバイス管理）をライセンス情報ファイルを使用してアクティベートしていて、ライセンスが必要な別の機能（例：脆弱性とパッチ管理）も使用したい場合、両方の機能をアクティベートするライセンスを購入し、そのライセンスを使用して管理サーバーをアクティベートする必要があります。

管理対象アプリケーションのライセンスの管理機能

管理対象アプリケーションのライセンスを管理する目的で、アクティベーションコードまたはライセンス情報ファイルを自動的に配信できます。また、ご都合に合わせて、別の方法での配信も可能です。アクティベーションコードまたはライセンス情報ファイルは、次の方法で配信できます：

- 自動配信

  > 異なる複数の管理対象アプリケーションを使用し、特定のライセンス情報ファイルまたはアクティベーションコードをデバイスに配信する必要がある場合は、他の配信方法を選択してください。

  Kaspersky Security Center を使用して、使用可能なライセンスをデバイスに配信できます。ここでは、3 個のライセンスが管理サーバーのリポジトリに保管されている場合を例にします。［**管理対象デバイスにライセンスを自動的に配信する**］を 3 個のライセンスすべてに対してオンにしていると仮定します。カスペルスキーのセキュリティ製品（例：Kaspersky Endpoint Security for Windows）が、組織内のデバイスにインストールされているとします。ライセンスを配信する必要がある新しいデバイスが検出されます。リポジトリ内に保管されている、名前がそれぞれ「*Key_1*」「*Key_2*」である 2 個のライセンス情報ファイルが、そのデバイスに配信可能であると本製品が判断します。そのうち 1 個のライセンス情報ファイルが、デバイスに配信されます。この場合、どのライセンス情報ファイルがデバイスに適用されるかは予測ができません。自動配信されるライセンスに対して、管理者が設定可能な項目がないからです。

  ライセンスが配信されると、そのライセンスを適用中のデバイスの台数が再度計上されます。ライセンスが適用可能な台数を超えないように、適用中のデバイスの台数を確認しておく必要があります。ライセンスを適用可能な台数の上限を超えると、ライセンスが適用されていないデバイスのステータスが「*緊急*」になります。

- ライセンス情報ファイルまたはアクティベーションコードを管理対象アプリケーションのインストールパッケージに追加

  インストールパッケージを使用して管理対象アプリケーションをインストールする場合、パッケージ内またはアプリケーションのポリシー内に含まれるアクティベーションコードまたはライセンス情報ファイルを指定できます。ライセンスが管理対象デバイスに配信されるのは、デバイスと管理サーバーの次回の同期時です。

- 管理対象アプリケーションへのライセンスの追加タスクを使用して配信

  管理対象アプリケーションへのライセンスの追加タスクを使用する場合、配信する必要があるライセンスを選択後、対象デバイスを都合のよい方法で選択できます。たとえば、管理グループを選択したり、デバイスの抽出を使用したりすることが可能です。

- アクティベーションコードまたはライセンス情報ファイルを手動でデバイスに追加

カスペルスキー製品：一元管理による導入

このセクションでは、カスペルスキー製品のリモートインストールとネットワーク上のデバイスからの削除の方法について説明します。

クライアントデバイスにアプリケーションを導入する前に、クライアントデバイスのハードウェアとソフトウェアが該当する要件を満たしていることを確認してください。

ネットワークエージェントは、管理コンソールにクライアントデバイスとの接続を提供するコンポーネントです。そのため、リモート一元管理システムに接続するすべてのクライアントデバイスにインストールする必要があります。管理サーバーがインストールされているデバイスでは、サーバー向けネットワークエージェントのみ使用できます。このバージョンのネットワークエージェントは、管理サーバーの一部として管理サーバーとともにインストールおよび削除されます。デバイスにネットワークエージェントをインストールする必要はありません。

アプリケーションと同様に、ネットワークエージェントのインストールはリモートでもローカルでも実行可能です。管理コンソールを用いたセキュリティ製品の一元的な導入時に、ネットワークエージェントをセキュリティ製品とともにインストールできます。

ネットワークエージェントは、連携して動作するカスペルスキー製品によって異なる場合があります。場合によっては、ネットワークエージェントのインストールがローカルでしかインストールできないことがあります（詳細については該当する製品のガイドを参照してください）。クライアントデバイスへのネットワークエージェントのインストールは、一度だけ必要です。

カスペルスキー製品は、管理プラグインを使用して管理コンソールで管理します。したがって、アプリケーションの管理インターフェイスに Kaspersky Security Center を介してアクセスするには、対応する管理プラグインが管理コンピューターにインストールされている必要があります。

Kaspersky Security Center アプリケーションのメインウィンドウで、管理コンピューターからアプリケーションをリモートインストールすることができます。

ソフトウェアをリモートインストールするには、リモートインストールタスクを作成する必要があります。

リモートインストール用に作成されたタスクは、設定されているスケジュールで起動します。タスクの実行を手動で停止することで、インストール手順を中断できます。

アプリケーションのリモートインストールでエラーが返される場合は、リモート導入準備ユーティリティを使用してエラーの原因を見つけて修正することができます。

導入レポートで、ネットワーク内のカスペルスキー製品のリモートインストールの進行状況を追跡できます。

各製品を Kaspersky Security Center で管理する場合の詳細については、該当の製品のガイドを参照してください。

サードパーティのセキュリティ製品からの移行とアンインストールの実施

カスペルスキーのセキュリティ製品を Kaspersky Security Center を使用してインストールする場合、インストールするアプリケーションと競合するサードパーティ製ソフトウェアを削除しなければならない場合があります。Kaspersky Security Center では、サードパーティ製品を削除する複数の方法が用意されています。

競合するアプリケーションをインストーラーを使用して削除

この方法は MMC ベースの管理コンソールでのみ利用できます。

競合するアプリケーションをインストーラーを使用して削除する方法は、様々なインストールでサポートされています。セキュリティ製品のインストールパッケージのプロパティウィンドウ（［**競合アプリケーション**］セクション）で、［**競合アプリケーションを自動的にアンインストールする**］がオンになっている場合、セキュリティ製品がインストールされる前に、すべての競合アプリケーションが自動的に削除されます。

競合するアプリケーションの削除をアプリケーションのリモートインストールの設定時に指定

セキュリティ製品のリモートインストールの設定時に［**競合アプリケーションを自動的にアンインストールする**］をオンにできます。MMC ベースの管理コンソールでは、リモートインストールウィザードでこのオプションを設定できます。Kaspersky Security Center Web コンソールでは、製品導入ウィザードでこのオプションを設定できます。このオプションをオンにすると、管理対象デバイスにセキュリティ製品をインストールする前に、Kaspersky Security Center は競合するアプリケーションを削除します。

実行手順の説明：

- 管理コンソール：リモートインストールウィザードを使用した競合アプリケーションの削除
- Kaspersky Security Center Web コンソール：セキュリティ製品をインストールする前に競合するアプリケーションを削除

専用タスクを使用した競合アプリケーションの削除

競合アプリケーションを削除するには、**アプリケーションのリモートアンインストール**タスクを使用します。このタスクは、セキュリティ製品のインストールタスクの前にデバイスで実行する必要があります。たとえば、インストールタスクのスケジュール種別として［**他のタスクが完了次第**］を選択し、条件の対象となるタスクとして［**アプリケーションのリモートアンインストール**］を指定できます。

このアンインストール方法は、セキュリティ製品のインストーラーでは競合アプリケーションを適切に削除できない場合に有用です。

管理コンソールの使用方法：タスクの作成

リモートインストールタスクを使用したアプリケーションのインストール

Kaspersky Security Center では、リモートインストールタスクを使用してデバイスにアプリケーションをリモートインストールできます。このタスクは、専用のウィザードを使用して作成しデバイスに割り当てます。タスクを簡単にデバイスに割り当てるには、次のいずれかの方法を使用し、ウィザードウィンドウでデバイス（最大 1000 台）を指定できます：

- **ネットワークの管理サーバーによって検出されたデバイスを選択する**：この場合、タスクを特定のデバイスに割り当てます。特定のデバイスには、管理グループに属するデバイスと管理グループが割り当てられていないデバイスの両方を含めることができます。
- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**：タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。
- **デバイスの抽出にタスクを割り当てる**：この場合、既に作成された抽出に属するデバイスにタスクを割り当てます。事前定義の抽出または作成済みのカスタム抽出を指定できます。
- **管理グループにタスクを割り当てる**：この場合、既に作成された管理グループに属するデバイスにタスクを割り当てます。

ネットワークエージェントがインストールされていないデバイスでリモートインストールを正常に行うには、次のポートを開いておく必要があります：TCP 139 および 445、UDP 137 および 138。既定では、これらのポートはドメイン内のすべてのデバイスで開いています。これらは、リモート導入準備ユーティリティによって自動的に開かれます。

選択したデバイスへのアプリケーションのインストール

選択したデバイスにアプリケーションをインストールするには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. ［**タスクの作成**］をクリックしてタスクの作成を実行します。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

   新規タスクウィザードの［**タスク種別の選択**］ウィンドウにある［**Kaspersky Security Center 管理サーバー**］ノードで、タスク種別に［**アプリケーションのリモートインストール**］を選択します。

   新規タスクウィザードが、指定したデバイスに選択したアプリケーションをリモートインストールするタスクを作成します。新規作成されたタスクが、［**タスク**］フォルダーの作業領域に表示されます。
3. 手動でタスクを実行するか、タスク設定で指定したスケジュールで開始されるのを待ちます。

リモートインストールタスクが完了すると、選択したアプリケーションが選択されたデバイスにインストールされます。

管理グループ内のクライアントデバイスへのアプリケーションのインストール

管理グループ内のクライアントデバイスにアプリケーションをインストールするには：

1. 関連する管理グループを管理している管理サーバーとの接続を確立します。
2. コンソールツリーで管理グループを選択します。
3. グループの作業領域で、［**タスク**］タブを選択します。
4. ［**タスクの作成**］をクリックしてタスクの作成を実行します。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

新規タスクウィザードの［**タスク種別の選択**］ウィンドウにある［**Kaspersky Security Center 管理サーバー**］ノードで、タスク種別に［**アプリケーションのリモートインストール**］を選択します。

新規タスクウィザードが、選択したアプリケーションをリモートインストールするグループタスクを作成します。管理グループの作業領域の［**タスク**］タブに新たなタスクが表示されます。

5. 手動でタスクを実行するか、タスク設定で指定したスケジュールで開始されるのを待ちます。

リモートインストールタスクが完了すると、選択したアプリケーションが管理グループ内のクライアントデバイスにインストールされます。

Active Directory グループポリシーを使用したアプリケーションのインストール

Kaspersky Security Center では、Active Directory グループポリシーを使用して、管理対象デバイスにカスペルスキー製品をインストールできます。

Active Directory グループポリシーを使用したインストールは、ネットワークエージェントを含むインストールパッケージからのみ可能です。

Active Directory グループポリシーを使用してアプリケーションをインストールするには：

1. リモートインストールウィザードを使用して、アプリケーションインストールの設定を開始します。
2. リモートインストールウィザードの［**リモートインストールタスク設定の定義**］ウィンドウで、［**Active Directory のグループポリシーにパッケージのインストールを割り当てる**］をオンにします。
3. リモートインストールウィザードの［**デバイスにアクセスするアカウントの選択**］ウィンドウで、［**アカウントが必要（ネットワークエージェントの使用なし）**］を選択します。
4. Kaspersky Security Center をインストールするデバイスの管理者権限があるアカウントまたは Group Policy Creator Owners ドメイングループに含まれるアカウントを追加します。
5. 選択したアカウントに権限を付与するには：
   a. ［**コントロールパネル**］→［**管理ツール**］の順に選択し、［**グループポリシーの管理**］を開きます。
   b. 必要なドメインのフォルダーをクリックします。
   c. ［**委任**］セクションをクリックします。
   d. ［**権限**］のドロップダウンリストから［**GPO をリンク**］を選択します。
   e. ［**追加**］をクリックします。
   f. 開いた［**ユーザー、コンピューター、またはグループの選択**］ウィンドウで、必要なアカウントを選択します。
   g. ［OK］をクリックして、［**ユーザー、コンピューター、またはグループの選択**］ウィンドウを閉じます。
   h. ［**グループとユーザー**］の一覧で、先ほど追加したアカウントを選択して、［**詳細**］→［**詳細**］の順にクリックします。

i. ［**権限エントリ**］リストで、追加したアカウントをダブルクリックします。

j. 次の権限を付与します：

- **グループオブジェクトの作成**
- **グループオブジェクトの削除**
- **グループポリシーコンテナーオブジェクトの作成**
- **グループポリシーコンテナーオブジェクトの削除**

k. ［**OK**］をクリックして変更内容を保存します。

6. ウィザードの指示に従って、他の設定を定義します。

7. 作成されたリモートインストールタスクを手動で実行するか、スケジュール済みの開始まで待機します。

リモートインストールが次の順番で開始されます：

1. タスクの実行時に、指定したすべてのクライアントデバイスが属する各ドメインに次の項目が作成されます：
   - ［**Kaspersky_AK{GUID}**］という名前のグループポリシーオブジェクト（GPO）。
   - GPO に対応するセキュリティグループこのセキュリティグループには、タスクが適用されるクライアントデバイスが含まれます。セキュリティグループの内容によって、GPO の範囲が定義されます。
2. Kaspersky Security Center は、選択されたカスペルスキー製品を、本製品の共有ネットワークフォルダー「Share」から直接クライアントデバイスにインストールします。Kaspersky Security Center のインストールフォルダーでは、アプリケーションをインストールするための MSI ファイルを含む補助的なサブフォルダーが作成されます。
3. 新しいデバイスをタスク範囲に追加すると、次回のタスク開始時に、新しいデバイスがセキュリティグループに追加されます。タスクスケジュールで［**未実行のタスクを実行する**］をオンにしていると、デバイスはすぐにセキュリティグループに追加されます。
4. デバイスがタスク範囲から削除されると、次回のタスク開始時にセキュリティグループからも削除されます。
5. タスクを Active Directory から削除すると、GPO、GPO へのリンクおよび対応するセキュリティグループも削除されます。

Active Directory を使用して別のインストールスキームを適用する場合は、必要な設定を手動で指定できます。手動での設定が必要な可能性がある場合は次の通りです：

- アンチウイルスによる保護の管理者が一部のドメインの Active Directory で変更権限を持っていない場合
- 元のインストールパッケージを別のネットワークリソースに保存する必要がある場合
- 特定の Active Directory ユニットに GPO をリンクする場合

Active Directory で別のインストールスキームのオプションは次の通りです：

- インストールが Kaspersky Security Center の共有フォルダーから直接実行される場合、GPO プロパティで、目的のアプリケーションのインストールパッケージフォルダーのサブフォルダー exec にある MSI ファイルを指定する必要があります。

- インストールパッケージを別のネットワークリソースに配置する必要がある場合は、フォルダー exec の内容全部をネットワークリソースにコピーする必要があります。これは、このフォルダーには MSI ファイルの他に、パッケージの作成時に生成された構成ファイルが含まれているためです。アプリケーションと同時にライセンスをインストールするには、ライセンス情報ファイルもこのフォルダーにコピーします。

セカンダリ管理サーバーへのアプリケーションのインストール

セカンダリ管理サーバーにアプリケーションをインストールするには：

1. 目的のセカンダリ管理サーバーを制御する管理サーバーとの接続を確立します。
2. インストールするアプリケーションに対応するインストールパッケージが、選択したそれぞれのセカンダリ管理サーバー上で使用可能であるか確認してください。いずれのセカンダリ管理サーバーでもインストールパッケージを見つけることができない場合は、インストールパッケージ配布タスクを使用して配布します。
3. 次のいずれかの方法で、セカンダリ管理サーバーでアプリケーションのインストールタスクを作成します：
   - 選択した管理グループ内のセカンダリ管理サーバー用のタスクを作成する場合は、そのグループのリモートインストールのグループタスクを作成します。
   - 特定のセカンダリ管理サーバー用のタスクを作成する場合は、特定のデバイスのリモートインストールタスクを作成します。

   導入タスク作成ウィザードが起動し、リモートインストールタスクの作成手順が実行されます。ウィザードの指示に従います。

   新規タスクウィザードの［**タスク種別の選択**］ウィンドウにある［**Kaspersky Security Center 管理サーバー**］セクションで、［**詳細**］フォルダーを開き、タスク種別として［**セカンダリ管理サーバーへのアプリケーションのリモートインストール**］を選択します。

   新規タスクウィザードが、特定のセカンダリ管理サーバー上に、選択したアプリケーションのリモートインストールタスクを作成します。
4. 手動でタスクを実行するか、タスク設定で指定したスケジュールで開始されるのを待ちます。

リモートインストールタスクが完了すると、選択したアプリケーションがセカンダリ管理サーバーにインストールされます。

リモートインストールウィザードを使用したアプリケーションのインストール

カスペルスキー製品をインストールするには、リモートインストールウィザードを使用できます。リモートインストールウィザードにより、特別に作成されたインストールパッケージまたは配布パッケージを使用してアプリケーションをリモートインストールすることができます。

ネットワークエージェントがインストールされていないクライアントデバイスでリモートインストールタスクを正しく実行するには、次のポートを開いておく必要があります：TCP 139 および 445、UDP 137 および 138。既定では、これらのポートはドメイン内のすべてのデバイスで開いています。これらは、リモート導入準備ユーティリティによって自動的に開かれます。

リモートインストールウィザードを使用して、選択したデバイスに製品をインストールするには：

1. コンソールツリーで、［**リモートインストール**］フォルダー - ［**インストールパッケージ**］サブフォルダーの順に選択します。
2. そのフォルダーの作業領域で、インストールした製品のインストールパッケージを選択します。
3. インストールパッケージのコンテキストメニューで、［**アプリケーションのインストール**］を選択します。

   リモートインストールウィザードが起動します。
4. ［**インストールするデバイスの選択**］ウィンドウでは、製品のインストール先となるデバイスのリストを作成できます。

   - **管理対象デバイスのグループへ製品をインストールする**

     このオプションをオンにすると、デバイスのグループに対してリモートインストールタスクが作成されます。

   - **インストールするデバイスの選択**

     このオプションをオンにすると、特定のデバイスに対してリモートインストールタスクが作成されます。特定のデバイスには、管理対象デバイスと未割り当てデバイスの両方を含めることができます。
5. ［**リモートインストールタスク設定の定義**］ウィンドウで、製品のリモートインストールを設定します。

   ［**インストールパッケージの強制ダウンロード**］セクションで、アプリケーションのインストールに必要なファイルをクライアントデバイスに配布する方法を指定します。

   - **ネットワークエージェントを使用する**

     このオプションをオンにすると、インストールパッケージのクライアントデバイスへの配布は、クライアントデバイスにインストールされたネットワークエージェントによって行われます。

     このオプションをオフにすると、インストールパッケージはクライアントデバイスのオペレーティングシステムのツールを使用して配信されます。

     ネットワークエージェントがインストールされたデバイスにタスクが割り当てられている場合は、このチェックボックスをオンにすることを推奨します。

     既定では、このオプションはオンです。

   - **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**

     このオプションをオンにすると、管理サーバーを通じてクライアントデバイスのオペレーティングシステムツールを使用してクライアントデバイスにファイルが送信されます。このオプションは、クライアントデバイスにネットワークエージェントがインストールされていないものの、クライアントデバイスが管理サーバーと同じネットワークに存在する場合にオンにできます。

     既定では、このオプションはオンです。

   - **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**

このオプションをオンにすると、ディストリビューションポイントがオペレーティングシステムのツールを使用してインストールパッケージをクライアントデバイスに送信します。この機能が使用できるのは、ネットワークに少なくとも1つのディストリビューションポイントがある場合です。

［**ネットワークエージェントを使用する**］をオンにすると、ネットワークエージェントのツールが使用できない場合に限り、ファイルがオペレーティングシステムのツールで配布されます。

既定では、仮想管理サーバーで作成されたリモートインストールタスクに対して、このオプションはオンです。

- **インストール試行回数**

リモートインストールタスクの実行時に、この設定で指定した回数、管理対象デバイスで対象製品のインストールに失敗した場合、Kaspersky Security Center はこの管理対象デバイスへのインストールパッケージの配布を中止し、そのデバイス上でインストーラーを起動しなくなります。

インストール試行回数の設定を使用することで、管理対象デバイス上でのリソースの消費量とネットワークのトラフィック量を軽減することができます（アンインストールの実行や MSI ファイルの実行によるリソース消費や、エラーメッセージのトラフィック）。

タスクの開始が繰り返し試行されるということは、デバイス上でインストールを阻害する問題が発生している可能性があります。管理者は、インストールの指定した試行回数以内で問題を解決し（例：十分なディスク容量の確保、競合する製品の削除、インストールを阻害しているその他のアプリケーションの設定の変更など）、スケジュールを指定するか手動でタスクを再実行する必要があります。

指定された試行回数以内にインストールが実行されない場合、問題は解決不可能なものと認識され、それ以上タスクの開始を試行することは不必要にリソースとトラフィックを消費してしまうものと判断されます。

タスクの作成時に、試行回数のカウンターは「`0`」にセットされます。デバイス上でインストーラーを実行してエラーが返されるたびに、カウンターの値が1ずつ増加します。

設定で指定した回数のインストールの試行が既に実行された後に、デバイス上でのインストール準備が完了した場合、［インストール試行回数］の値を増やすことでインストールタスクを開始できます。または、リモートインストールタスクを新規に作成することもできます。

次のオプションを使用して、他の管理サーバーで管理されているクライアントデバイス上での処理を指定できます：

- **全デバイスにインストール**

他の管理サーバーで管理されているクライアントデバイスにもアプリケーションがインストールされます。

既定ではこのオプションが選択されます。ネットワーク内に管理サーバーが1台しかない場合は、この設定を変更する必要はありません。

- **この管理サーバーで管理されているデバイスにのみインストール**

アプリケーションはこの管理サーバーによって管理されているデバイスにのみインストールされます。ネットワーク内に複数の管理サーバーがあり、管理サーバー間での競合を回避したい場合は、このオプションを選択してください。

詳細設定を行います：

- **アプリケーションが既にインストールされている場合再インストールしない**

  このオプションをオンにすると、選択したアプリケーションがクライアントデバイスに既にインストールされていた場合、インストールされません。

  このオプションをオフにすると、アプリケーションは常にインストールされます。

  既定では、このオプションはオンです。

- **Active Directory のグループポリシーにパッケージのインストールを割り当てる**

  このオプションをオンにすると、Active Directory のグループポリシーを使用してインストールパッケージがインストールされます。

  このオプションは、ネットワークエージェントのインストールパッケージが選択されている場合に使用可能になります。

  既定では、このオプションはオフです。

6. ［**ライセンスの選択**］ウィンドウで、ライセンスとライセンスの配信方法を選択します：

   - **ライセンスやアクティベーションコードをインストールパッケージに含めない（推奨）**

     次の条件を満たす場合、ライセンスは互換性のあるすべてのデバイスへ自動的に配信されます：

     - ライセンスのプロパティで［自動配信］が有効になっている場合。
     - ［**ライセンスの追加**］タスクが作成されている場合。

   - **ライセンスまたはアクティベーションコードをインストールパッケージに含める**

     ライセンスはインストールパッケージと共にデバイスへ配信されます。

     共有読み取りアクセス権がインストールパッケージのリポジトリに対して有効になっているため、この方法はできるだけ使用しないでください。

   ［**ライセンスの選択**］ウィンドウは、インストールパッケージにライセンスが含まれていない場合に表示されます。

   インストールパッケージにライセンスが含まれている場合、ライセンスの詳細が記載された［**ライセンスのプロパティ**］ウィンドウが表示されます。

7. ［**オペレーティングシステムの再起動のオプションを選択**］ウィンドウで、アプリケーションのインストール中にオペレーティングシステムを再起動する場合、デバイスを再起動する必要があるか指定します：

   - **デバイスを再起動しない**

     このオプションをオンにすると、セキュリティ製品のインストール後にデバイスが再起動されません。

   - **デバイスを再起動する**

このオプションをオンにすると、セキュリティ製品のインストール後にデバイスが再起動されます。

- **ユーザーに処理を確認する**

  このオプションをオンにすると、セキュリティ製品のインストール後に、デバイスを再起動する必要があることを知らせる通知がユーザーに表示されます。［**変更**］を使用すると、メッセージの本文、メッセージの表示時間、および自動再起動の時間を変更できます。

  既定では、このオプションがオンです。

- **セッションがブロックされたアプリケーションを強制終了する**

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。

  既定では、このオプションはオフです。

8. ［**デバイスにアクセスするアカウントの選択**］ウィンドウで、リモートインストールタスクの開始に使用するアカウントを追加できます：

   - **アカウントが不要 (ネットワークエージェントインストール済み)**

     このオプションをオンにすると、アプリケーションのインストーラーを実行するアカウントを指定する必要はありません。タスクは管理サーバーのサービスを実行しているアカウントで実行されます。

     クライアントデバイスにネットワークエージェントがインストールされていない場合、このオプションは使用できません。

   - **アカウントが必要（ネットワークエージェントの使用なし）**

     リモートインストールタスクを割り当てるデバイスにネットワークエージェントがインストールされていない場合は、このオプションをオンにします。この場合、ユーザーアカウントまたは SSH 証明書を指定して、アプリケーションをインストールできます。

     - **ローカルアカウント**。このオプションをオンにする場合、アプリケーションのインストーラーを実行するユーザーアカウントを指定します。［**追加**］をクリックし、［**ローカルアカウント**］を選択してから、ユーザーアカウントの資格情報を指定します。

       タスクを割り当てるすべてのデバイスで必要なすべての権限をどのアカウントも持たない場合などのために、複数のユーザーアカウントを追加できます。この場合、追加されたすべてのアカウントが上から下へ順番に使用され、タスクが実行されます。

     - **SSH 証明書**。Linux ベースのクライアントデバイスにアプリケーションをインストールする場合、ユーザーアカウントの代わりに SSH 証明書を指定できます。［**追加**］をクリックし、［**SSH 証明書**］を選択してから、証明書の秘密鍵と公開鍵を指定します。

       秘密鍵を生成するには、ssh-keygen ユーティリティを使用できます。Kaspersky Security Center は PEM 形式の秘密鍵をサポートしますが、ssh-keygen ユーティリティは既定で SSH 鍵を OPENSSH 形式で生成します。OPENSSH 形式は Kaspersky Security Center ではサポートされていません。サポートされる PEM 形式で秘密鍵を作成するには、ssh-keygen コマンドに -m PEM オプションを追加します。例：

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "<ユーザーのメールアドレス>"
       ```

9. ［**インストールの開始**］ウィンドウで、［**次へ**］をクリックし、選択したデバイスでリモートインストールタスクの作成と開始を行います。

   ［**インストールの開始**］ウィンドウ内にある［**リモートインストールウィザードの終了後にタスクを実行しない**］が選択されている場合、リモートインストールタスクは開始されません。このタスクは後から手動で開始できます。タスク名はアプリケーションのインストールパッケージの名前に対応し、「**<インストールパッケージの名前> のインストール**」となります。

管理グループ内のデバイスに、リモートインストールウィザードを使用してアプリケーションをインストールするには：

1. 関連する管理グループを管理している管理サーバーとの接続を確立します。
2. コンソールツリーで管理グループを選択します。
3. このグループの作業領域で、［**処理を実行**］をクリックし、ドロップダウンリストから［**アプリケーションのインストール**］を選択します。

   リモートインストールウィザードが起動します。ウィザードの指示に従ってください。
4. ウィザードの最終ステップで［**次へ**］をクリックすると、選択したデバイスに対するリモートインストールタスクが作成され、実行されます。

リモートインストールウィザードが完了すると、Kaspersky Security Center が以下を実行します：

- アプリケーションをインストールするためのインストールパッケージを作成します（まだ作成されていない場合）。インストールパッケージは、［**リモートインストール**］フォルダー内の［**インストールパッケージ**］サブフォルダーに格納されており、これにはアプリケーションの名前とバージョンに対応する名前が付けられています。今後アプリケーションをインストールする時に、このインストールパッケージを使用できます。
- 特定のデバイスまたは管理グループに対するリモートインストールタスクを作成して実行します。作成したリモートインストールタスクは［**タスク**］フォルダーに保存されるか、作成された管理グループのタスクに追加されます。このタスクは後から手動で開始できます。タスク名はアプリケーションのインストールパッケージの名前に対応し、「**<インストールパッケージの名前> のインストール**」となります。

管理プラグインの使用

カスペルスキー製品は、管理プラグインを使用して管理コンソールで管理します。Kaspersky Security Center で管理できるカスペルスキー製品には、管理プラグインが含まれています。アプリケーションの管理プラグインを使用すると、管理コンソールで次の処理を行うことができます：

- アプリケーションポリシーと設定、およびアプリケーションタスクの設定の作成および編集
- クライアントデバイスから受信したアプリケーションタスク、アプリケーションイベント、およびアプリケーション動作の統計データに関する情報の取得

インストールされているプラグインとそのバージョンのリストを確認するには：

1. 管理コンソールツリーで、［**管理サーバー <Server_name>**］を右クリックし、［**プロパティ**］を選択します。
2. ［**詳細**］→［**インストール済みアプリケーション管理プラグインの詳細情報**］をクリックします。

インストールされている管理プラグインとそのバージョンのリストが右側のペインに表示されます。

Kaspersky Security Center の初期セットアップ中に管理サーバーのクイックスタートウィザードを実行する場合、管理対象アプリケーションのプラグインをインストールできます。また、管理プラグインを手動でインストールすることもできます。

管理プラグインを手動でインストールするには：

1. カスペルスキーテクニカルサポート Web ページから、カスペルスキー製品の管理プラグインと必要なバージョン（たとえば、 Kaspersky Endpoint Security for Windows 12.6）をダウンロードします。
2. 管理コンソールが実行中の場合は、閉じます。
3. ダウンロードしたプラグインファイルを解凍し、ファイル klcfginst.msi または klcfginst.exe を実行します。ウィザードの指示に従ってください。
4. インストールが完了したら、管理コンソールを実行し、前の手順で説明したように、インストールされているプラグインのリストにプラグインが表示されていることを確認します。

管理対象アプリケーションのクイックスタートウィザードをサポートする管理プラグインをインストールした後に管理コンソールを実行すると、このウィザードが自動的に起動されます。管理対象アプリケーションのクイックスタートウィザードの手順に従って、既定のカスペルスキー製品ポリシーとタスクを作成できます。ウィザードは、プラグインの初期インストール後、またはタスクとポリシーがまだ作成されていないカスペルスキー製品の別のバージョンと互換性のあるバージョンに管理プラグインをアップデートした後に、管理コンソールを実行した場合にのみ自動的に起動します。管理対象アプリケーションのクイックスタートウィザードを手動で起動することもできます。

管理対象アプリケーションのクイックスタートウィザードを手動で起動するには：

1. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。
2. 管理サーバーノードのコンテキストメニューで、［**すべてのタスク**］→［**管理対象アプリケーションのクイックスタートウィザード**］の順に選択します。
3. 管理対象アプリケーションのクイックスタートウィザードが起動します。ウィザードの手順に従って、既定のカスペルスキー製品ポリシーとタスクを作成します。

管理プラグインを削除するには：

1. 管理コンソールが実行中の場合は、閉じます。
2. Windows レジストリエディタを開きます。
3. 次のライセンスを見つけます：

   - 32 ビットシステムの場合は、
     `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\28\Plugins`
   - 64 ビットシステムの場合は、
     `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins`

   ライセンスには、インストールされた管理プラグインが含まれています。各プラグインの `DisplayName` 値にはプラグイン名が含まれ、`UninstallString` 値にはプラグインをアンインストールするコマンドが含まれます。
4. アンインストールするプラグインのライセンスを見つけて、その `UninstallString` 値をクリップボードにコピーします。
5. 値をコマンド文字列に貼り付け、システム管理者権限で実行します。

管理プラグインのバージョンは、カスペルスキー管理対象アプリケーションのバージョンよりも前であってはなりません。デバイス上のカスペルスキー製品をアップデートする場合は、同じバージョンの管理プラグインをインストールする必要があります。

以前のバージョンのプラグインで作成されたポリシーを開くと、Kaspersky Security Network に関する声明に同意するよう求められます。

Kaspersky Security Center Web コンソールをアンインストールすると、すべての管理プラグインもアンインストールされます。

管理対象アプリケーションのバージョンよりも新しいバージョンのプラグインでポリシーを開いて保存すると、ポリシーがアップデートされ、以前のバージョンのプラグインでは開くことができなくなります。

製品導入レポートの確認

製品導入レポートを使用すると、ネットワーク保護の導入の進行状況を監視できます。

製品導入レポートを確認するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**レポート**］タブを選択します。
3. ［**レポート**］フォルダーの作業領域で「**製品導入レポート**」という名前のレポートテンプレートを選択します。

ネットワーク内のすべてのデバイスへの製品導入に関するレポートが作業領域に表示されます。

新規の製品導入レポートを生成し、次の内容を含むデータの種類を指定できます：

- 管理グループ
- 特定のデバイス
- デバイスの抽出
- すべてのデバイス

Kaspersky Security Center は、デバイスにセキュリティ製品がインストールされていてリアルタイム保護が有効になっている場合に、そのデバイスに製品が導入されているとみなします。

アプリケーションのリモート削除

Kaspersky Security Center では、リモート削除タスクを使用してデバイスからアプリケーションをリモート削除できます。このタスクは、専用のウィザードを使用して作成しデバイスに割り当てます。タスクを簡単にデバイスに割り当てるには、次のいずれかの方法を使用し、ウィザードウィンドウでデバイスを指定できます：

- **ネットワークの管理サーバーによって検出されたデバイスを選択する**：この場合、タスクを特定のデバイスに割り当てます。特定のデバイスには、管理グループに属するデバイスと管理グループが割り当てられていないデバイスの両方を含めることができます。
- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**：タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。
- **デバイスの抽出にタスクを割り当てる**：この場合、既に作成された抽出に属するデバイスにタスクを割り当てます。事前定義の抽出または作成済みのカスタム抽出を指定できます。
- **管理グループにタスクを割り当てる**：この場合、既に作成された管理グループに属するデバイスにタスクを割り当てます。

管理グループのクライアントデバイスからのアプリケーションのリモート削除

管理グループのクライアントデバイスからアプリケーションをリモート削除するには：

1. 関連する管理グループを管理している管理サーバーとの接続を確立します。
2. コンソールツリーで管理グループを選択します。
3. グループの作業領域で、［**タスク**］タブを選択します。
4. ［**新規タスク**］をクリックしてタスクの作成を実行します。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

   新規タスクウィザードの［**タスク種別の選択**］ウィンドウで［**Kaspersky Security Center 管理サーバー**］ノードを選択し、［**詳細**］フォルダーでタスク種別に［**アプリケーションのリモートアンインストール**］を選択します。

   新規タスクウィザードが、選択したアプリケーションをリモートで削除するグループタスクを作成します。管理グループの作業領域の［**タスク**］タブに新たなタスクが表示されます。
5. 手動でタスクを実行するか、タスク設定で指定したスケジュールで開始されるのを待ちます。

リモート削除タスクが完了すると、選択したアプリケーションが該当の管理グループのクライアントデバイスから削除されます。

特定のデバイスからのアプリケーションのリモート削除

アプリケーションを特定のデバイスからリモート削除するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. ［**新規タスク**］をクリックしてタスクの作成を開始します。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

新規タスクウィザードの［**タスク種別の選択**］ウィンドウで［**Kaspersky Security Center 管理サーバー**］ノードを選択し、［**詳細**］フォルダーでタスク種別に［**アプリケーションのリモートアンインストール**］を選択します。

新規タスクウィザードが、指定したデバイスから選択したアプリケーションをリモートで削除するタスクを作成します。新規作成されたタスクが、［**タスク**］フォルダーの作業領域に表示されます。

3. 手動でタスクを実行するか、タスク設定で指定したスケジュールで開始されるのを待ちます。

リモート削除タスクが完了すると、選択したアプリケーションが選択されたデバイスから削除されます。

インストールパッケージの使用

リモートインストールタスクの作成時には、ソフトウェアのインストールに必要なパラメータのセットを含むインストールパッケージが使用されます。

インストールパッケージにライセンス情報ファイルを含めることができます。ライセンス情報ファイルを含むインストールパッケージへのアクセスを共有することは避けてください。

インストールパッケージは何度でも使用できます。

管理サーバー用に作成したインストールパッケージは、コンソールツリーの［**リモートインストール**］フォルダーの［**インストールパッケージ**］サブフォルダーに格納されます。インストールパッケージは、管理サーバーで指定された共有フォルダー内のサブフォルダー Packages に置かれています。

インストールパッケージの作成

この記事では、次の種類のインストールパッケージを作成する手順について説明します：

- カスペルスキー製品のインストールパッケージ
- 指定された実行ファイルのインストールパッケージ
- カスペルスキー定義データベースからのアプリケーションのインストールパッケージ

ネットワークエージェントをリモートインストールするためのインストールパッケージを手動で作成する必要はありません。Kaspersky Security Center のインストール時に自動的に作成され、［**インストールパッケージ**］フォルダーに保存されます。ネットワークエージェントのリモートインストールパッケージが削除されている場合に再作成するには、Kaspersky Security Center の配布パッケージのフォルダー NetAgent にあるファイル nagent.kud を選択します。

インストールパッケージを作成するには：

1. 目的の管理サーバーに接続します。
2. コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］フォルダーの順に選択します。
3. 次のいずれかの方法で新しいインストールパッケージの作成を開始します：

- ［**インストールパッケージ**］フォルダーを右クリックし、コンテキストメニューから［**新規**］→［**インストールパッケージ**］を選択します。
- インストールパッケージリストの空白領域を右クリックし、コンテキストメニューから［**作成**］→［**インストールパッケージ**］を選択します。
- インストールパッケージのリスト管理セクションにある［**インストールパッケージの作成**］をクリックします。

新規パッケージウィザードが起動します。

4. 対応するアイコンをクリックして、次のいずれかのインストールパッケージタイプを選択します。
   - カスペルスキー製品のインストールパッケージ。
   - 指定された実行ファイルのインストールパッケージ。
   - カスペルスキー定義データベースからのアプリケーションのインストールパッケージ。
5. 作成するインストールパッケージの名前を指定します。

   任意の名前を指定できます。
6. 次のいずれかの方法で、インストールパッケージを作成するアプリケーションまたは実行ファイルを選択します。
   - ［**参照**］をクリックし、標準の Windows の［**開く**］ウィンドウで、使用可能なディスクにある必要なアプリケーションの配布パッケージを選択します。

     このオプションは、カスペルスキー製品または指定された実行ファイルのインストールパッケージを作成する場合に適用されます。
   - ［**参照**］をクリックし、［**アプリケーションの選択**］ウィンドウで、必要なアプリケーションの配布パッケージを選択します。

     このオプションは、カスペルスキー定義データベースからアプリケーションのインストールパッケージを作成する場合に適用されます。

   管理サーバーのインストールパッケージを作成する場合は、ファイル sc.kud を選択します。ファイル sc.kud は、Kaspersky Security Center 配布パッケージのルートフォルダーにあります。

   インストールパッケージの設定では、特別な権限を持つアカウントを指定しないでください。
7. 使用許諾契約書とプライバシーポリシーを確認します。

   アプリケーションのインストールパッケージを作成する時に、そのアプリケーションのエンドユーザー使用許諾契約書およびプライバシーポリシーを表示して同意するように要求される場合があります。

   両方のドキュメントを読んでください。使用許諾契約書およびプライバシーポリシーのすべての条件に同意する場合は、該当するチェックボックスをオンにすることで同意します。

   デバイスへのアプリケーションのインストールが続行され、インストールパッケージの作成が再開されます。

   Kaspersky Endpoint Security for Mac のインストールパッケージを作成する場合、使用許諾契約書およびプライバシーポリシーの言語を選択できます。
8. 必要に応じて、システムコンポーネントの自動インストールを有効にします。

カスペルスキー定義データベースからアプリケーションのインストールパッケージを作成する場合は、必要なシステムコンポーネントの自動インストールを有効にすることができます。新規パッケージウィザードに、選択した製品に使用可能なすべてのシステムコンポーネントのリストが表示されます。インストールパッケージのプロパティでいつでもこのリストにアクセスできます。

パッチインストールパッケージを作成する場合、リストにはこのパッチの導入に必要なすべてのシステムコンポーネントが含まれます。

9. ［**終了**］をクリックして、パッケージ作成プロセスを完了します。

新規パッケージウィザードが完了すると、コンソールツリーの［**インストールパッケージ**］フォルダーのワークスペースに、新規作成されたインストールパッケージが表示されます。

スタンドアロンインストールパッケージの作成

組織内の管理者とユーザーがデバイスに手動でアプリケーションをインストールするために、スタンドアロンインストールパッケージを使用できます。

スタンドアロンパッケージは実行ファイル形式（installer.exe）で、Web サーバーや共有フォルダーへの配置などによりクライアントデバイスに受け渡すことができます。スタンドアロンインストールパッケージへのリンクをメールで送ることもできます。クライアントデバイスで受け取った実行ファイルをローカルで起動することで、Kaspersky Security Center を使用せずにアプリケーションをインストールすることが可能となります。

スタンドアロンインストールパッケージは、権限のないユーザーからアクセスできないようにしてください。

カスペルスキー製品および Windows、macOS、Linux プラットフォーム用のサードパーティ製品のスタンドアロンインストールパッケージを作成できます。サードパーティ製品のインストールパッケージを作成するには、カスタムインストールパッケージを最初に作成する必要があります。

スタンドアロンインのストールパッケージは、管理サーバーで作成されたリスト内のインストールパッケージを元に作成します。

スタンドアロンインストールパッケージを作成するには：

1. コンソールツリーで、［**管理サーバー**］→［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］の順に選択します。

   管理サーバーで利用可能なインストールパッケージのリストが表示されます。

2. インストールパッケージのリストで、スタンドアロンパッケージを作成するインストールパッケージを選択します。

3. コンテキストメニューで、［**スタンドアロンインストールパッケージの作成**］を選択します。

   スタンドアロンインストールパッケージ作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

4. 選択したカスペルスキー製品のインストールパッケージとネットワークエージェントを合わせてインストールする場合、ウィザードの最初のページで［**このアプリケーションと同時にネットワークエージェントをインストールする**］がオンであることを確認します。

既定では、このオプションはオンです。デバイスにネットワークエージェントがインストール済みかどうかが不明な場合は、このオプションをオンにすることを推奨します。ネットワークエージェントがデバイスにインストールされている場合、ネットワークエージェントを含めたスタンドアロンインストールパッケージのインストール後に、ネットワークエージェントが新しいバージョンにアップデートされます。

このオプションがオフの場合、デバイスにはネットワークエージェントはインストールされず、デバイスは管理対象外のデバイスになります。

選択したアプリケーションのスタンドアロンインストールパッケージが既に管理サーバー上に存在する場合、ウィザードに通知が表示されます。この場合、次のいずれかのオプションを選択する必要があります：

- **スタンドアロンインストールパッケージの作成**：新しいバージョンのアプリケーションのスタンドアロンインストールパッケージを新規に作成し、なおかつ以前のバージョンのアプリケーションで作成したスタンドアロンインストールパッケージも保持する場合などにこのオプションをオンにします。新しいスタンドアロンインストールパッケージは別のフォルダーに配置されます。

- **既存のスタンドアロンインストールパッケージを使用**：既存のスタンドアロンインストールパッケージを使用する場合は、このオプションをオンにします。パッケージの作成プロセスは開始されません。

- **既存のスタンドアロンインストールパッケージを再構築**：同じアプリケーションのインストールパッケージを再作成する場合、このオプションを選択します。スタンドアロンインストールパッケージは、同じフォルダーに保存されます。

5. ウィザードの次のページで、［**未割り当てデバイスをこのグループへ移動**］をオンにし、ネットワークエージェントのインストール後にクライアントデバイスを移動させる管理グループを指定します。

   既定では、デバイスは［**管理対象デバイス**］グループに移動されます。

   ネットワークエージェントのインストール後にクライアントデバイスを管理グループに移動させたくない場合は、［**デバイスを移動しない**］をオンにします。

6. ウィザードの次のページで、スタンドアロンインストールパッケージの作成プロセスが完了すると、スタンドアロンパッケージの作成結果とスタンドアロンパッケージのパスが表示されます。

   リンクをクリックし、次の操作を実行できます：

   - スタンドアロンインストールパッケージのフォルダーを開きます。

   - 作成されたスタンドアロンインストールパッケージへのリンクをメールで送信します。この操作を実行するには、メールソフトを起動する必要があります。

   - Web サイトで公開するリンクのサンプル HTML コードを生成します。TXT ファイルが作成され、TXT 形式に関連付けられたアプリケーションで開きます。ファイルには、HTML の <a> タグ（属性付き）が表示されます。

7. ウィザードの次のページで、スタンドアロンインストールパッケージのリストを開く場合は、［**スタンドアロンパッケージのリストを開く**］をオンにします。

8. ［**終了**］をクリックします。

   ［スタンドアロンインストールパッケージ作成ウィザード］が閉じます。

スタンドアロンインストールパッケージが作成され、管理サーバーの共有フォルダーのパッケージ用のサブフォルダーにダウンロードされます。インストールパッケージのリストの上にある［**スタンドアロンパッケージリストの表示**］をクリックすると、スタンドアロンパッケージのリストを確認できます。

カスタムインストールパッケージの作成

以下のような用途でカスタムインストールパッケージを使用できます：

- たとえばタスクを使用して、サードパーティ製を含む任意のアプリケーション（テキストエディターなど）をクライアントデバイスにインストールするため。
- スタンドアロンインストールパッケージを作成するため。

カスタムインストールパッケージは、複数のファイルを含んだフォルダーです。カスタムインストールパッケージは、*圧縮ファイル*を元に作成します。圧縮ファイルには、カスタムインストールパッケージに含める必要のあるファイルが含まれているようにします。カスタムインストールパッケージの作成時に、コマンドラインのパラメータを指定できます（例：製品をサイレントモードでインストールするパラメータ）。

カスタムインストールパッケージを作成するには：

1. コンソールツリーで、［**管理サーバー**］→［**詳細設定**］→［**リモートインストール**］→［**インストールパッケージ**］の順に選択します。

   管理サーバーで利用可能なインストールパッケージのリストが表示されます。

2. インストールパッケージのリストの上にある［**インストールパッケージの作成**］をクリックします。

   新規パッケージウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ウィザードの最初のページで、［**指定した実行ファイルのインストールパッケージを作成する**］を選択します。

4. ウィザードの次のページで、カスタムインストールパッケージの名前を指定します。

5. ウィザードの次のページでは、［**参照**］をクリックすると表示される Windows 標準の［**ファイルを開く**］ウィンドウで、使用可能なディスクにある圧縮ファイルを選択して、カスタムインストールパッケージを作成します。

   ZIP、CAB、TAR、または TAR.GZ アーカイブをアップロードできます。インストールパッケージを SFX ファイル（自己解凍型の圧縮ファイル）から作成することはできません。

   ファイルは Kaspersky Security Center 管理サーバーにダウンロードされます。

6. ウィザードの次のページで、実行ファイルのコマンドラインパラメータを指定します。

   インストールパッケージから製品をサイレントモードでインストールするためのコマンドラインのパラメータを指定できます。コマンドラインのパラメータの指定は省略可能です。

   必要に応じて、次のオプションを設定します：

   - **フォルダー全体をインストールパッケージへコピー**

     アプリケーションのインストールに、実行ファイル以外のファイルが追加で必要となる場合、このオプションを選択します。このオプションをオンにする前に、必要なすべてのファイルが同じフォルダーに保存されていることを確認してください。このオプションをオンにすると、指定した実行ファイルを含めてフォルダー内のすべてのファイルがインストールパッケージに追加されます。

   - **Kaspersky Security Center で認識されたアプリケーションの設定値を推奨値に変換する**

カスペルスキーのデータベースに該当するアプリケーションの情報が含まれていた場合は、アプリケーションは推奨設定でインストールされます。

［**実行ファイルのコマンドライン**］でパラメータを指定していた場合も、推奨設定でパラメータが上書きされます。

既定では、このオプションはオンです。

カスペルスキーのデータベースは、カスペルスキーの担当者によって作成・維持されています。データベースに追加されたそれぞれのアプリケーションに対して、カスペルスキーの担当者が最適なインストール設定を指定しています。これらの設定は、クライアントデバイスへのリモートインストールが正常に完了するように指定されます。管理サーバー上のこのデータベースは、管理サーバーのリポジトリへのアップデートのダウンロードタスクの実行時に自動的にアップデートされます。

カスタムインストールパッケージを作成するプロセスが開始されます。

プロセスが終了すると、ウィザードで通知されます。

カスタムインストールパッケージが作成されなかった場合、メッセージで通知されます。

7. ［**終了**］をクリックしてウィザードを終了します。

作成したインストールパッケージは、管理サーバーの共有フォルダーのパッケージ用のサブフォルダーにダウンロードされます。ダウンロード後、カスタムインストールパッケージがインストールパッケージのリストに表示されます。

管理サーバー上のインストールパッケージのリストで、カスタムインストールパッケージのプロパティを表示および編集できます。

カスタムインストールパッケージのプロパティの表示と編集

カスタムインストールパッケージを作成した後、プロパティウィンドウでインストールパッケージに関する一般情報を確認し、インストール設定を指定できます。

カスタムインストールパッケージのプロパティを表示したり編集するには：

1. コンソールツリーで、［**管理サーバー**］→［**詳細設定**］→［**リモートインストール**］→［**インストールパッケージ**］の順に選択します。

   管理サーバーで利用可能なインストールパッケージのリストが表示されます。

2. インストールパッケージのコンテキストメニューで、［**プロパティ**］を選択します。

   選択したインストールパッケージのプロパティウィンドウが表示されます。

3. 次の情報を確認します：

   - インストールパッケージ名
   - カスタムインストールパッケージに含まれるアプリケーションの名前
   - アプリケーションのバージョン
   - インストールパッケージの作成日
   - 管理サーバー上のカスタムインストールパッケージへのパス

- 実行ファイルのコマンドライン

4. 次の設定を指定します：

- インストールパッケージ名
- **必要なシステムコンポーネントをインストールする**

  このオプションをオンにすると、アップデートのインストール前にインストールが必要な一般システムコンポーネントをすべて自動的にインストールします。インストールが必要な対象とは、たとえばオペレーティングシステムのアップデートなどです。

  このオプションをオフにすると、必須コンポーネントを手動でインストールすることが必要となる場合があります。

  既定では、このオプションはオフです。

  このオプションは、インストールパッケージに追加されたアプリケーションが Kaspersky Security Center によって認識されている場合にのみ使用できます。

- **実行ファイルのコマンドライン**

  インストール対象のアプリケーションでサイレントインストールのパラメータを指定する必要がある場合は、このフィールドで指定します。詳細については、該当する製品の製造元の資料を参照してください。

  その他のパラメータを指定することもできます。

  このオプションは、カスペルスキー製品以外を対象に作成したインストールパッケージでのみ実行できます。

5. ［**OK**］または［**適用**］をクリックして、変更がある場合は保存します。

新しい設定が保存されます。

Kaspersky Security Center 配信キットからネットワークエージェントインストールパッケージを入手する

ネットワークエージェントのインストールパッケージは、Kaspersky Security Center 配信キットから入手できます。Kaspersky Security Center のインストールは不要です。インストールパッケージを使用して、ネットワークエージェントをクライアントデバイスにインストールできます。

Kaspersky Security Center の配信キットからネットワークエージェントのインストールパッケージを入手するには：

1. Kaspersky Security Center の配布キットから、実行ファイル ksc_<バージョン番号>.<ビルド番号>_full_<言語>.exe を実行します。
2. ウィンドウが表示されたら、［**インストールパッケージの解凍**］をクリックします。

3. インストールパッケージのリストで、ネットワークエージェントインストールパッケージに隣接するチェックボックスをオンにして、［**次へ**］をクリックします。

4. 必要に応じて、［**参照**］をクリックして、インストールパッケージを展開するために表示されたフォルダーを変更します。

5. ［**解凍**］をクリックします。
   ネットワークエージェントのインストールパッケージが展開されます。

6. ダウンロードが完了したら、［**閉じる**］をクリックします。

ネットワークエージェントのインストールパッケージが、選択したフォルダに展開されます。

インストールパッケージを使用して、次のいずれかの方法でネットワークエージェントをインストールできます：

- ローカルで展開されたフォルダーからファイル setup.exe を実行
- サイレントインストールを使用
- Microsoft Windows のグループポリシーを使用

セカンダリ管理サーバーへのインストールパッケージの配布

セカンダリ管理サーバーにインストールパッケージを配布するには：

1. 目的のセカンダリ管理サーバーを制御する管理サーバーとの接続を確立します。

2. 次のいずれかの方法で、セカンダリ管理サーバーへのインストールパッケージの配布タスクを作成します：

   - 選択した管理グループ内でセカンダリ管理サーバー用のタスクを作成する場合は、そのグループのグループタスクを作成します。

   - 特定のセカンダリ管理サーバー用のタスクを作成するには、デバイスを指定してタスクを作成します。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
   新規タスクウィザードの［**タスク種別の選択**］ウィンドウで［**Kaspersky Security Center 管理サーバー**］ノードを選択し、［**詳細**］フォルダーでタスク種別に［**インストールパッケージの配布**］を選択します。
   指定したインストールパッケージをセカンダリ管理サーバーに配布するタスクが作成されます。

3. 手動でタスクを実行するか、タスク設定で指定したスケジュールに基づいてタスクが起動するのを待ちます。

選択したインストールパッケージが指定のセカンダリ管理サーバーにコピーされます。

ディストリビューションポイントを使用したインストールパッケージの配布

ディストリビューションポイントを使用して、インストールパッケージを管理グループ内に配布できます。

ディストリビューションポイントは、管理サーバーからのインストールパッケージの受信後、IP マルチキャストを用いてクライアントデバイスにパッケージを自動配布します。管理グループ内で、新しいインストールパッケージの IP マルチキャストが一度だけ実行されます。配布時にクライアントデバイスが企業ネットワークから切断されていた場合は、インストールタスクを開始した時に、必要なインストールパッケージがディストリビューションポイントから自動的にダウンロードされます。

Kaspersky Security Center へのアプリケーション導入結果の送信

アプリケーションのインストールパッケージの作成後、そのアプリケーションのインストール結果に関するすべての診断情報が Kaspersky Security Center に送信されるように設定できます。カスペルスキー製品のインストールパッケージに関しては、アプリケーションのインストール結果に関する診断情報の送信が既定で設定されており、詳細設定は必要ありません。

アプリケーションのインストールに関する診断情報を Kaspersky Security Center に送信するよう設定するには：

1. Kaspersky Security Center を使用して選択されたアプリケーションに対して作成したインストールパッケージのフォルダーに移動します。このフォルダーは、Kaspersky Security Center のインストール時に指定された共有フォルダー内にあります。

2. Microsoft Windows メモ帳などで、拡張子が kpd または kud のファイルを編集用に開きます。

   ファイルの形式は通常の INI ファイルと同様です。

3. 次の行をファイルに追加します：

   ```
   [SetupProcessResult]
   Wait=1
   ```

   このコマンドによって、Kaspersky Security Center はインストールパッケージを作成したアプリケーションのセットアップの完了を待機し、インストーラーのリターンコードを分析するように設定されます。診断データの送信を無効にする必要がある場合は、Wait ライセンスの値を 0 に設定します。

4. 成功したインストールのリターンコードの説明を追加します。次の行をファイルに追加します：

   ```
   [SetupProcessResult_SuccessCodes]
   <リターンコード>=[<説明>]
   <リターンコード 1>=[<説明>]
   ...
   ```

   > [ ] で囲まれた項目はオプションキーです。

   行の構文は次の通りです：

   - <リターンコード>：インストーラーのリターンコードに対応する数字。リターンコードの数値は任意です。
   - <説明>：インストール結果の説明テキスト。説明は省略可能です。

5. 失敗したインストールのリターンコードの説明を追加します。次の行をファイルに追加します：

   ```
   [SetupProcessResult_ErrorCodes]
   <リターンコード>=[<説明>]
   <リターンコード 1>=[<説明>]
   ```

...
これらの行の構文は、成功したセットアップのリターンコードを含む行の構文と同一です。

6. すべての変更を保存して、kpd または kud ファイルを閉じます。

ユーザー定義アプリケーションのインストール結果に関する情報が Kaspersky Security Center のログに登録され、イベントのリスト、レポートおよびタスクのログで、関係するイベントのリストに表示されます。

インストールパッケージの KSN プロキシサーバーアドレスの定義

管理サーバーのアドレスまたはドメインが変更された場合は、インストールパッケージの KSN プロキシサーバーアドレスを定義できます。

インストールパッケージの KSN プロキシサーバーアドレスを定義するには、次の手順に従います：

1. コンソールツリーの［**リモートインストール**］フォルダーで、［**インストールパッケージ**］サブフォルダーをダブルクリックします。
2. 開いたメニューで、［**プロパティ**］を選択します。
3. タスクのプロパティウィンドウが開いたら、［**全般**］セクションを選択します。
4. プロパティウィンドウの［**一般**］サブセクションに、KSN プロキシサーバーのアドレスを入力します。

インストールパッケージは、このアドレスを既定として使用します。

アプリケーションの最新バージョンの取得

Kaspersky Security Center で、カスペルスキーのサーバー上に保存されている法人向け製品の最新版を取得できます。

カスペルスキーの法人向け製品の最新バージョンを取得するには：

1. 次のいずれかの手順を実行します：

   - コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。［**監視**］タブが選択されていることを確認し、［**製品の導入**］セクションで、［**カスペルスキー製品の新しいバージョンが入手可能です**］をクリックします。

     ［**カスペルスキー製品の新しいバージョンが入手可能です**］は、カスペルスキーのサーバー上でアプリケーションの最新バージョンが見つかった時点で表示されます。

   - コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］の順に選択し、作業領域で［**その他の操作**］をクリックして、ドロップダウンリストから［**カスペルスキー製品の現在のバージョンの表示**］を選択します。

   カスペルスキー製品の、現在のバージョンのリストが表示されます。

2. カスペルスキー製品のリストをフィルタリングして、必要な製品を検索しやすくできます。

   ［**現在入手可能な製品バージョン**］ウィンドウの上部にある［**フィルター**］をクリックして、次の条件で製品のリストをフィルタリングします：

- **コンポーネント**：この条件を使用して、ネットワークで使用されている保護領域でカスペルスキー製品のリストをフィルタリングします。
- **ダウンロードされたソフトウェアの種別**：この条件を使用して、カスペルスキー製品のリストを製品の種別でフィルタリングします。
- **表示するソフトウェアとアップデート**：この条件を使用して、使用可能なカスペルスキー製品を特定のバージョン別に表示します。
- **ソフトウェアおよびアップデートを表示する言語**：この条件を使用して、特定のローカライズ言語でカスペルスキー製品を表示します。

［**適用する**］をクリックして、選択したフィルターを適用します。

3. リストから目的のアプリケーションを選択します。
4. ［**配布パッケージの URL**］内のリンクをクリックし、アプリケーションの配布パッケージをダウンロードします。

管理対象の製品のアップデートには、Kaspersky Security Center の特定の最小バージョンをインストールする必要がある場合があります。この最小バージョンが現在のバージョンよりも新しい場合、これらのアップデートは表示されますが、承認はできません。また、Kaspersky Security Center をアップグレードするまでは、このようなアップデートからインストールパッケージを作成することもできません。Kaspersky Security Center インスタンスを必要な最小バージョンにアップグレードするように要求されます。

選択したアプリケーションに対して［**アプリケーションのダウンロードとインストールパッケージの作成**］が表示されている場合、このボタンをクリックすると、アプリケーション配布パッケージをダウンロードしインストールパッケージを自動的に作成することができます。Kaspersky Security Center により、そのインストール時に指定した管理サーバーの共有フォルダーにアプリケーションの配布パッケージがダウンロードされます。自動作成されたインストールパッケージは、コンソールツリーの［**リモートインストール**］フォルダーにある［**インストールパッケージ**］サブフォルダーに表示されます。

［**現在入手可能な製品バージョン**］ウィンドウを閉じた後、［**カスペルスキー製品の新しいバージョンが入手可能です**］は［**製品の導入**］セクションに表示されなくなります。

アプリケーションの新規バージョンのインストールパッケージを作成して、この新しいインストールパッケージをコンソールツリーの［**リモートインストール**］フォルダーの［**インストールパッケージ**］サブフォルダーで管理することができます。

［**現在入手可能な製品バージョン**］ウィンドウは、［**インストールパッケージ**］フォルダーの作業領域で［**カスペルスキー製品の現在のバージョンの表示**］をクリックする方法でも開けます。

リモートインストールのための Windows デバイスの準備

次のような理由によって、クライアントデバイスへのリモートインストールでエラーが返されることがあります：

- タスクが既に同じデバイスで正常に実行されている。
  この場合、タスクを再度実行する必要はありません。

- タスクの開始時点でデバイスが停止していた。

  この場合、デバイスを起動して、タスクを再起動してください。

- 管理サーバーと、クライアントデバイスにインストールされているネットワークエージェントとが接続されていない。

  原因を解明するには、クライアントデバイスのユーティリティ（klactgui）のリモート診断機能を使用してください。

- ネットワークエージェントがデバイスにインストールされていない場合、リモートインストール時に次の問題が生じることがあります：

  - クライアントデバイスで［**簡易ファイルの共有を無効にする**］がオンになっている
  - サーバーのサービスがクライアントデバイスで実行されていない
  - クライアントデバイス上で必要なポートが閉じている
  - タスクの実行に使用されるアカウントに十分な権限がない

  ネットワークエージェントがインストールされていないクライアントデバイスにアプリケーションをインストールする際に発生する可能性のある問題を回避するには、Kaspersky Security Center のリモートインストールタスクによる強制導入の手順に従って実行する必要があります。

以前は、リモートインストール用のデバイスを準備するために riprep ユーティリティを使用していました。これは現在、オペレーティングシステムを構成するための時代遅れの方法であると考えられています。riprep ユーティリティは、Windows XP および Windows Server 2003 R2 より新しいオペレーティングシステムでの使用は推奨されません。

Linux デバイスの準備と Linux デバイスへのネットワークエージェントのリモートインストール

ネットワークエージェントのインストールは、次の 2 つの手順で実行されます：

- Linux デバイスの準備
- ネットワークエージェントのリモートインストール

Linux デバイスの準備

Linux で動作するデバイスにネットワークエージェントをリモートインストールのために準備するには：

1. 対象となる Linux デバイスに次のソフトウェアがインストールされていることを確認します：
   - Sudo
   - Perl 言語インタープリターのバージョン 5.10 以降
2. デバイスの構成をテストします：
   a. デバイスに SSH クライアント（PuTTY など）で接続できることを確認します。

デバイスに接続できない場合、ファイル `/etc/ssh/sshd_config` を開き、次の設定をそれぞれの値に変更します：

```
PasswordAuthentication no
ChallengeResponseAuthentication yes
```

> デバイスに問題なく接続できる場合は、/etc/ssh/sshd_config ファイルを変更しないでください。そうしないと、リモートインストールタスクの実行時に SSH 認証エラーが発生する可能性があります。

必要に応じてファイルを保存し、`sudo service ssh restart` コマンドを使用して SSH サービスを再起動します。

b. デバイスへの接続に使用するユーザーアカウントで sudo パスワードを無効にします。

c. sudo で `visudo` コマンドを使用し、sudoers 構成ファイルを開きます。

開いたファイルで、`%sudo`（CentOS オペレーティングシステムを使用している場合は、`%wheel`）で開始される行を探します。該当の行で、次を指定します：<ユーザー名> `ALL = (ALL) NOPASSWD: ALL`
この場合、< ユーザー名 > は、SSH を経由してデバイスを接続するために使用するユーザーアカウントです。Astra Linux オペレーティングシステムを使用している場合は、ファイル /etc/sudoers の最後の行に次のテキストを追加します：`%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

d. sudoers ファイルを保存して閉じます。

e. SSH を使用して再度デバイスに接続し、sudo サービスがパスワードの入力を要求しないことを確認します。そのためには `sudo whoami` コマンドを使用できます。

3. ファイル `/etc/systemd/logind.conf` を開き、次のいずれかを実行します：

- KillUserProcesses 設定の値として「no」を指定します：`KillUserProcesses=no`
- KillExcludeUsers の設定にリモートインストールを実行するアカウントのユーザー名を入力します。例：`KillExcludeUsers=root`

対象デバイスが Astra Linux を実行している場合は、`export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` 文字列をファイル `/home/<` ユーザー名 `>/.bashrc` に追加します。< ユーザー名 >は、SSH を使用したデバイス接続に使用されるユーザーアカウントです。

変更した設定を適用するには、Linux デバイスを再起動するか、次のコマンドを実行してください：

```
$ sudo systemctl restart systemd-logind.service
```

4. SUSE Linux Enterprise Server 15 オペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントの設定前に、insserv-compat パッケージをインストールします。

5. Astra Linux オペレーティングシステムが閉鎖ソフトウェア環境モードで実行されているデバイスにネットワークエージェントをインストールする場合は、追加の手順を実行して Astra Linux デバイスを準備します。

ネットワークエージェントのリモートインストール

Linux デバイスにネットワークエージェントをリモートインストールするには、次の手順に従います：

1. インストールパッケージをダウンロードして作成します：

   a. パッケージのインストール前に、このパッケージが依存するプログラムやライブラリのすべてがデバイスにインストールされていることを確認してください。

   パッケージの依存関係は、パッケージのインストール先の Linux ディストリビューションに含まれるユーティリティで確認できます。それらのユーティリティについて詳しくは、オペレーティングシステムのマニュアルを参照してください。

   b. アプリケーションインターフェイスを使用するか、カスペルスキー Web サイトからネットワークエージェントインストールパッケージをダウンロードします。

   c. リモートインストールパッケージを作成するには、次のファイルを使用します：

   - klnagent.kpd
   - akinstall.sh
   - ネットワークエージェントの DEB または RPM パッケージ

2. 次の設定でリモートインストールタスクを作成します：

   - 新規タスクウィザードの［**設定**］ページで、［**管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**］をオンにします。それ以外のチェックボックスはすべてオフにします。
   - ［**タスクを実行するアカウントの選択**］ページで、SSH でデバイスに接続するために使用するユーザーアカウントの設定を指定します。

3. リモートインストールタスクを実行します。`su` コマンドのオプションを使用して、環境を保持します: `-m, -p, --preserve-environment`。

ネットワークエージェントをインストールする SUSE Linux Enterprise Server 15 デバイスの準備

SUSE Linux Enterprise Server 15 オペレーティングシステムのデバイスにネットワークエージェントを準備するには:

ネットワークエージェントのインストール前に、次のコマンドを実行します：

```
$ sudo zypper install insserv-compat
```

これにより、insserv-compat パッケージのインストールと、ネットワークエージェントの適切な設定が可能になります。

`rpm -q insserv-compat` コマンドを実行し、パッケージがインストール済みかどうかをチェックします。

多くの SUSE Linux Enterprise Server 15 デバイスがネットワークに存在する場合、会社のインフラストラクチャを設定、管理する専用のソフトウェアを使用できます。このソフトウェアを使用することで、必要なすべてのデバイスに insserv-compat パッケージを一度に自動的にインストールできます。たとえば、Puppet、Ansible、Chef を使用したり、独自のスクリプトを作成したりできます。都合のよい方法を使用してください。

デバイスに SUSE Linux Enterprise の GPG 署名ライセンスがない場合は、次の警告が表示される場合があります：`Package header is not signed!` 警告を無視するには、［`i`］をオンにします。

insserv-compat パッケージのインストールに加えて、Linux デバイスが確実に準備されていることを確認してください。その後、ネットワークエージェントを配信してインストールします。

ネットワークエージェントのリモートインストール用の macOS デバイスの準備

ネットワークエージェントをリモートでインストールする macOS 搭載デバイスを準備するには：

1. 対象となる macOS デバイスに、sudo がインストールされていることを確認します。
2. デバイスの構成をテストします：
   a. クライアントデバイスでポート 22 が開いていることを確認します。これを行うには、［**システム環境設定**］で［**共有**］ペインを開き、［**リモートログイン**］がオンになっていることを確認します。
      SSH 経由でクライアントデバイスに接続できるのはポート 22 を介した場合のみです。ポート番号は変更できません。
      `ssh <デバイス名>` コマンドを使用して macOS デバイスにリモートでログインできます。［**共有**］ペインで、［**アクセスを許可する**］を使用して、macOS デバイスへのアクセスを許可するユーザーの範囲を設定できます。
   b. デバイスへの接続に使用するユーザーアカウントで sudo パスワードを無効にします。
      端末で `sudo visudo` コマンドを使用して sudoers 設定ファイルを開きます。開いたファイルの `User privilege specification` エントリで、次のように指定します。`username ALL = (ALL) NOPASSWD: ALL`。この場合、`username` は SSH を経由してデバイスを接続するために使用するユーザーアカウントを表します。
   c. sudoers ファイルを保存して閉じます。
   d. SSH を使用して再度デバイスに接続し、sudo サービスがパスワードの入力を要求しないことを確認します。そのためには `sudo whoami` コマンドを使用できます。
3. インストールパッケージをダウンロードして作成します：
   a. 次のいずれかの方法で、ネットワークエージェントのインストールパッケージをダウンロードします：
      - コンソールツリーで、［**リモートインストール**］→［**インストールパッケージ**］の順に選択してコンテキストメニューを開き、［**現在入手可能な製品バージョンを表示**］を選択し、使用可能なパッケージから選択する
      - https://support.kaspersky.co.jp/ のテクニカルサポートサイトから関連バージョンのネットワークエージェントをダウンロードする
      - テクニカルサポート担当者にインストールパッケージをリクエストする
   b. リモートインストールパッケージを作成するには、次のファイルを使用します：
      - klnagent.kud
      - install.sh

- klnagentmac.dmg

4. 次の設定でリモートインストールタスクを作成します：

- 新規タスクウィザードの［**設定**］ページで、［**管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**］をオンにします。それ以外のチェックボックスはすべてオフにします。

- ［**タスクを実行するアカウントの選択**］ページで、SSH を使用したデバイス接続に使用するユーザーアカウントの設定を指定します。

作成したタスクを使用したネットワークエージェントのリモートインストールに対して、クライアントデバイスの準備ができています。

カスペルスキー製品：ライセンスとアクティベーション

このセクションでは、管理対象のカスペルスキー製品のライセンスを Kaspersky Security Center で操作する方法について説明します。

Kaspersky Security Center では、クライアントデバイスにカスペルスキー製品のライセンスを一元的に配信し、使用状況の監視およびライセンスの更新を実行できます。

Kaspersky Security Center でライセンスを追加すると、ライセンスの設定が管理サーバーで保存されます。アプリケーションでは、この情報に基づいて、ライセンス使用レポートを生成し、ライセンスの有効期限と、ライセンスのプロパティで設定されるライセンスの制限事項の違反について管理者に通知します。ライセンス使用の通知の設定は管理サーバーで設定できます。

管理対象アプリケーションのライセンスの管理

管理対象デバイスにインストールされているカスペルスキー製品には、各製品のライセンス情報ファイルまたはアクティベーションコードを適用してライセンスを付与する必要があります。ライセンス情報ファイルとアクティベーションコードは次の方法で展開できます：

- 自動配信
- 管理対象アプリケーションのインストールパッケージ
- 管理対象アプリケーションへの *ライセンスの追加*タスク
- 管理対象アプリケーションの手動アクティベーション

上記のいずれかの方法で、新しい現在のライセンスまたは予備のライセンスを追加できます。カスペルスキー製品は、現時点で現在のライセンスを使用し、現在のライセンスの有効期限が切れた後に適用する予備のライセンスを保存します。ライセンスを追加するアプリケーションは、ライセンスが現在のライセンスか予備のライセンスかを定義します。ライセンスの定義は、新しいライセンスの追加方法には依存しません。

自動配信

異なる複数の管理対象アプリケーションを使用し、特定のライセンス情報ファイルまたはアクティベーションコードをデバイスに配信する必要がある場合は、他の配信方法を選択してください。

Kaspersky Security Center を使用して、使用可能なライセンスをデバイスに配信できます。ここでは、3 個のライセンスが管理サーバーのリポジトリに保管されている場合を例にします。［**管理対象デバイスにライセンスを自動的に配信する**］を 3 個のライセンスすべてに対してオンにしていると仮定します。カスペルスキーのセキュリティ製品（例：Kaspersky Endpoint Security for Windows）が、組織内のデバイスにインストールされているとします。ライセンスを配信する必要がある新しいデバイスが検出されます。リポジトリ内に保管されている、名前がそれぞれ「*Key_1*」「*Key_2*」である 2 個のライセンス情報ファイルが、そのデバイスに配信可能であると本製品が判断します。そのうち 1 個のライセンス情報ファイルが、デバイスに配信されます。この場合、どのライセンス情報ファイルがデバイスに適用されるかは予測ができません。自動配信されるライセンスに対して、管理者が設定可能な項目がないからです。

ライセンスが配信されると、そのライセンスを適用中のデバイスの台数が再度計上されます。ライセンスが適用可能な台数を超えないように、適用中のデバイスの台数を確認しておく必要があります。ライセンスを適用可能な台数の上限を超えると、ライセンスが適用されていないデバイスのステータスが「*緊急*」になります。

配信前に、管理サーバーのリポジトリにライセンス情報ファイルまたはアクティベーションコードを追加する必要があります。

実行手順の説明：

- 管理コンソール：
  - ライセンスの管理サーバーリポジトリへの追加
  - ライセンスの自動配信

  または
- Kaspersky Security Center Web コンソール：
  - ライセンスの管理サーバーリポジトリへの追加
  - ライセンスの自動配信

次の場合、自動的に配布されたライセンスが仮想管理サーバーのリポジトリに表示されない場合があることに注意してください：

- ライセンスがアプリケーションに対して有効ではありません。
- 仮想管理サーバーには管理対象デバイスがありません。
- ライセンスは別の仮想管理サーバーによって管理されているデバイスに既に使用されており、デバイス数の制限に達しています。

ライセンス情報ファイルまたはアクティベーションコードを管理対象アプリケーションのインストールパッケージに追加

セキュリティ上の理由から、このオプションの使用は推奨されません。インストールパッケージに追加したライセンス情報ファイルまたはアクティベーションコードは、漏洩などの危険にさらされる可能性があります。

インストールパッケージを使用して管理対象アプリケーションをインストールする場合、パッケージ内またはアプリケーションのポリシー内に含まれるアクティベーションコードまたはライセンス情報ファイルを指定できます。ライセンスが管理対象デバイスに配信されるのは、デバイスと管理サーバーの次回の同期時です。

実行手順の説明：

- 管理コンソール：
  - インストールパッケージの作成
  - クライアントデバイスへのアプリケーションのインストール

  または
- Kaspersky Security Center Web コンソール：インストールパッケージへのライセンスの追加

管理対象アプリケーションへのライセンスの追加タスクを使用して配信

管理対象アプリケーションへの*ライセンスの追加*タスクを使用する場合、配信する必要があるライセンスを選択後、対象デバイスを都合のよい方法で選択できます。たとえば、管理グループを選択したり、デバイスの抽出を使用したりすることが可能です。

配信前に、管理サーバーのリポジトリにライセンス情報ファイルまたはアクティベーションコードを追加する必要があります。

実行手順の説明：

- 管理コンソール：
  - ライセンスの管理サーバーリポジトリへの追加
  - ライセンスのクライアントデバイスへの配信

  または
- Kaspersky Security Center Web コンソール：
  - ライセンスの管理サーバーリポジトリへの追加
  - ライセンスのクライアントデバイスへの配信

アクティベーションコードまたはライセンス情報ファイルを手動でデバイスに追加

インストール済みのカスペルスキー製品を、製品インターフェイス内のツールを使用してローカルでアクティベーションできます。詳しくは、インストールされているアプリケーションのヘルプを参照してください。

使用中のライセンスに関する情報の表示

使用中のライセンスについての情報を表示するには：

コンソールツリーで、［**カスペルスキーのライセンス**］フォルダーを選択します。

フォルダーの作業領域に、クライアントデバイスで使用中のライセンスのリストが表示されます。

ライセンスの隣に使用状況を示すアイコンが表示されます：

-  —現在使用しているライセンスについての情報は、管理サーバーに接続しているクライアントデバイスから取得されます。このライセンスのファイルは管理サーバー外に保存されています。
-  —ライセンスは管理サーバーのリポジトリに保存されます。このライセンスの自動配信が無効になっています。
-  —ライセンスは管理サーバーのリポジトリに保存されます。このライセンスの自動配信が有効になっています。

クライアントデバイスのプロパティウィンドウの［**アプリケーション**］セクションを表示すると、クライアントデバイス上の製品のアクティベーションで使用されているライセンスについての情報を表示できます。

仮想管理サーバーのライセンスの最新の設定を定義するため、管理サーバーはカスペルスキーのアクティベーションサーバーに少なくとも毎日1度はリクエストを送信します。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。

ライセンスをクライアントデバイスから受信した場合、それをファイルとしてエクスポートすることはできません。

ライセンスの管理サーバーリポジトリへの追加

ライセンスを管理サーバーリポジトリに追加するには：

1. コンソールツリーで、［**カスペルスキーのライセンス**］フォルダーを選択します。
2. 次のいずれかの方法で、ライセンスの追加タスクを開始します：
   - ライセンスのコンテキストメニューで、［**アクティベーションコードまたはライセンス情報ファイルの追加**］を選択します。
   - ライセンスリストの作業領域で、［**アクティベーションコードまたはライセンス情報ファイルの追加**］をクリックします。
   - ［**アクティベーションコードまたはライセンス情報ファイルの追加**］をクリックします。

   ライセンス追加ウィザードが起動します。
3. 管理サーバーをアクティベートする方法を選択します：アクティベーションコードを使用するか、ライセンス情報ファイルを使用します。
4. アクティベーションコードまたはライセンス情報ファイルを指定します。
5. ネットワーク上で関連するライセンスをすぐに配信する場合は［**管理対象デバイスにライセンスを自動的に配信する**］を選択します。このオプションを選択しない場合は、後から手動でライセンスを配信することができます。

結果、ライセンス情報ファイルがダウンロードされ、［ライセンス追加ウィザード］が完了します。追加されたライセンスがカスペルスキーのライセンスのリストに表示されるようになりました。

管理サーバーのライセンスの削除

管理サーバーのライセンスを削除するには：

1. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
2. 開いた［管理サーバーのプロパティ］ウィンドウで、［**ライセンス**］セクションを選択します。
3. ［**削除**］をクリックして、ライセンスを削除します。

   これにより、ライセンスが削除されます。

予備のライセンスが追加されている場合、予備のライセンスは、前の現在のライセンスが削除された後、自動的に現在のライセンスになります。

管理サーバーの現在のライセンスが削除された後、［脆弱性とパッチ管理］および［モバイルデバイス管理］は使用できなくなります。削除されたライセンスの再追加や、新しいライセンスの追加も可能です。

ライセンスのクライアントデバイスへの配信

Kaspersky Security Center では、［*ライセンス配信*］タスクによってクライアントデバイスにライセンスを配信できます。

配信前に、ライセンスを管理サーバーリポジトリに追加します。

クライアントデバイスにライセンスを配信するには：

1. コンソールツリーで、［**カスペルスキーのライセンス**］フォルダーを選択します。
2. 作業領域のライセンスのリストで［**管理対象デバイスにライセンスを自動配信する**］をクリックします。

   ［**アプリケーションのアクティベーションタスク作成ウィザード**］が起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. アプリケーションのリストで、タスクを作成するアプリケーションを選択します。
4. ウィザードの**ライセンスの追加**ステップで、次のオプションのいずれかを使用してライセンスを追加します：

   - Kaspersky Security Center リポジトリから［**アクティベーションコード**］を選択し、アクティベーションコードを追加します。

     ［**選択**］をクリックします。ウィンドウが開いたら、アクティベーションコードを選択し、［**OK**］をクリックします。
   - ［**ライセンス情報ファイルまたはライセンス**］を選択し、次の操作を行います：

     a. ［**選択**］をクリックします。

     b. コンテキストメニューで、次のいずれかのオプションを選択します。

- ［**フォルダー上のライセンス情報ファイル**］。

  開いたウィンドウで、デバイスからライセンス情報ファイルを選択し、［**開く**］をクリックします。

- ［**Kaspersky Security Center のリポジトリのライセンス情報ファイル**］

  開いたウィンドウで、Kaspersky Security Center リポジトリからライセンスを選択し、［**OK**］をクリックします。

5. 現在のライセンスを置き換える場合は、既定の［**Use as a reserve key**］をオフにします。

   たとえば、組織が変更され、デバイスで別の組織のライセンスが必要な場合や、ライセンスが再発行され、新しいライセンスの有効期限が現在のライセンスよりも早く切れる場合に、これが必要になります。エラーを回避するには、［**Use as a reserve key**］をオフにする必要があります。

   Kaspersky Security Center Windows にライセンスを追加する際に発生する可能性のある問題とその解決方法の詳細については、Kaspersky Security Center ナレッジベースを参照してください。

6. ライセンス情報を確認し、［**次へ**］をクリックします。

7. ウィザードのこのステップでは、ライセンスの追加タスクを割り当てるデバイスを選択します。以下のいずれかの方法でデバイス（最大 1000 台）を指定できます：

   - **ネットワークの管理サーバーによって検出されたデバイスを選択する**：この場合、タスクを特定のデバイスに割り当てます。特定のデバイスには、管理グループに属するデバイスと管理グループが割り当てられていないデバイスの両方を含めることができます。

   - ［**デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**］。タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

   - **デバイスの抽出にタスクを割り当てる**：この場合、既に作成された抽出に属するデバイスにタスクを割り当てます。事前定義の抽出または作成済みのカスタム抽出を指定できます。

   - **管理グループにタスクを割り当てる**：この場合、既に作成された管理グループに属するデバイスにタスクを割り当てます。

8. ウィザードの［**タスクスケジュールの設定**］ステップで、タスク開始のスケジュールを作成します：

   - **実行予定**：

     - **1回**

       タスクは、指定された日時に1回実行されます（既定では、タスクが作成された日）。

     - **手動**

       タスクは、自動的には実行されません。手動でのみ開始できます。

       既定では、このオプションがオンです。

     - **新しいアップデートがリポジトリにダウンロードされ次第**

       アップデートのリポジトリへのダウンロードが完了すると、タスクが実行されます。たとえば、脆弱性とアプリケーションのアップデートの検索タスクのスケジュールを設定する時に、このオプションを使用すると便利です。

- **ウイルスアウトブレイク検知次第**

  ［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

  - ワークステーションとファイルサーバー向けアンチウイルス製品
  - 境界防御向けアンチウイルス製品
  - メールサーバー向けアンチウイルス製品

  既定では、すべてのアプリケーション種別がオンです。

  ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

  他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

  テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

  必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

  - タスク名で検索するには、検索フィールドにタスク名を入力します。
  - 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。

    既定では、タスクはアルファベットの昇順で並べ替えられます。
  - フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

  このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

  このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

  このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

  既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる(分)**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  既定では、このオプションはオフです。既定の時間は1分です。

9. ウィザードの［**タスク名の定義**］ステップで、タスクの名前を指定します。タスク名は100文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

10. ［**タスク作成の終了**］ステップで、［**終了**］をクリックしてウィザードを終了します。

    ウィザード終了後にすぐにタスクを開始するには、［**ウィザードの終了後にタスクを実行**］をオンにします。

［**アプリケーションのアクティベーションタスク作成ウィザード**］で作成したタスクは、特定のデバイスに対するタスクであり、コンソールツリーの［**タスク**］フォルダーに保存されます。

管理グループまたはクライアントデバイスに対するタスク作成ウィザードでグループまたはローカルのライセンス配信タスクを作成することもできます。

ライセンスの自動配信

Kaspersky Security Centerでは、管理サーバーのライセンスリポジトリにあるライセンスを管理対象デバイスに自動配信できます。ライセンスの自動配信は、［**未割り当てデバイス**］フォルダー内のデバイスには適用されません。

管理対象デバイスにライセンスを自動配信するには：

1. コンソールツリーで、［**カスペルスキーのライセンス**］フォルダーを選択します。

2. フォルダーの作業領域で、デバイスに自動配信するライセンスを選択します。

3. 次のいずれかの方法で、選択したライセンスのプロパティウィンドウを開きます：

   - ライセンスのコンテキストメニューの［**プロパティ**］を選択します。

   - 選択したライセンスの情報ボックスで、［**ライセンスのプロパティの表示**］をクリックします。

4. 表示されるライセンスのプロパティウィンドウで［**自動配信されるライセンス**］をオンにします。ライセンスのプロパティウィンドウを閉じます。

ライセンスは、互換性のあるすべてのデバイスに自動的に配信されます。

ライセンスはネットワークエージェント経由で配信されます。アプリケーションに対するライセンスの配信タスクは作成されません。

ライセンスを自動で配信している最中に、ライセンスのデバイス台数上限が考慮されます（ライセンス単位は、ライセンスのプロパティで設定されます）。ライセンスの上限に達した場合、デバイスへのライセンス配信が自動的に停止されます。

仮想管理サーバーは、そのリポジトリと管理サーバーのリポジトリからライセンスを自動的に配布します。以下を推奨します。

- *ライセンスの追加*タスクを使用して、デバイスに導入する必要があるライセンスを選択します。
- 仮想管理サーバーの設定で、［**この仮想管理サーバーからデバイスへのライセンスの自動配信を許可する**］をオフにしないでください。オフにした場合、仮想管理サーバーは、管理サーバーリポジトリからのライセンスを含め、ライセンスをデバイスに配布しません。

ライセンスのプロパティウィンドウで［**自動配信されるライセンス**］がオンになっている場合、ライセンスはネットワークにすぐに配布されます。このオプションを選択しない場合は、後から手動でライセンスを配信することができます。

ライセンス使用レポートの作成と表示

クライアントデバイスのライセンス使用レポートを作成するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**レポート**］タブを選択します。
3. ［**ライセンス使用レポート**］テンプレートを選択するか、同じ種別の新規レポートテンプレートを作成します。

ライセンス使用レポートの作業領域にクライアントデバイスの現在のライセンスと予備のライセンスに関するレポートが表示されます。レポートには、ライセンスを使用しているデバイスに関する情報と、ライセンスのプロパティで指定されている制限に関する情報も表示されます。

製品のライセンスに関する情報の表示

カスペルスキー製品で使用されているライセンスを確認するには：

1. Kaspersky Security Center のコンソールツリーで、［**管理対象デバイス**］フォルダーを選択して、［**デバイス**］タブに移動します。
2. 目的のデバイスを右クリックしてコンテキストメニューを開いて、［**プロパティ**］を選択します。
3. デバイスのプロパティウィンドウが開いたら、［**アプリケーション**］セクションを選択します。

4. アプリケーションのリストが表示されたら、ライセンスを表示するアプリケーションを選択して、［**プロパティ**］をクリックします。

5. アプリケーションのプロパティウィンドウが開いたら、［**ライセンス**］セクションを選択します。

   このセクションの作業領域に情報が表示されます。

ライセンス情報ファイルのエクスポート

ライセンスを誤って削除し、復元したい場合は、他の管理サーバーからライセンス情報ファイルをエクスポートできます。

ライセンス情報ファイルをエクスポートするには、［**ライセンス情報ファイルのエクスポート：ライセンス管理**］機能領域で［**一般的な機能**］権限が付与されている必要があります。

ライセンスをクライアントデバイスから受信した場合、それをエクスポートすることはできません。

ライセンスをエクスポートするには：

1. コンソールツリーで、［**カスペルスキーのライセンス**］フォルダーを選択します。

2. リストから、ファイルとしてエクスポートするライセンスを選択します。

3. 開いた情報ボックスで、［**ライセンス情報ファイルのエクスポート**］をクリックします。

4. 開いたウィンドウで、ライセンス情報ファイルを保存するフォルダーのパスを指定し、ファイル名を指定します。その後、［**保存**］をクリックします。

   ライセンス情報ファイルは選択したフォルダーにエクスポートされます。

ネットワーク保護の設定

このセクションには、ポリシーとタスクの手動設定、ユーザーロール、管理グループの構造とタスクの階層構造の構築に関する情報を記載しています。

シナリオ：ネットワーク保護の設定

クイックスタートウィザードにより、既定の設定でポリシーとタスクが作成されます。これらの設定は、組織のルールなどに照らして最適でない、または許容できない内容を含む可能性があります。したがって、ネットワークの必要性に応じて、これらのポリシーとタスクを調整し、他のポリシーとタスクを作成してください。

必須条件

導入を開始する前に、次が完了していることを確認してください：

- Kaspersky Security Center 管理サーバーをインストール済み
- Kaspersky Security Center Web コンソールをインストール済み（任意）
- Kaspersky Security Center の主要なインストールシナリオを完了済み
- クイックスタートウィザードを完了済みまたは［**管理対象デバイス**］管理グループで以下のポリシーとタスクを手動で作成済み：
  - Kaspersky Endpoint Security のポリシー
  - Kaspersky Endpoint Security をアップデートするグループタスク
  - ネットワークエージェントのポリシー
  - *脆弱性とアプリケーションのアップデートの検索*タスク

ネットワーク保護の設定は、次の手順で進みます：

1. **カスペルスキー製品のポリシーとポリシーのプロファイルの設定と各デバイスへの反映**

   管理対象デバイスにインストールされているカスペルスキー製品のポリシーとポリシーのプロファイルを設定しデバイスに反映するには、デバイスベースとユーザーベースの 2 種類のセキュリティ管理方法を使用できます。これらの 2 つの管理方法を組み合わせることもできます。デバイスベースのセキュリティ管理を実施するには、MMC ベースの管理コンソールまたは Kaspersky Security Center Web コンソールで提供されているツールを使用できます。ユーザーベースのセキュリティ管理は、Kaspersky Security Center Web コンソールでのみ実施できます。

2. **カスペルスキー製品のリモート管理用のタスクの設定**

   必要に応じて、クイックスタートウィザードを使用して作成したタスクを確認、調整します。

   実行手順の説明：

   - 管理コンソール：
     - Kaspersky Endpoint Security をアップデートするグループタスクの設定
     - 脆弱性とアプリケーションのアップデートの検索タスクのスケジュール設定
   - Kaspersky Security Center Web コンソール：
     - Kaspersky Endpoint Security をアップデートするグループタスクの設定
     - 脆弱性とアプリケーションのアップデートの検索タスクの設定

   必要に応じて、クライアントデバイスにインストールされているカスペルスキー製品を管理するためのタスクを追加で作成します。

3. **データベースでのイベント情報による負荷の評価と制限**

   管理対象アプリケーションの動作中のイベントに関する情報は、クライアントデバイスから送信され、管理サーバーデータベースに記録されます。管理サーバーの負荷を軽減するには、データベースに保管される可能性のあるイベント数の最大値を評価し、上限を設定します。

   実行手順の説明：

   - 管理コンソール：イベント数の上限の設定
   - Kaspersky Security Center Web コンソール：イベント数の上限の設定

結果

この手順を完了すると、カスペルスキー製品、タスク、管理サーバーで取得されるイベントの設定によってネットワークの保護が機能するようになります。

- ポリシーとポリシーのプロファイルに従ってカスペルスキー製品が設定されます。
- 製品が一連のタスクによって管理されるようになります。
- データベースに保存されるイベント数の上限が設定されます。

ネットワーク保護の設定が完了すると、定義データベースとカスペルスキー製品の定期アップデートの設定ステップに進むことができます。

Kaspersky Sandbox により検知された脅威への自動応答を設定する方法の詳細は、Kaspersky Sandbox 2.0 のオンラインヘルプを参照してください。

ポリシーの設定と継承先への反映：デバイスベースの管理

この手順を完了すると、すべての管理対象デバイスにインストールされている製品が、定義した製品ポリシーとポリシープロファイルに従って設定されます。

必須条件

手順を開始する前に、Kaspersky Security Center 管理サーバーと Kaspersky Security Center Web コンソール（任意）のインストールが完了していることを確認してください。Kaspersky Security Center Web コンソールをインストールしている場合、デバイスベースの管理方法の代替案もしくは追加で組み合わせて使用する管理方法としてユーザーベースのセキュリティ管理も検討すると有益な場合があります。

実行するステップ

カスペルスキー製品のデバイスベースの管理シナリオは、次の 2 つの手順からなります。

1. **製品ポリシーの設定**

   管理対象デバイスにインストールされているカスペルスキー製品ごとにポリシーを作成して、製品の設定を指定します。これらのポリシーはクライアントデバイスに反映されます。

   クイックスタートウィザードを使用してネットワークの保護を設定する場合、Kaspersky Security Center は次のアプリケーションの既定のポリシーを作成します：

   - Kaspersky Endpoint Security for Windows - Windows ベースのクライアントデバイス用
   - Kaspersky Endpoint Security for Linux - Linux ベースのクライアントデバイス用

   このウィザードを使用して設定プロセスを完了した場合、この製品の新しいポリシーを作成する必要はありません。Kaspersky Endpoint Security ポリシーの手動セットアップに進みます。

複数の管理サーバーと管理グループからなる階層構造が存在する場合、既定では、セカンダリ管理サーバーと子管理グループはプライマリ管理サーバーのポリシーを継承します。子グループとセカンダリ管理サーバーでの継承を強制的に適用して、上位のポリシーで指定された設定の変更を禁止することもできます。一部の設定のみを強制的に継承させたい場合は、上位のポリシーで該当する設定項目をロックできます。残りのロックされていない設定は下位のポリシーで変更できます。ポリシーの階層を作成することで、管理グループ内の管理対象デバイスを効果的に管理できます。

実行手順の説明：

- 管理コンソール：ポリシーの作成
- Kaspersky Security Center Web コンソール：ポリシーの作成

2. **ポリシーのプロファイルの作成（任意）**

同じ管理グループ内にあるデバイスを異なるポリシー設定に従って動作させる場合には、ポリシーのプロファイルを作成します。ポリシーのプロファイルには、ポリシー設定のサブセットが指定されています。このサブセットはポリシーとともに対象デバイスに配信され、*プロファイルの有効化条件*と呼ばれる特定の条件下でポリシーを補完する機能を果たします。プロファイルに含まれるのは、管理対象デバイスでアクティブな「基本」ポリシーとは異なる設定（差分）のみです。

プロファイルの有効化条件を使用することで、たとえば、Active Directory の特定の組織単位やセキュリティグループに属するデバイス、特定のハードウェア設定のデバイス、特定のタグが付与されているデバイスなどの条件に応じて異なるポリシープロファイルを適用できます。タグを使用すると特定の基準を満たすデバイスをフィルタリングできます。たとえば、「*Windows*」というタグを作成し、Windows オペレーティングシステムを実行しているデバイスすべてにこのタグを付与し、ポリシープロファイルの有効化条件としてこのタグを指定します。これにより、Windows を実行しているすべてのデバイスにインストールされているカスペルスキー製品は該当するポリシープロファイルで管理されます。

実行手順の説明：

- 管理コンソール：
  - ポリシーのプロファイルの作成
  - ポリシーのプロファイルの有効化ルールの作成
- Kaspersky Security Center Web コンソール：
  - ポリシーのプロファイルの作成
  - ポリシーのプロファイルの有効化ルールの作成

3. **ポリシーとポリシープロファイルの管理対象デバイスへの反映**

既定では、管理サーバーは 15 分ごとに管理対象デバイスと自動的に同期します。自動同期を回避して、［強制同期］コマンドを使用して手動で同期を実行できます。また、ポリシーまたはポリシープロファイルを作成または変更すると、同期が強制的に行われます。同期中に、新しいまたは変更されたポリシーとポリシープロファイルが管理対象デバイスに反映されます。

Kaspersky Security Center Web コンソールを使用する場合、ポリシーとポリシーのプロファイルがデバイスに配信されたかを確認できます。Kaspersky Security Center では、デバイスのプロパティで該当する配信日時が表示されます。

実行手順の説明：

- 管理コンソール：強制同期
- Kaspersky Security Center Web コンソール：強制同期

実行結果

デバイスベースの管理の導入手順が完了すると、ポリシーの階層を通して指定または反映された設定がカスペルスキー製品に適用されます。

管理グループに新しく追加されたデバイスには、設定された製品ポリシーとポリシープロファイルが自動的に適用されます。

デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理の概要

セキュリティ設定を、デバイスの仕様の観点やユーザーロールの観点から管理できます。1つ目のアプローチは*デバイスベースのセキュリティ管理*、2つ目のアプローチは*ユーザーベースのセキュリティ管理*と呼ばれます。異なるデバイスに異なる設定を適用するには、いずれかの管理方法あるいは両者を組み合わせた管理方法を使用できます。デバイスベースのセキュリティ管理を実施するには、MMC ベースの管理コンソールまたは Kaspersky Security Center Web コンソールで提供されているツールを使用できます。ユーザーベースのセキュリティ管理は、Kaspersky Security Center Web コンソールでのみ実施できます。

デバイスベースのセキュリティ管理では、デバイスごとの状況などに合わせて、セキュリティ製品について複数の異なる設定を管理対象デバイスに適用できます。たとえば、異なる管理グループに属するデバイスに、異なる設定を適用できます。あるいは、Active Directory でデバイスに割り当てられている用途や、ハードウェアの仕様などに応じて、デバイスを区分することもできます。

ユーザーベースのセキュリティ管理を使用すると、ユーザーロールに応じて、異なるセキュリティ設定を適用できます。複数のユーザーロールを作成し、ユーザーごとに適切なユーザーロールを割り当てた上で、デバイスの所有者のユーザーロールに応じて、異なるセキュリティ設定をデバイスに適用できます。たとえば、経理部門の従業員と人事部門の従業員それぞれのデバイスに異なるアプリケーション設定を適用する場合などがありえます。これにより、ユーザーベースのセキュリティ管理を実施すると、経理部門の従業員と人事部門の従業員のカスペルスキー製品に対して、それぞれ独自の設定が適用されます。詳細設定により、製品設定のどの部分をユーザー側で設定でき、どの部分は管理者による設定が強制的に適用されるかを指定できます。

ユーザーベースのセキュリティ管理を使用すると、特定の1人のユーザーに特定の製品設定を適用できます。該当する従業員が社内で固有のロールを担っていたり、特定のユーザーのデバイスに関連したセキュリティ問題を監視したい場合などに、こうした処理が必要になることがあります。社内でのこの従業員のロールに基づいて、ユーザーが製品設定を変更できる権限を拡張したり制限できます。たとえば、ローカルオフィスのクライアントデバイスを管理しているシステム管理者の権限を拡張する場合などです。

デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理を組み合わせることもできます。たとえば、管理グループごとに製品ポリシーを設定した上で、企業内の1つ以上のユーザーロールを対象としたポリシープロファイルを作成するなどの方法を使用できます。この場合、ポリシーとポリシープロファイルは次の順序で適用されます。

1. デバイスベースのセキュリティ管理用に作成されたポリシーが適用されます。
2. ポリシーは、ポリシープロファイルの優先度に応じてポリシープロファイルで変更されます。
3. ポリシーは、ユーザーロールと関連付けられたポリシープロファイルで変更されます。

Kaspersky Endpoint Security ポリシーの手動セットアップ

このセクションでは、クイックスタートウィザードで作成される、Kaspersky Endpoint Security ポリシーの設定方法に関する推奨事項を説明します。ポリシーのプロパティウィンドウで設定を実行できます。

設定を編集する際には、ワークステーションでその値を使用できるように、関連する設定の上にあるロックアイコンをクリックする必要があることに注意してください。

［先進の脅威対策］セクションでのポリシーの設定

このセクションに記載されている設定の詳細な説明は、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

［**先進の脅威対策**］セクションで、Kaspersky Endpoint Security for Windows の Kaspersky Security Network の使用を設定できます。ふるまい検知、脆弱性攻撃ブロック、ホスト侵入防止、修復エンジンなどの Kaspersky Endpoint Security for Windows モジュールを設定することもできます。

［**Kaspersky Security Network**］サブセクションで、［**KSN プロキシを使用する**］を有効にすることを推奨します。このオプションを使用することで、ネットワーク上でトラフィックを再分配し、最適化できます。［**KSN プロキシを使用する**］がオフになっている場合は、KSN サーバーの直接使用を有効にできます。

［脅威対策］セクションでのポリシーの設定

このセクションに記載されている設定の詳細な説明については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

ポリシープロパティウィンドウの［**脅威対策**］セクションで、［**ファイアウォール**］および［**ファイル脅威対策**］のサブセクションに追加の設定を指定することを推奨します。

［**ファイアウォール**］サブセクションには、クライアントデバイス上のアプリケーションのネットワークアクティビティを制御できる設定が含まれています。クライアントデバイスは、パブリック、ローカル、信頼済みのいずれかのステータスが割り当てられているネットワークを使用します。ネットワークステータスに応じて、Kaspersky Endpoint Security はデバイスでのネットワークアクティビティを許可または拒否できます。組織に新しいネットワークを追加する時は、適切なネットワークステータスを割り当てる必要があります。たとえば、クライアントデバイスがノート PC の場合、ノート PC は常にローカルネットワークに接続されているとは限らないため、このデバイスではパブリックネットワークまたは信頼できるネットワークを使用することを推奨します。［**ファイアウォール**］サブセクションで、組織で使用するネットワークにステータスを正しく割り当てたことを確認できます。

ネットワークのリストを確認するには：

1. ポリシーのプロパティで、［**脅威対策**］→［**ファイアウォール**］の順に選択します。
2. ［**使用可能なネットワーク**］セクションで、［**設定**］をクリックします。
3. 表示される［**ファイアウォール**］ウィンドウで、［**ネットワーク**］タブに移動してネットワークのリストを表示します。

［**ファイル脅威対策**］サブセクションで、ネットワークドライブのスキャンを無効にできます。ネットワークドライブのスキャンを行うと、ネットワークドライブに大幅な負荷がかかることがあります。ファイルサーバーで間接スキャンを実行するのが有効です。

ネットワークドライブのスキャンを無効にするには：

1. ポリシーのプロパティで、［**脅威対策**］→［**ファイル脅威対策**］の順に選択します。
2. ［**セキュリティレベル**］セクションで、［**設定**］をクリックします。
3. ［**ファイル脅威対策**］ウィンドウが開いたら、［**全般**］タブで［**すべてのネットワークドライブ**］をオフにします。

［全般設定］セクションでのポリシーの設定

このセクションに記載されている設定の詳細な説明については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

ポリシープロパティウィンドウの［**全般設定**］セクションで、［**レポートと保管領域**］および［**インターフェイス**］サブセクションに追加の設定を指定することを推奨します。

［**レポートと保管領域**］サブセクションで、［**管理サーバーへのデータ転送**］セクションに移動します。［**起動されたアプリケーションの情報**］は、管理サーバー定義データベースに、ネットワーク接続されたデバイス上にあるすべてのバージョンのソフトウェアモジュールに関する情報を保存するかどうかを指定します。このチェックボックスをオンにすると、保存された情報は、Kaspersky Security Center データベース内に大量のディスク容量を必要とする場合があります（数十ギガバイト）。トップレベルのポリシーで［**起動されたアプリケーションの情報**］がオンになっている場合は、オフにします。

管理コンソールが、組織のネットワーク上の脅威対策による保護を集中管理する場合は、ワークステーションでの Kaspersky Endpoint Security for Windows ユーザーインターフェイスの表示を無効にします。これを行うには、［**インターフェイス**］サブセクションで、［**ユーザー**とのやり取り］セクションに移動し、［**表示しない**］オプションを選択します。

ワークステーションでパスワード保護を有効にするには、［**インターフェイス**］サブセクションで［**パスワード保護**］セクションに移動し、［**設定**］ボタンをクリックした後、［**パスワードによる保護を有効にする**］をオンにします。

［イベントの設定］セクションでのポリシーの設定

［**イベントの設定**］セクションで、管理サーバーに関する次の項目以外のすべてのイベントを保存しないように設定する必要があります：

- ［**緊急イベント**］タブ：
  - コンピューター起動時の自動起動が無効です
  - アクセスが拒否されました
  - アプリケーションの起動が禁止されました
  - 駆除できません
  - ライセンス違反です
  - 暗号化モジュールを読み込めません

- 2 つのタスクを同時に開始できません
- アクティブな脅威が検知されました。特別な駆除を開始してください
- ネットワーク攻撃が検知されました
- アップデートされていないコンポーネントがあります
- アクティベーションエラー
- ポータブルモードの有効化中にエラーが発生しました
- Kaspersky Security Center との対話中にエラーが発生しました
- ポータブルモードの無効化中にエラーが発生しました
- アプリケーション機能の変更中にエラーが発生しました
- ファイル暗号化 / 復号化ルールの適用中にエラーが発生しました
- ポリシーを適用できません
- プロセスが終了しました
- ネットワーク動作がブロックされました

- ［**機能エラー**］タブ：タスク設定が無効です。設定は適用されません
- ［**警告**］タブ：
  - セルフディフェンスが無効です
  - 予備のライセンスが正しくありません
  - ユーザーが暗号化ポリシーを拒否しました
- ［**情報**］タブ：アプリケーションの起動がテストモードでブロックされています

Kaspersky Endpoint Security のグループアップデートタスクの手動セットアップ

Kaspersky Endpoint Security バージョン 10 以降の最適かつ推奨されるスケジュールオプションは、［**タスクの開始を自動的かつランダムに遅延させる**］をオンにした上で、［**新しいアップデートがリポジトリにダウンロードされ次第**］を使用することです。

Kaspersky Endpoint Security がインストールされたデバイスのスキャン用グループタスクの手動セットアップ

クイックスタートウィザードにより、デバイススキャン用のグループタスクが作成されます。既定では、このタスクは**金曜日の午後 7 時に実行**するよう設定されており、［**未実行のタスクを実行する**］がオフになっています。

つまり、組織内のデバイスが、たとえば、金曜日の午後 6 時 30 分にシャットダウンされる場合、そのデバイスのスキャンタスクは一切実行されません。組織で採用されている職場のルールに基づいて、このタスクに対する最も効率的なスケジュールをセットアップする必要があります。

脆弱性とアプリケーションのアップデートの検索タスクのスケジュール設定

クイックスタートウィザードにより、ネットワークエージェントでの*脆弱性とアプリケーションのアップデートの検索*タスクが作成されます。既定では、このタスクは**火曜日の午後 7 時に実行**するよう設定されており、［**未実行のタスクを実行する**］がオンになっています。

組織で採用されている職場のルールによりこの時刻にすべてのデバイスをシャットダウンするように定められている場合は、デバイスが再度電源オンになる時刻、つまり水曜日の朝以降に、*脆弱性とアプリケーションのアップデートの検索*タスクが実行されます。脆弱性スキャン時には CPU とディスクサブシステムの負荷が増大するため、このように業務時間中に処理が実行されてしまうことが問題となる可能性があります。組織で採用されている職場のルールに基づいて、このタスクに対する最も効率的なスケジュールをセットアップする必要があります。

アップデートのインストールと脆弱性の修正用グループタスクの手動セットアップ

クイックスタートウィザードにより、ネットワークエージェントのアップデートのインストールと脆弱性の修正用のグループタスクが作成されます。既定では、このタスクの実行時間は毎日午前 1 時に設定されており、［**未実行のタスクを実行する**］がオフになっています。

組織の職場のルールにより夜間はデバイスをシャットダウンするように定められている場合、アップデートのインストールは一切実行されません。組織で採用されている職場のルールに基づいて、脆弱性スキャンタスクに対する最も効率的なスケジュールをセットアップする必要があります。また、アップデートのインストール時には、デバイスの再起動を要求される場合があることにも注意してください。

イベントのリポジトリに保管できるイベントの最大数の設定

管理サーバーのプロパティウィンドウ内にある［**イベントリポジトリ**］セクションで、管理サーバーデータベース内で保管するイベントの設定を編集できます。編集可能な設定項目は、イベントのレコード数上限やレコードの保管期間があります。保管するイベント数の上限を指定すると、指定した数に応じて必要なディスク容量の概算値が算出されます。データベースのオーバーフローを避けるために十分な空き容量があるかどうかのこの概算値を使用できます。既定の設定では、管理サーバーデータベース内に保管できるイベント数は 400,000 件までとなっています。データベースで推奨される範囲でのイベント数の上限は、45,000,000 件です。

アプリケーションは 10 分ごとにデータベースをチェックします。イベント数が指定された最大値に 10,000 を加えた値に達すると、アプリケーションは最も古いイベントを削除し、指定された最大数のイベントのみが残ります。

管理サーバーが古いイベントを削除する際に、新しいイベントのデータベースへの保存は行えません。この期間、拒否したイベントの情報は Kaspersky イベントログに書き込まれます。新しいイベントはキューに追加され、削除操作が完了した後にデータベースに保存されます。

管理サーバーのイベントリポジトリに保存できるイベント数を制限するには：

1. 管理サーバーを右クリックして、［**プロパティ**］を選択します。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**イベントリポジトリ**］セクションの作業領域で、データベースに保存するイベントの最大数を指定します。
3. ［**OK**］をクリックします。

さらに、任意のタスクの設定を変更して、タスクの進行状況に関連するイベントを保存したり、タスクの実行結果のみを保存したりできます。それにより、データベース内のイベントの数を削減することで、データベース内のイベントの分析を伴う操作の実行速度を向上し、多数のイベントによって重要なイベントが上書きされる可能性を低下させることができます。

対応済みの脆弱性に関する情報を保管する期間

管理対象デバイス上ですでに対応済みの脆弱性に関する情報をデータベースに保管する期間を設定するには：

1. 管理サーバーを右クリックして、［**プロパティ**］を選択します。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**イベントリポジトリ**］セクションの作業領域で、脆弱性に関する情報をデータベースに保管する期間を設定します。
   既定では、保存期間は 90 日です。
3. ［**OK**］をクリックします。

脆弱性に関する情報をデータベースに保管する期間が指定した日数に制限されます。その後、管理サーバーのメンテナンスタスクがデータベースから期限切れの情報を削除します。

タスクの管理

Kaspersky Security Center は、様々なタスクを作成して実行することにより、デバイス上にインストールされたアプリケーションを管理します。アプリケーションのインストール、起動、停止、ファイルのスキャン、定義データベースやソフトウェアモジュールのアップデート、アプリケーションでのその他のタスクを実行するには、タスクが必要です。

タスクは、次の種別に分類されます：

- *グループタスク*：特定の管理グループのデバイスで実行されるタスク
- *管理サーバーのタスク*：管理サーバーで実行されるタスク
- *特定のデバイスに対するタスク*：管理グループに含まれるかどうかに関係なく、特定のデバイスで実行されるタスク

- *ローカルタスク*：特定の1台のデバイスで実行されるタスク

アプリケーションのタスクを作成できるのは、そのアプリケーション用の管理プラグインが管理コンピューターにインストールされている場合に限られます。

以下のいずれかの方法で、タスクを作成するデバイスのリスト（最大1000台）を作成することができます：

- ネットワークの管理サーバーによって検出されたデバイスを選択する。
- 手動でデバイスのリストを指定する。デバイスのアドレスとして、IPアドレス（またはIPアドレス範囲）、NetBIOS名またはDNS名を使用できます。
- 追加するデバイスのアドレスが記載されているtxtファイルからデバイスのリストをインポートする（各アドレスを独立した行に記載する必要があります）。

  デバイスのリストをファイルからインポートするか、または手動で作成し、デバイスが名前によって識別される場合、リストに含まれるのは、接続時またはデバイスの検索中にその情報が管理サーバーのデータベースに既に入力されているデバイスのみです。

アプリケーションごとに、任意の数のグループタスク、特定のデバイスに対するタスク、ローカルタスクを作成できます。

ネットワークエージェントと管理サーバーの接続時に、デバイスにインストールされているアプリケーションとKaspersky Security Centerのデータベースの間で、タスクに関する情報が交換されます。

タスクの設定に変更を加え、タスクの進行状況を表示し、タスクをコピー、エクスポート、インポート、および削除できます。

タスクは、そのタスクを作成した対象のアプリケーションが実行中である場合のみ、デバイス上で開始されます。アプリケーションが実行されていない場合は、実行中のすべてのタスクが取り消されます。

タスクの実行結果は、管理サーバー上のMicrosoft WindowsとKaspersky Security Centerのイベントログに一元的に保存されます。また、各デバイスのローカルにも保存されます。

タスクの設定には個人データを使用しないでください。たとえば、ドメイン管理者パスワードを指定することは避けてください。

マルチテナントをサポートするアプリケーションのタスク管理の詳細

マルチテナントをサポートするアプリケーションのグループタスクは、管理サーバーとクライアントデバイスの階層構造に応じてアプリケーションに適用されます。タスクの作成元となる仮想管理サーバーは、アプリケーションがインストールされているクライアントデバイスと同じ管理グループまたは下位の管理グループに存在する必要があります。

タスクの実行結果に相当するイベントで、サービスプロバイダーの管理者は、タスクが実行されたデバイスの情報を確認できます。これに対して、テナント管理者には、［**マルチテナントノード**］が表示されます。

タスクの作成

管理コンソールで、グループタスクを作成する管理グループのフォルダー内で直接タスクを作成することも、［**タスク**］フォルダーで作成することもできます。

管理グループのフォルダー内でグループタスクを作成するには：

1. コンソールツリーで、タスクを作成する管理グループを選択します。
2. グループの作業領域で、［**タスク**］タブを選択します。
3. ［**タスクの作成**］をクリックしてタスクの作成を実行します。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

*［**タスク**］フォルダー内の作業領域でタスクを作成するには：*

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. ［**終了**］をクリックしてタスクの作成を実行します。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

タスクの設定には個人データを使用しないでください。たとえば、ドメイン管理者パスワードを指定することは避けてください。

管理サーバーのタスクの作成

管理サーバーは、次のタスクを実行します：

- レポートの配信
- 管理サーバーのリポジトリへのアップデートのダウンロード
- 管理サーバーデータのバックアップ
- 管理サーバーのメンテナンス
- Windows Update の同期の実行
- 基準デバイスの OS イメージに基づくインストールパッケージの作成
- アプリケーションのリモートインストール
- アプリケーションのリモートアンインストール
- インストールパッケージの配布
- セカンダリ管理サーバーへのアプリケーションのリモートインストール

仮想管理サーバーでは、自動レポート配信タスクと、基準となるデバイスのオペレーティングシステムイメージに基づくインストールパッケージの作成タスクのみが使用できます。仮想管理サーバーのリポジトリには、プライマリ管理サーバーにダウンロードされたアップデートが表示されます。仮想管理サーバーのデータのバックアップは、プライマリ管理サーバーのデータのバックアップとともに実行されます。

管理サーバーのタスクを作成するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. 次のいずれかの方法で、タスクの作成を開始します：
   - コンソールツリーの［**タスク**］フォルダーのコンテキストメニューで、［**新規**］→［**タスク**］の順に選択します。
   - ［**タスク**］フォルダーの作業領域の［**タスクの作成**］をクリックします。

新規タスクウィザードが起動します。ウィザードの指示に従ってください。

［管理サーバーのリポジトリへのアップデートのダウンロード］タスク、［Windows Update の同期の実行］タスク、［データベースのメンテナンス］タスク、［*管理サーバーデータのバックアップ*］タスクを作成できるのは一度のみです。*管理サーバーのリポジトリへのアップデートのダウンロード*、*管理サーバーのメンテナンス*、*管理サーバーデータのバックアップ*および *Windows Update の同期の実行*タスクが既に管理サーバーで作成されている場合、それらのタスクは新規タスクウィザードのタスク種別選択ウィンドウに表示されません。

特定のデバイスに対するタスクの作成

Kaspersky Security Center では、特定のデバイスに対するタスクを作成できます。セットに加えられたデバイスは、様々な管理グループに含めたり、管理グループに含めなかったりすることができます。特定のデバイスに対して、次の主なタスクを実行できます：

- アプリケーションのリモートインストール
- ユーザーへのメッセージの送信
- 管理サーバーの変更
- デバイスの管理
- アップデートの検証
- インストールパッケージの配布
- セカンダリ管理サーバーへのアプリケーションのリモートインストール
- アプリケーションのリモートアンインストール

特定のデバイスに対するタスクを作成するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。

2. 次のいずれかの方法で、タスクの作成を開始します：

   - コンソールツリーの［**タスク**］フォルダーのコンテキストメニューで、［**新規**］→［**タスク**］の順に選択する。
   - ［**タスク**］フォルダーの作業領域の［**タスクの作成**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

ローカルタスクの作成

デバイスのローカルタスクを作成するには：

1. デバイスを含むグループの作業領域で、［**デバイス**］タブを選択します。
2. ［**デバイス**］タブのデバイスリストで、ローカルタスクを作成するデバイスを選択します。
3. 次のいずれかの方法で、選択したデバイスのタスクの作成を開始します：

   - ［**処理を実行**］をクリックし、ドロップダウンリストから［**タスクの作成**］を選択します。
   - デバイスの作業領域で［**タスクの作成**］をクリックします。
   - デバイスのプロパティを次のように使用します：

     a. デバイスのコンテキストメニューで［**プロパティ**］を選択します。

     b. デバイスのプロパティウィンドウが表示されたら、［**タスク**］セクションを選択して［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

ローカルタスクの作成と設定方法に関する詳細な手順については、各カスペルスキー製品のガイドを参照してください。

ネストされたグループの作業領域での継承したグループタスクの表示

ネストされたグループが継承したタスクを作業領域に表示するには：

1. ネストされたグループの作業領域で、［**タスク**］タブを選択します。
2. ［**タスク**］タブの作業領域で、［**継承したタスクの表示**］をクリックします。

   継承したタスクが次のいずれかのアイコンとともにタスクのリストに表示されます：

-  —プライマリ管理サーバー上で作成されたグループから継承された場合。
-  —トップレベルのグループから継承された場合。

継承モードが有効になっている場合、継承したタスクは、それが作成されたグループでのみ編集できます。継承したタスクは、タスクを継承したグループでは編集できません。

タスク開始前のデバイスの自動起動

Kaspersky Security Center は、電源がオフになっているデバイスでタスクを実行しません。これらのデバイスの電源を、タスク実行前に自動的に電源をオンにするように、Wake-on-LAN 機能を使用して設定できます。

タスク実行前に、デバイスが自動的に起動するように設定するには：

1. タスクのプロパティウィンドウで［**スケジュール**］セクションを選択します。
2. デバイスの動作を設定するには、［**詳細**］をクリックします。
3. 表示される［**詳細**］ウィンドウで、［**Wake on LAN の機能を使用してタスク開始前にデバイスを起動する（分）**］をオンにして、分単位で時間を指定します。

これにより、タスク実行前の指定した時間に、Wake-on-LAN を使用してデバイスが起動し、オペレーティングシステムが読み込まれます。タスクの完了後、デバイスユーザーがシステムにログインしてない場合は、デバイスが自動的にシャットダウンします。自動的にシャットダウンされるのは、Wake-on-LAN 機能を使用して起動されたデバイスのみであることにご注意ください。

オペレーティングシステムを自動的に開始可能なのは、Wake-on-LAN（WoL）標準をサポートするデバイスのみであることにご注意ください。

タスク完了後のデバイスの自動停止

Kaspersky Security Center では、タスクの完了後にタスクが配信されたデバイスが自動的に停止されるようにタスクを設定できます。

タスク完了後にデバイスを自動的にオフにするには：

1. タスクのプロパティウィンドウで［**スケジュール**］セクションを選択します。
2. ［**詳細**］をクリックして、デバイスに対する処理を設定するためのウィンドウを開きます。
3. 表示される［**詳細**］ウィンドウで、［**タスク完了後にデバイスをシャットダウンする**］をオンにします。

タスク実行時間の制限

タスクがデバイス上で実行される時間を制限するには：

1. タスクのプロパティウィンドウで［**スケジュール**］セクションを選択します。
2. ［**詳細**］をクリックすると、クライアントデバイスに対して実行する処理の設定ウィンドウが開きます。

3. 表示される［**詳細**］ウィンドウで、［**次の時間を超える場合はタスクを停止する（分）**］をオンにして、分単位で時間を指定します。

指定した時間が経過してもデバイス上でタスクが完了していない場合、Kaspersky Security Center はタスクを自動的に停止します。

タスクのエクスポート

グループタスクと特定のデバイスに対するタスクをファイルにエクスポートできます。管理サーバーのタスクはエクスポートできません。

タスクをエクスポートするには：

1. タスクのコンテキストメニューから、［**すべてのタスク**］→［**エクスポート**］の順に選択します。
2. 開かれる［**名前を付けて保存**］ウィンドウで、ファイル名のパスを指定します。
3. ［**保存**］をクリックします。

ローカルユーザーの権限はエクスポートされません。

タスクのインポート

グループタスクと特定のデバイスに対するタスクをインポートできます。管理サーバーのタスクはインポートできません。

タスクをインポートするには：

1. タスクをインポートする必要があるタスクリストを選択します。
   - タスクをグループタスクのリストにインポートする場合は、該当する管理グループの作業領域で、［**タスク**］タブを選択します。
   - 特定のデバイスのタスクリストにタスクをインポートする場合は、コンソールツリーで［**タスク**］フォルダーを選択します。
2. 次のオプションのいずれかを選択して、タスクをインポートします：
   - タスクリストのコンテキストメニューで、［すべてのタスク］→［**インポート**］の順に選択します。
   - タスクリストの管理セクションで［**タスクをファイルからインポート**］をクリックします。
3. 表示されるウィンドウで、タスクのインポート元となるファイルのパスを指定します。
4. ［**開く**］をクリックします。

タスクがタスクリストに表示されます。

新しくインポートされたタスクと同じ名前のタスクが既に存在している場合、インポートされたタスクの名前に、たとえば **(1)**、**(2)** のようなインデックス「**(<次の連番>)**」が付きます。

タスクの変換

Kaspersky Security Center では、カスペルスキー製品の旧バージョンのタスクを最新バージョンのタスクに変換できます。

変換は次のアプリケーションのタスクに対して可能です：

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Endpoint Security 8 for Windows
- Kaspersky Endpoint Security 10 for Windows

タスクを変換するには：

1. コンソールツリーで、タスクを変換する管理サーバーを選択します。
2. 管理サーバーのコンテキストメニューで、［**すべてのタスク**］→［**ポリシーとタスクの一括変換ウィザード**］の順に選択します。

   ポリシーとタスクのバッチ変換ウィザードが起動します。ウィザードの指示に従ってください。

ウィザードの処理が終了すると、アプリケーションの旧バージョンのタスク設定を使用する新しいタスクが作成されます。

タスクの手動での開始と終了

タスクのコンテキストメニューから、またはタスクが割り当てられたクライアントデバイスのプロパティウィンドウで、タスクを手動で起動および終了できます。

デバイスのコンテキストメニューからのグループタスクの開始は、**KLAdmins グループ**に含まれるユーザーにのみ許可されます。

タスクのコンテキストメニューまたはプロパティウィンドウからタスクを開始または停止するには：

1. タスクリストでタスクを選択します。
2. 次のいずれかの方法で、タスクを開始または停止します：
   - タスクのコンテキストメニューで、［**開始**］または［**停止**］を選択する。
   - タスクプロパティウィンドウの［**全般**］セクションで、［**開始**］または［**停止**］をクリックする。

クライアントデバイスのコンテキストメニューまたはプロパティウィンドウからタスクを開始または停止するには：

1. デバイスのリストでデバイスを選択します。
2. 次のいずれかの方法で、タスクを開始または停止します：
   - デバイスのコンテキストメニューから［**すべてのタスク**］→［**タスクの実行**］の順に選択します。タスクのリストから関連するタスクを選択します。

     タスクが割り当てられているデバイスのリストが、選択したデバイスに置き換えられます。タスクが開始します。
   - デバイスのプロパティウィンドウの［**タスク**］セクションで開始ボタン（  ）または停止ボタン（  ）をクリックします。

タスクの手動での一時停止と再開

実行中のタスクを手動で一時停止または再開するには：

1. タスクリストでタスクを選択します。
2. 次のいずれかの方法で、タスクを一時停止または再開します：
   - タスクのコンテキストメニューで、［**一時停止**］または［**再開**］を選択する。
   - タスクのプロパティウィンドウで［**全般**］セクションを選択し、［**一時停止**］または［**再開**］をクリックする。

タスク実行の監視

タスク実行を監視するには：

タスクのプロパティウィンドウで［**全般**］セクションを選択します。

［**全般**］セクションの中央部に、タスクの現在のステータスが表示されます。

管理サーバーに保存されているタスク実行結果の確認

Kaspersky Security Center では、グループタスク、特定のデバイスに対するタスク、管理サーバータスクの実行結果を確認できます。

タスク結果を表示するには：

1. タスクのプロパティウィンドウで［**全般**］セクションを選択します。
2. ［**履歴**］をクリックして、［**タスク履歴**］ウィンドウを開きます。

セカンダリ管理サーバーのタスク結果を表示するには：

1. タスクのプロパティウィンドウで［**全般**］セクションを選択します。
2. ［**履歴**］をクリックして、［**タスク履歴**］ウィンドウを開きます。
3. ［**セカンダリサーバーからの統計**］をクリックします。
4. ［**タスク履歴**］ウィンドウを表示するセカンダリサーバーを選択します。

タスク実行結果に関する情報フィルタリングの設定

Kaspersky Security Center では、グループタスク、特定のデバイスに対するタスク、管理サーバータスクの実行結果に関する情報をフィルタリングできます。ローカルタスクにはフィルタリングは適用されません。

タスク実行結果に関する情報フィルタリングを設定するには：

1. タスクのプロパティウィンドウで［**全般**］セクションを選択します。
2. ［**履歴**］をクリックして、［**タスク履歴**］ウィンドウを開きます。
   上部のテーブルには、タスクが割り当てられているすべてのデバイスのリストが表示されます。下部のテーブルには、選択したデバイスで実行されたタスクの結果が表示されます。
3. 該当するテーブルを右クリックして、コンテキストメニューを開き、［**フィルター**］を選択します。
4. 表示される［**フィルターの設定**］ウィンドウの［**イベント**］、［**デバイス**］、［**日時**］セクションでフィルターを設定します。［OK］をクリックします。

   ［**タスク履歴**］ウィンドウに、フィルターで指定した設定を満たす情報が表示されます。

タスクの変更：変更のロールバック

タスクを変更するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. ［**タスク**］フォルダーの作業領域で、タスクを選択し、コンテキストメニューを使用してタスクのプロパティウィンドウを開きます。
3. 必要な変更を加えます。

   ［**タスク範囲からの除外**］セクションでは、タスクを適用しないサブグループのリストを設定できます。

4. ［**適用**］をクリックします。

タスクに加えた変更は、タスクのプロパティウィンドウの［**変更履歴**］セクションに保存されます。

必要に応じて、タスクの変更をロールバックできます。

タスクの変更をロールバックするには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. 変更をロールバックするタスクを選択し、コンテキストメニューを使用してタスクのプロパティウィンドウを開きます。
3. タスクのプロパティウィンドウで［**変更履歴**］セクションを選択します。
4. タスクのリビジョンのリストで、変更のロールバック先となるリビジョンの番号を選択します。
5. ［**詳細**］をクリックして、ドロップダウンリストから［**ロールバック**］を選択します。

タスクの比較

同じ種別のタスクを比較することができます。たとえば、2 つのマルウェアスキャンタスクは比較可能ですが、マルウェアスキャンタスクとアップデートのインストールタスクは比較できません。比較後、一致するタスクの設定と異なる設定を示すレポートが届きます。タスクの比較レポートは印刷するか、ファイルとして保存することができます。社内の諸部署に同じ種別の様々なタスクが割り当てられている場合、タスクを比較することが必要になる場合があります。たとえば、経理部の従業員の場合は、コンピューターのローカルディスクのみにマルウェアスキャンを実行するタスクがある一方で、営業部の従業員は顧客とやり取りしているため、ローカルディスクとメールの両方をスキャンするタスクがあります。すべてのタスクの設定を確認しなくても、タスクを比較するだけで、そのような相違をすぐに把握することができます。

比較できるのは同じ種別のタスクだけです。

ペアの状態でのみ、タスクの比較が可能です。

1 つのタスクを選択して別のタスクと比較する方法、またはタスクのリストの 2 つのタスクを比較する方法のいずれかでタスクを比較できます。

1 つのタスクを選択して別のタスクと比較するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. ［**タスク**］フォルダーの作業領域で、別のタスクと比較するタスクを選択します。
3. タスクのコンテキストメニューから、［**すべてのタスク**］→［**他のタスクと比較**］の順に選択します。
4. ［**タスクの選択**］ウィンドウで、比較するタスクを選択します。
5. ［OK］をクリックします。

   2 つのタスクを比較する HTML 形式のレポートが表示されます。

タスクのリストにある 2 つのタスクを比較するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。

2. ［**タスク**］フォルダーのタスクのリストで **SHIFT** キーまたは **CTRL** キーを押して、同じ種別の 2 つのタスクを選択します。

3. コンテキストメニューから［**比較**］を選択します。

   選択したタスクを比較する HTML 形式のレポートが表示されます。

タスクの比較時、パスワードが一致しない場合、アスタリスク（******）がタスク比較レポートに表示されます。

タスクプロパティでパスワードが変更された場合、アスタリスク（******）がリビジョン比較レポート（******）に表示されます。

タスクを開始するアカウント

タスクを実行するアカウントを指定できます。

たとえば、オンデマンドスキャンタスクを実行するには、スキャン対象オブジェクトに対するアクセス権限が必要であり、アップデートタスクを実行する場合はプロキシサーバーに対する認証が必要です。タスクを実行するアカウントを指定できれば、タスクを実行するユーザーに必要なアクセス権限がない場合に、オンデマンドスキャンタスクやアップデートタスクで問題が生じるのを防ぐことができます。

リモートインストールやアンインストールのタスクの実行中、ネットワークエージェントがインストールされていないか使用できない時に、アプリケーションのインストールまたはアンインストールに必要なファイルをクライアントデバイスにダウンロードする場合は、指定のアカウントが使用されます。ネットワークエージェントがインストールされていて使用可能な場合、タスク設定に従ってファイル配信が Microsoft Windows ユーティリティのみを使用して共有フォルダーから実行される時に、このアカウントが使用されます。この場合、アカウントはデバイス上で次の権限を持っている必要があります：

- アプリケーションをリモート起動する権限
- Admin$ リソースを使用する権限
- *サービスとしてログオンする権限*

ファイルがネットワークエージェントによってデバイスに配信される場合、アカウントは使用されません。その後のファイルのコピーおよびインストールのすべての操作は**ネットワークエージェント**（**ローカルシステムアカウント**）によって実行されます。

タスクのパスワード変更ウィザード

非ローカルタスクの場合、タスクを実行するアカウントを指定できます。アカウントは、タスクの作成時または既存のタスクのプロパティで指定できます。指定されたアカウントが組織のセキュリティ指示に従って使用されている場合、その指示によってアカウントパスワードの変更が必要になる場合があります。アカウントパスワードの有効期限が切れて新しいパスワードを設定すると、タスクプロパティで新しい有効なパスワードを指定するまで、タスクを開始しません。

タスクのパスワード変更ウィザードを使用すると、アカウントが指定されているすべてのタスクで、古いパスワードを新しいパスワードに自動的に置換できます。または、各タスクのプロパティで手動で設定できます。

タスクのパスワード変更ウィザードを起動するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。

2. フォルダーのコンテキストメニューで、［**タスクのパスワード変更ウィザード**］を選択します。

ウィザードの指示に従います。

ステップ 1：資格情報の指定

［**アカウント**］と［**パスワード**］で、お使いのシステム（Active Directory など）で現在有効な新しい資格情報を指定します。ウィザードの次のステップに進むと、指定されたアカウント名が、非ローカルタスクそれぞれのプロパティのアカウント名と一致するかどうか確認されます。アカウント名が一致すると、タスクのプロパティのパスワードは自動的に新しいものに置換されます。

［**以前のパスワード (任意)**］に手動で入力した場合、アカウント名と古いパスワードの両方が見つかったタスクの、パスワードのみが置き換えられます。置換は自動で実行されます。その他の場合はすべて、ウィザードの次の手順で、実行する処理を選択する必要があります。

ステップ 2：実行する処理の選択

ウィザードの最初のステップで古いパスワードを指定していない場合、または指定した古いパスワードがタスクのパスワードと一致しない場合、見つかったタスクに対して実行する処理を選択する必要があります。

［*承認が必要です*］ステータスを持つ各タスクに対して、タスクのプロパティのパスワードを削除するか、新しいパスワードに置き換えるかを決定します。パスワードの削除を選択した場合、タスクは既定のアカウントで実行されるように切り替わります。

ステップ 3：結果の表示

ウィザードの最後のステップで、見つかった各タスクの結果を表示します。ウィザードを終了するには、［**終了**］をクリックします。

仮想管理サーバーの下位となる管理グループの階層の作成

仮想管理サーバーの作成が完了すると、自動的に「**管理対象デバイス**」という名前の管理グループが含まれます。

仮想管理サーバーの下位となる管理グループ階層の作成手順は、物理管理サーバーの下位となる管理グループ階層の作成手順と同様です。

> 仮想管理サーバーの下位となる管理グループにセカンダリ管理サーバーおよび仮想管理サーバーを追加することはできません。これは仮想管理サーバーの制限によるためです。

ポリシーとポリシーのプロファイル

Kaspersky Security Center Web コンソールを使用して、カスペルスキー製品のポリシーを作成できます。このセクションでは、ポリシーおよびポリシーのプロファイルの概要、作成方法、編集方法を説明しています。

ポリシーのプロファイルを使用した、ポリシーの階層

このセクションでは、管理グループ内のデバイスにポリシーを適用する方法について説明します。また、ポリシープロファイルについても説明します。

ポリシーの階層

Kaspersky Security Center では、複数のデバイスに対して単一の一連の設定を定義するためにポリシーを使用します。たとえば、管理グループ G で定義されているアプリケーション P のポリシー範囲には、グループ G とそのすべてのサブグループの、アプリケーション P がインストールされた管理対象デバイスが含まれます。ただし、プロパティで［**親グループから継承する**］がオフになっているサブグループを除きます。

ポリシーは、設定の横にロックアイコン（🔒）がある点で、ローカル設定とは異なります。ポリシープロパティの設定（または設定のグループ）がロックされている場合は、効率的な設定を作成する際に最初にこの設定（または、設定のグループ）を使用し、次に下位のポリシーに対して設定または設定のグループを記述する必要があります。

デバイスに対して効率的な設定を作成する際の説明は次の通りです。ロックされていない設定値をすべてポリシーから取得し、その値をローカル設定値で上書きします。これにより、生成されたコレクションがポリシーから取得したロック済みの設定値により上書きされます。

同じアプリケーションのポリシーは、管理グループの階層を介してお互いに影響を与えます。上位のポリシーのロック済みの設定は、下位のポリシーの同じ設定を上書きします。

モバイルユーザーに対しては、特別なポリシーが存在します。このポリシーは、デバイスがモバイルユーザーモードに切り替わった際に有効になります。モバイルユーザーポリシーが管理グループの階層を介して他のポリシーに影響することはありません。

> Kaspersky Security Center の今後のバージョンでは、モバイルユーザーポリシーはサポートされなくなります。モバイルユーザーポリシーに代わって、ポリシーのプロファイルが使用されます。

ポリシーのプロファイル

多数の環境において、デバイスにポリシーを適用する方法が管理グループの階層を使用するだけというのは適切ではありません。複数の管理グループで 1 つまたは 2 つの設定値が異なる単一ポリシーで複数のインスタンスを作成し、将来これらのポリシーの内容を同期させることが必要になる場合があります。

このような問題を回避するために、Kaspersky Security Center は*ポリシープロファイル*をサポートしています。ポリシーのプロファイルには、ポリシー設定のサブセットが指定されています。このサブセットはポリシーとともに対象デバイスに配信され、*プロファイルの有効化条件*と呼ばれる特定の条件下でポリシーを補完する機能を果たします。プロファイルに含まれるのは、クライアントデバイス（コンピューターまたはモバイルデバイス）でアクティブな「基本」ポリシーとは異なる設定のみです。プロファイルを有効にすると、プロファイルが有効になる前にデバイスで有効になっていたポリシー設定が修正されます。こうした設定により、プロファイルで指定された値が得られます。

現在、ポリシーのプロファイルに適用されている制限事項は次の通りです：

- ポリシーには最大 100 個のプロファイルを含めることができます。
- ポリシーのプロファイルにその他のプロファイルを含めることはできません。
- ポリシーのプロファイルに通知の設定を含めることはできません。

プロファイルの内容

ポリシーのプロファイルには、次の構成要素が含まれています：

- 名前：同じ名前のプロファイルは、共通のルールが含まれる管理グループの階層によって相互に影響します。
- ポリシー設定のサブセット：すべての設定が含まれているポリシーとは異なり、プロファイルには実際に必要な設定のみが含まれています（ロック済みの設定）。
- アクティベーション条件：デバイスのプロパティを使用した論理式。プロファイルが有効になる（ポリシーを補完する）のは、プロファイルの有効化条件に該当する場合のみです。その他の場合はすべて、プロファイルは非アクティブで無視されます。論理式には、次のデバイスプロパティを含めることができます：
  - モバイルユーザーモードのステータス
  - ネットワーク環境のプロパティ：ネットワークエージェント接続の有効なルールの名前
  - 指定したタグがデバイスに存在するかどうか
  - Active Directory 単位におけるデバイスの場所：明示的（デバイスはまさに指定した OU 内にある）、または暗黙的（デバイスは OU 内にある。ただし、任意のネストレベルで指定した OU 内にある）
  - デバイスが属している Active Directory セキュリティグループ（明示的または暗黙的）
  - デバイス所有者が属している Active Directory セキュリティグループ（明示的または暗黙的）
- プロファイルを無効にする：無効化されたプロファイルは常に無視され、それぞれの有効化条件は検証されません。
- プロファイルの優先度：異なるプロファイルの有効化条件は独立しているため、複数のプロファイルを同時に有効化することができます。アクティブなプロファイルに重複しない一連の設定が含まれている場合、問題は発生しません。ただし、2 つのアクティブなプロファイルで同じ設定の値が異なる場合は、不明確さが発生します。この不明確さを回避するために、プロファイルの優先度が使用されます。不明確な変数の値は、優先度が高い方（プロファイルのリスト内での位置付けが高い方）のプロファイルから取得されます。

ポリシーが階層を介してお互いに影響を与え合う場合のプロファイルの動作

名前が同じプロファイルは、ポリシー統合ルールに従って統合されます。上位のポリシーのプロファイルは、下位のポリシーのプロファイルよりも優先度が高くなっています。上位のポリシーで設定の編集がブロックされている（ロック状態）場合、下位のポリシーでは上位のポリシーのプロファイルの有効化条件が使用されます。一方、上位のポリシーで設定の編集が許可されている場合は、下位のポリシーのプロファイルの有効化条件が使用されます。

ポリシーのプロファイルの有効化条件には［**オフラインのデバイス**］プロパティが含まれているため、プロファイルではサポートされていないモバイルユーザー用のポリシー機能は完全に置き換えられます。

モバイルユーザー用のポリシーにはプロファイルが含まれていることがありますが、そのプロファイルがアクティブ化されるのは、デバイスがモバイルユーザーモードに切り替えられた後だけです。

ポリシー設定の継承

ポリシーは管理グループに対して指定します。ポリシーの設定を*継承し*、ポリシーが設定されている管理グループのサブグループ（子グループ）に設定を反映させることができます。以降の説明では、親グループで設定されているポリシーを「*親ポリシー*」と表記する場合があります。

継承に関して2つのオプションをオンまたはオフにできます：［**親ポリシーから設定を継承する**］と［**設定を子ポリシーへ強制的に継承させる**］：

- 子ポリシーで［**親ポリシーから設定を継承する**］をオンにし、親ポリシーの設定の一部をロック状態にすると、子グループでこれらの設定を変更できません。ただし、親ポリシーでロック状態になっていない設定は変更できます。
- 子ポリシーで［**親ポリシーから設定を継承する**］をオフにすると、親ポリシーでロック状態の設定も含めて、子ポリシー側ですべての設定を変更できます。
- 親ポリシーで［**設定を子ポリシーへ強制的に継承させる**］をオンにすると、すべての子ポリシーで［**親ポリシーから設定を継承する**］がオンになります。この場合、子ポリシーの側でこのオプションをオフにすることはできません。親ポリシーでロックされている設定はすべて強制的に子ポリシーに継承され、子グループ側でこれらの設定を変更することはできません。
- ［**管理対象デバイス**］グループにはそれより上位のグループが存在せず、他のポリシーを継承することがないため、［**管理対象デバイス**］グループのポリシーの［**親ポリシーから設定を継承する**］が設定に影響を及ぼすことはありません。

既定では、新規に作成したポリシーでは［**親ポリシーから設定を継承する**］はオンです。

ポリシーにポリシープロファイルが存在する場合、子ポリシーでもこれらのプロファイルが継承されます。

ポリシーの管理

クライアントデバイスにインストールされたアプリケーションは、ポリシーの定義を使用して一元的に設定されます。

管理グループのアプリケーションに対して作成されたポリシーは、作業領域の［**ポリシー**］タブに表示されます。それぞれのポリシー名の前に、ポリシーのステータスを表すアイコンがあります。

ポリシーが削除または無効化された後も、ポリシーで指定された設定が引き続き使用されます。これらの設定は後から手動で変更できます。

ポリシーは次のように適用されます：デバイスで常駐タスク（リアルタイム保護タスク）が実行されている場合、新しい設定の値で実行を続けます。開始された定期的なタスク（オンデマンドスキャン、定義データベースのアップデート）は、変更前の値で実行され続けます。次回は、新しい設定値で実行されます。

マルチテナントサポートのアプリケーションのポリシーは、下位の管理グループだけでなく上位の管理グループにも継承され、アプリケーションがインストールされているすべてのクライアントデバイスに反映されます。

管理サーバーが階層構造になっている場合、セカンダリ管理サーバーがプライマリ管理サーバーからポリシーを受け取ってクライアントデバイスに配信します。継承が有効な場合は、プライマリ管理サーバーでポリシー設定を変更できます。その後、ポリシー設定の変更がセカンダリ管理サーバーで継承されたポリシーに反映されます。

プライマリ管理サーバーとセカンダリ管理サーバー間の接続が切断された場合、セカンダリ管理サーバーのポリシーは適用された設定を引き続き使用します。プライマリ管理サーバー上で変更されたポリシー設定は、接続の再確立後にセカンダリ管理サーバーに配信されます。

継承が無効な場合は、プライマリ管理サーバーとは無関係に、セカンダリ管理サーバー上でポリシー設定を変更できます。

管理サーバーとクライアントデバイスとの間の接続が切断されている場合、クライアントデバイスはモバイルユーザーポリシー（定義されている場合）の使用を開始するか、接続が再確立されるまで、適用されたポリシー設定を引き続き使用します。

セカンダリ管理サーバーへのポリシー配信の結果は、プライマリ管理サーバーのコンソールのポリシープロパティウィンドウに表示されます。

クライアントデバイスへのポリシー配信の結果は、接続している管理サーバーのポリシープロパティウィンドウに表示されます。

ポリシーの設定には個人情報を使用しないでください。たとえば、ドメイン管理者パスワードを指定することは避けてください。

ポリシーの作成

管理コンソールで、ポリシーを作成する管理グループのフォルダー内で直接ポリシーを作成することも、［**ポリシー**］フォルダーで作成することもできます。

管理グループのフォルダー内でポリシーを作成するには：

1. コンソールツリーで、ポリシーを作成する管理グループを選択します。
2. グループの作業領域で、［**ポリシー**］タブを選択します。
3. ［**新規ポリシー**］をクリックして新規ポリシーウィザードを実行します。

新規ポリシーウィザードが起動します。ウィザードの指示に従ってください。

*［**ポリシー**］フォルダー内の作業領域でポリシーを作成するには：*

1. コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. ［**新規ポリシー**］をクリックして新規ポリシーウィザードを実行します。

新規ポリシーウィザードが起動します。ウィザードの指示に従ってください。

グループで1つのアプリケーションについて複数のポリシーを作成できますが、一度に有効にできるポリシーは1つのみです。新しいアクティブポリシーを作成すると、以前のアクティブポリシーは非アクティブになります。

ポリシーを作成する際に、アプリケーションの動作に必要な最小限のパラメータを指定できます。その他の値はすべて、アプリケーションのローカルインストール時に適用される既定値に設定されています。ポリシーは作成した後でも変更できます。

ポリシーの設定には個人情報を使用しないでください。たとえば、ドメイン管理者パスワードを指定することは避けてください。

ポリシーの適用後に変更されたカスペルスキー製品の設定の詳細については、各ガイドを参照してください。

ポリシーを作成すると、それまでアプリケーションに対して指定されていた設定に関係なく、変更がロックされている（鍵アイコン（）が表示されている）設定が、クライアントデバイスで有効になります。

下位グループに継承されたポリシーの表示

ネストされた管理グループで継承したポリシーの表示を有効にするには：

1. コンソールツリーで、継承したポリシーを表示する必要がある管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 作業領域のポリシーのリストのコンテキストメニューで、［**表示**］→［**継承したポリシー**］の順に選択します。

継承したポリシーが次のアイコンを付けてポリシーのリストに表示されます。

- —プライマリ管理サーバー上で作成されたグループから継承された場合。
- —トップレベルのグループから継承された場合。

設定の継承モードが有効になっている場合、継承したポリシーは、そのポリシーが作成されたグループ内でのみ変更できます。ポリシーを継承したグループ内で、継承したポリシーを変更することはできません。

ポリシーのアクティベーション

選択したグループのポリシーをアクティブにするには：

1. グループの作業領域の［**ポリシー**］タブで、アクティブにする必要があるポリシーを選択します。
2. ポリシーをアクティブにするには、次の処理のいずれかを実行します：
   - ポリシーのコンテキストメニューから［**アクティブポリシー**］を選択します。
   - ポリシーのプロパティウィンドウの［**全般**］セクションで、［**ポリシーのステータス**］から［**アクティブポリシー**］を選択します。

選択した管理グループのポリシーがアクティブになります。

多数のクライアントデバイスにポリシーを適用すると、管理サーバーの負荷とネットワークのトラフィックが一時的に大幅に増加します。

［ウイルスアウトブレイク］イベント発生時におけるポリシーの自動アクティブ化

［ウイルスアウトブレイク］イベント発生時にポリシーの自動アクティベーションを実行するには：

1. 管理サーバーのプロパティウィンドウで［**ウイルスアウトブレイク**］セクションを開きます。
2. ［［**ウイルスアウトブレイク］イベント発生時にアクティブ化するポリシーの設定**］をクリックして［**ポリシーのアクティブ化**］ウィンドウを開き、ウイルスアウトブレイクの検知時にアクティブ化されるポリシーの選択リストにそのポリシーを追加します。

［*ウイルスアウトブレイク*］イベントでポリシーがアクティブ化された場合は、手動モードを使用することによってのみ前のポリシーに戻ることができます。

モバイルユーザーポリシーの適用

デバイスが組織のネットワークから切断されると、モバイルユーザーポリシーが有効になります。

モバイルユーザーポリシーを適用するには：

ポリシープロパティウィンドウで、［**全般**］セクションを開き、［**ポリシーのステータス**］で［**モバイルユーザーポリシー**］を選択します。

デバイスが組織のネットワークから切断されると、そのデバイスにモバイルユーザーポリシーが適用されます。

ポリシーの変更：変更のロールバック

ポリシーを変更するには：

1. コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. ［**ポリシー**］フォルダーの作業領域で、ポリシーを選択し、コンテキストメニューを使用してポリシーのプロパティウィンドウを開きます。
3. 必要な変更を加えます。
4. ［**適用**］をクリックします。

ポリシーに加えた変更は、ポリシーのプロパティの［**変更履歴**］セクションに保存されます。

必要に応じて、ポリシーの変更をロールバックできます。

ポリシーの変更をロールバックするには：

1. コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 変更をロールバックするポリシーを選択し、コンテキストメニューを使用してポリシーのプロパティウィンドウを開きます。
3. ポリシーのプロパティウィンドウで［**変更履歴**］セクションを選択します。
4. ポリシーのリビジョンのリストで、変更のロールバック先となるリビジョンの番号を選択します。
5. ［**詳細**］をクリックして、ドロップダウンリストから［**ロールバック**］を選択します。

ポリシーの比較

1つの管理対象アプリケーションの 2 つのポリシーを比較することができます。比較後、一致するポリシーの設定と異なる設定を示すレポートが届きます。たとえば、複数の管理者がそれぞれのオフィスで1つの管理対象アプリケーションのポリシーを各自で作成した場合、または1つの上位ポリシーがすべてのローカルオフィスに継承された後でそれぞれのオフィスで変更された場合は、ポリシーの比較が必要になる場合があります。ポリシーを比較するには、1つのポリシーを選択して他のポリシーと比較するか、ポリシーのリストにある 2 つのポリシーを比較します。

比較できるのは、リビジョン履歴に現在のリビジョンがあるポリシーのみです。

1 つのポリシーを他のポリシーと比較するには：

1. コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. ［**ポリシー**］フォルダーの作業領域で、他のポリシーと比較するポリシーを選択します。
3. ポリシーのコンテキストメニューで［**ポリシーを他のポリシーと比較**］を選択します。
4. ［**ポリシーの選択**］ウィンドウで、ポリシーの比較対照にするポリシーを選択します。
5. ［OK］をクリックします。

同じアプリケーションの 2 つのポリシーの比較が HTML 形式のレポートで表示されます。

ポリシーのリストにある 2 つのポリシーを比較するには：

1. ［**ポリシー**］フォルダーのポリシーのリストで **SHIFT** キーまたは **CTRL** キーを使用して、1つの管理対象アプリケーションの 2 つのポリシーを選択します。
2. コンテキストメニューから［**比較**］を選択します。

同じアプリケーションの 2 つのポリシーの比較が HTML 形式のレポートで表示されます。

Kaspersky Endpoint Security for Windows のポリシー設定の比較に関するレポートには、ポリシープロファイルの比較も詳述されています。ポリシープロファイルの比較結果は最小化することができます。セクションを最小化するには、セクション名に隣接する矢印アイコン（▲）をクリックします。

ポリシー導入ステータス図の表示

Kaspersky Security Center では、各デバイスでのポリシー適用の結果を表示できます。

各デバイスのポリシー導入ステータスを表示するには：

1. グループのワークスペースの［**ポリシー**］タブで、配布ステータスを表示するポリシーを選択します。
   右側のペインのグラフには、ポリシーの適用の概要が表示されます。
2. ［**詳細**］をクリックします。
   ［**ポリシー適用の結果**］ウィンドウが開きます。
   ポリシーの適用の結果を CSV ファイルまたは TXT ファイルにエクスポートできます。

ポリシーの削除

ポリシーを削除するには：

1. 管理グループの作業領域の［**ポリシー**］タブで、削除するポリシーを選択します。
2. 次のいずれかの方法で、ポリシーを削除します：
   - ポリシーのコンテキストメニューで［**削除**］を選択する。
   - 選択したポリシーの情報ボックスで、［**ポリシーの削除**］をクリックします。

ポリシーのコピー

ポリシーをコピーするには：

1. 任意のグループの作業領域の［**ポリシー**］タブでポリシーを選択します。
2. ポリシーのコンテキストメニューで［**コピー**］を選択します。
3. コンソールツリーで、ポリシーを追加するグループを選択します。
   コピー元のグループにポリシーを追加することもできます。
4. 選択したグループの［**ポリシー**］タブで、ポリシーリストのコンテキストメニューから［**貼り付け**］を選択します。

ポリシーがそのすべての設定とともにコピーされ、コピー先のグループ内のデバイスに適用されます。ポリシーをコピー元と同じグループに貼り付けた場合、ポリシー名の末尾に、たとえば「**(1)**」「**(2)**」のように「**(<次の連番>)**」が自動的に追加されます。

コピー中のアクティブポリシーは非アクティブになります。必要に応じて、アクティブにすることができます。

ポリシーのエクスポート

ポリシーをエクスポートするには：

1. ポリシーを次のいずれかの方法でエクスポートします：

   - ポリシーのコンテキストメニューから［**すべてのタスク**］→［**エクスポート**］の順に選択します。
   - 選択したポリシーの情報ボックスで、［**ポリシーをファイルにエクスポート**］をクリックします。

2. 開かれる［**名前を付けて保存**］ウィンドウで、ポリシーファイルの名前とパスを指定します。［**保存**］をクリックします。

ポリシーのインポート

ポリシーをインポートするには：

1. 目的のグループの作業領域の［**ポリシー**］タブで、次のポリシーのインポート方法のいずれかを選択します：

   - ポリシーリストのコンテキストメニューから［**すべてのタスク**］→［**インポート**］の順に選択します。
   - ポリシーリストの管理セクションで［**ポリシーをファイルからインポート**］をクリックします。

2. 表示されるウィンドウで、ポリシーのインポート元となるファイルのパスを指定します。［**開く**］をクリックします。

インポートされたポリシーがポリシーリストに表示されます。ポリシーの設定とプロファイルもインポートされます。エクスポート中に選択されたポリシーステータスにかかわらず、インポートされたポリシーは非アクティブです。ポリシーのプロパティでポリシーステータスを変更できます。

新しくインポートされたポリシーと同じ名前のポリシーが既に存在している場合、インポートされたポリシーの名前に、たとえば **(1)**、**(2)** のようなインデックス「**(<次の連番>)**」が付きます。

ポリシーの変換

Kaspersky Security Center では、管理対象のカスペルスキー製品の旧バージョンのポリシーを最新バージョンのポリシーに変換できます。変換されたポリシーには、更新前に指定された現在の管理者の設定が保持されるだけでなく、製品の最新バージョンの新しい設定が含まれます。カスペルスキー製品の管理プラグインが、これらのアプリケーションのポリシーを変換できるかどうかを判断します。サポート対象の各カスペルスキー製品のポリシーの変換については、次のリストから関連するヘルプを参照してください：

- **ワークステーション用のカスペルスキー製品：**
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Linux ARM64 Edition
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Embedded Systems Security for Windows

- **Kaspersky Industrial CyberSecurity：**
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Linux Nodes
  - Kaspersky Industrial CyberSecurity for Networks（一元的な導入はサポート対象外です）
- **モバイルデバイス用のカスペルスキー製品：**
  - Kaspersky Endpoint Security for Android
  - Kaspersky Security for iOS
- **ファイルサーバー用のカスペルスキー製品：**
  - Kaspersky Security for Windows Server
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
- **仮想マシン用のカスペルスキー製品：**
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Security for Virtualization Agentless
- **メールシステムおよび SharePoint / コラボレーションサーバー用のカスペルスキー製品：**
  - Kaspersky Security for Linux Mail Server
  - Kaspersky Security for Microsoft Exchange Servers
- **標的型攻撃の検知用のカスペルスキー製品：**
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- **KasperskyOS デバイス用のカスペルスキー製品：**
  - Kaspersky IoT Secure Gateway
  - Kaspersky Security Management Suite（Kaspersky Thin Client 用のプラグイン）

ポリシーを変換するには：

1. コンソールツリーで、ポリシーを変換する管理サーバーを選択します。
2. 管理サーバーのコンテキストメニューで、［**すべてのタスク**］→［**ポリシーとタスクの一括変換ウィザード**］の順に選択します。

ポリシーとタスクのバッチ変換ウィザードが起動します。ウィザードの指示に従ってください。

ウィザードが完了すると、現在の管理者のポリシー設定とカスペルスキー製品の最新バージョンの新しい設定を使用する新しいポリシーが作成されます。

ポリシーのプロファイルの管理

ポリシーのプロファイルは、デバイスが特定の有効化ルールを満たす時に、クライアントデバイス（コンピューターまたはモバイルデバイス）上で有効化される一連のポリシー設定に名前を付けたものです。プロファイルを有効にすると、プロファイルが有効になる前にデバイスで有効になっていたポリシー設定が修正されます。こうした設定により、プロファイルで指定された値が得られます。

ポリシーのプロファイルは、同じ管理グループ内にあるデバイスが異なるポリシー設定に従って作動可能にする場合に必要です。管理グループ内のデバイスのうち数台に対してのみ、ポリシーの設定を変更しなくてはならない状況が発生することがあります。この場合、管理グループ内の選択したデバイスに対してのみポリシーの設定を編集できるようなポリシーのプロファイルを設定できます。たとえば、管理グループ「ユーザー」内のすべてのデバイスに対して GPS ナビゲーションソフトウェアの使用を禁止するポリシーがあるとします。管理グループ「ユーザー」内に配達を行う社員が所有するデバイスが 1 台存在しており、そのデバイスでのみ GPS ナビゲーションソフトウェアを使用する必要があるとします。このデバイスに「配達担当者」のタグを付け、「配達担当者」のタグが付いたデバイスでのみ GPS ナビゲーションソフトウェアの使用が可能、それ以外のポリシーの設定はそのままとなるようにポリシーのプロファイルを再設定できます。このように設定すると、「配達担当者」というタグの付いたデバイスが管理グループ「ユーザー」に出現すると、そのデバイスでは GPS ナビゲーションソフトウェアの使用が許可されるようになります。管理グループ「ユーザー」内の「配達担当者」のタグが付いていない他のデバイスでは、GPS ナビゲーションソフトウェアの使用は禁止されたままとなります。

プロファイルは、以下のポリシーでのみサポートされます：

- Kaspersky Endpoint Security for Windows のポリシー
- Kaspersky Endpoint Security for Mac のポリシー
- Kaspersky Mobile Device Management プラグインのバージョン 10 Service Pack 1 から 10 Service Pack 3 Maintenance Release 1 までのポリシー
- Kaspersky Device Management for iOS プラグインのポリシー
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows のポリシー
- Kaspersky Security for Virtualization 5.1 Light Agent for Linux のポリシー

ポリシーのプロファイルは、ポリシーを適用するクライアントデバイスの管理を簡略化します：

- ポリシーのプロファイルの設定は、ポリシーの設定と変えることができます。
- いくつかの設定のみ異なる単一のポリシーの複数のインスタンスを維持および手動で適用する必要がありません。
- モバイルユーザーに個別のポリシーを割り当てる必要がありません。
- ポリシーのプロファイルはエクスポートとインポートが可能です。また、既存のポリシーのプロファイルを使用して新しいものを作成できます。
- 1 個のポリシー内に、複数のアクティブポリシーのプロファイルを作成できます。デバイスに適用されるプロファイルは、そのデバイスで有効な有効化ルールを満たすもののみです。
- プロファイルには、ポリシーの階層が存在します。継承されたすべてのポリシーは、より上位のポリシーのすべてのプロファイルを含みます。

プロファイルの優先度

ポリシー向けに作成されたプロファイルは、優先度の降順でソートされます。たとえば、プロファイルのリストで、プロファイル「X」がプロファイル「Y」よりも上に位置している場合、「X」が「Y」よりも優先度が高いということになります。1台のデバイスに複数のプロファイルを同時に適用できます。プロファイル間で設定値が異なる場合、優先度の最も高いプロファイルの値がデバイスに適用されます。

プロファイルの有効化ルール

ポリシーのプロファイルは、有効化ルールが適合すると、クライアントデバイスで有効になります。［*有効化ルール*］は、デバイスでポリシーのプロファイルを開始するために満たす必要がある一連の条件です。有効化ルールには、次の条件を指定することができます：

- クライアントデバイス上のネットワークエージェントが、特定の接続パラメータ（サーバーアドレス、ポート番号など）の管理サーバーと接続する。
- クライアントデバイスはオフラインである。
- クライアントデバイスに特定のタグが割り当てられている。
- クライアントデバイスが明示的（デバイスは直接指定のユニットに配置される）または暗示的（デバイスはすべてのネストレベルで指定のユニット内にあるいずれかのユニットに配置される）に Active Directory の指定のユニットに配置されている、デバイスまたはその所有者が Active Directory のセキュリティグループに配置されている。
- クライアントデバイスが特定の所有者のものであるか、デバイスの所有者が Kaspersky Security Center の内部セキュリティグループに含まれている。
- クライアントデバイスの所有者に特定のロールが割り当てられている。

管理グループの階層におけるポリシー

下位の管理グループ内にポリシーを作成する場合、このポリシーは、より上位のグループのアクティブポリシーのプロファイルを継承します。同じ名前のプロファイルは統合されます。より上位のグループに対するポリシーのプロファイルは、優先度もより高くなります。たとえば、管理グループ「*A*」で、ポリシー「*P（A）*」にはプロファイル「*X1*」「*X2*」「*X3*」（優先度降順）があるとします。管理グループ「*B*」（グループ「*A*」のサブグループ）では、ポリシー「*P（B）*」が、プロファイル「*X2*」「*X4*」「*X5*」とともに作成されているとします。ポリシー「*P（B）*」は「*P（A）*」によって修正され、ポリシー「*P（B）*」のプロファイルのリストが次のように表示されます：「*X1*」「*X2*」「*X3*」「*X4*」「*X5*」（優先度降順）。プロファイル「*X2*」の優先度は、ポリシー「*P（B）*」の「*X2*」の初期の状態に、ポリシー「*P（A）*」の「*X2*」の初期の状態に、それぞれ依存します。「*P（B）*」の作成後は、「*P（A）*」はサブグループ「*B*」に表示されなくなります。

アクティブポリシーの内容は、ネットワークエージェントの起動時、オフラインモードを有効および無効にした時、またはクライアントデバイスに割り当てたタグのリストの編集時に、毎回再計算されます。たとえば、デバイスの RAM サイズを増加すると、その後、大容量 RAM のデバイスに適用されるポリシーのプロファイルがそのデバイスで有効になります。

ポリシーのプロファイルのプロパティと制限

プロファイルには次の特徴があります：

- 非アクティブポリシーのプロファイルは、クライアントデバイスに影響を与えません。

- ポリシーに「**モバイルユーザーポリシー**」ステータスが指定されている場合、そのポリシーのプロファイルもデバイスが企業ネットワークから切断された時にのみ適用されます。
- プロファイルは、実行ファイルへのアクセスの静的分析をサポートしません。
- ポリシーのプロファイルにイベント通知の設定を含めることはできません。
- デバイスを管理サーバーへ接続する際に UDP ポート 15000 が使用される場合、デバイスにタグを付けてから 1 分以内に、対応するポリシーのプロファイルが有効になります。
- プロファイルの有効化ルールの作成時には、管理サーバーへのネットワークエージェントの接続ルールを使用できます。

ポリシーのプロファイルの作成

プロファイルの作成は次のアプリケーションのポリシーでのみ実行できます：

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows 以降
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac
- Kaspersky Mobile Device Management プラグインのバージョン 10 Service Pack 1 から 10 Service Pack 3 Maintenance Release 1 まで
- Kaspersky Device Management for iOS プラグイン
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows および Kaspersky Security for Virtualization 5.1 Light Agent for Linux

ポリシーのプロファイルを作成するには：

1. コンソールツリーで、プロファイルを作成する必要があるポリシーの管理グループを選択します。
2. 管理グループの作業領域で、［**ポリシー**］タブを選択します。
3. ポリシーを選択し、コンテキストメニューを使用して、ポリシーのプロパティウィンドウに切り替えます。
4. ポリシーのプロパティウィンドウで［**ポリシーのプロファイル**］セクションを開き、［**追加**］をクリックします。

   新規ポリシープロファイルウィザードが起動します。
5. ウィザードの［**ポリシーのプロファイル名**］ウィンドウで次を指定します：

   a. ポリシーのプロファイル名

      プロファイル名を 100 文字以上にすることはできません。

   b. ポリシープロファイルのステータス（*有効*または*無効*）。

      ポリシープロファイルの有効化の設定、条件の指定を完全に終了した後にのみ、非アクティブなポリシープロファイルを作成および有効化することを推奨します。
6. ［**新規ポリシープロファイルウィザードの終了後、ポリシープロファイルの有効化ルールの設定に進む**］をオンにして、新規ポリシープロファイル有効化ルールウィザードを起動します。ウィザードの指示に従

います。

7. ポリシープロファイルのプロパティウィンドウで、必要に応じてポリシープロファイルの設定を編集します。

8. ［**OK**］をクリックして変更内容を保存します。
   プロファイルが保存されます。プロファイルは、有効化ルールの条件を満たすデバイスで有効になります。

1つのポリシーに対して複数のプロファイルを作成できます。ポリシー用に作成されたプロファイルが、ポリシーのプロパティの［**ポリシーのプロファイル**］セクションに表示されます。ポリシーのプロファイルとプロファイルの優先順位を変更したり、プロファイルを削除できます。

ポリシーのプロファイルの編集

ポリシーのプロファイルにおける設定の編集

ポリシーのプロファイルの編集機能は、Kaspersky Endpoint Security for Windows のポリシーにのみ使用可能です。

ポリシーのプロファイルを変更するには：

1. コンソールツリーで、ポリシーのプロファイルを変更する必要がある管理グループを選択します。

2. グループの作業領域で、［**ポリシー**］タブを選択します。

3. ポリシーを選択し、コンテキストメニューを使用して、ポリシーのプロパティウィンドウに切り替えます。

4. ポリシーのプロパティで［**ポリシーのプロファイル**］セクションを開きます。
   このセクションには、ポリシー用に作成したプロファイルのリストがあります。プロファイルは、その優先度に従ってリストに表示されます。

5. ポリシーのプロファイルを選択し、［**プロパティ**］をクリックします。

6. プロパティウィンドウでプロファイルを設定します。

   - 必要に応じて、［**全般**］セクションでプロファイル名を変更し、［**プロファイルの有効化**］を使用してプロファイルを有効または無効にします。
   - ［**有効化ルール**］セクションでは、プロファイルの有効化ルールを編集できます。
   - 該当するセクションでポリシーの設定を編集します。

7. ［**OK**］をクリックします。

デバイスが管理サーバーと同期した後（ポリシーのプロファイルが有効な場合）、または有効化ルールが適合した時（ポリシーのプロファイルが無効な場合）、変更した設定が有効になります。

ポリシーのプロファイルにおける優先度の変更

ポリシーのプロファイルの優先度は、クライアントデバイスでのプロファイルの有効化の順番を定義します。同一の有効化ルールが異なるポリシーのプロファイルに設定されている場合、優先度が使用されます。

たとえば、*プロファイル1*と*プロファイル2*の2つのポリシープロファイルが作成されたとします。これらのプロファイルは、1つの設定における値が異なります（*値1*および*値2*）。*プロファイル1*の優先度が*プロファイル2*の優先度より高いとします。また、*プロファイル2*よりも優先度が低いプロファイルもあります。これらのプロファイルの有効化ルールは、同一です。

有効化ルールが適合すると、*プロファイル1*が有効になります。デバイスの設定では、*値1*が適用されます。*プロファイル1*を削除すると、*プロファイル2*が最も高い優先度となり、設定では*値2*が得られます。

ポリシープロファイルのリストでは、プロファイルが各優先度に従って表示されます。最も高い優先度のプロファイルが1番最初にランクされます。プロファイルの優先度は上矢印（  ）ボタンや下矢印（  ）ボタンを押すと変更できます。

ポリシーのプロファイルの削除

ポリシーのプロファイルを削除するには：

1. コンソールツリーで、ポリシーのプロファイルを削除する管理グループを選択します。
2. 管理グループの作業領域で、［**ポリシー**］タブを選択します。
3. ポリシーを選択し、コンテキストメニューを使用して、ポリシーのプロパティウィンドウに切り替えます。
4. Kaspersky Endpoint Security のポリシーのプロパティで、［**ポリシーのプロファイル**］セクションを開きます。
5. 削除するポリシーのプロファイルを選択し、［**削除**］をクリックします。

ポリシーのプロファイルが削除されます。有効ステータスは、デバイス上で有効化ルールが適合する別のポリシープロファイルか、元のポリシーに移ります。

ポリシーのプロファイルの有効化ルールの作成

ポリシーのプロファイルの有効化ルールを作成するには：

1. コンソールツリーで、ポリシーのプロファイルを作成する管理グループを選択します。
2. グループの作業領域で、［**ポリシー**］タブを選択します。
3. ポリシーを選択し、コンテキストメニューを使用して、ポリシーのプロパティウィンドウに切り替えます。
4. ポリシーのプロパティウィンドウで［**ポリシーのプロファイル**］セクションを選択します。
5. 有効化ルールを作成するポリシープロファイルを選択して、［**プロパティ**］をクリックします。
   ポリシーのプロファイルのプロパティウィンドウが開きます。
   ポリシープロファイルのリストが空の場合は、ポリシーのプロファイルを作成できます。
6. ［**有効化ルール**］セクションを選択し、［**追加**］をクリックします。
   新規ポリシープロファイル有効化ルールウィザードが起動します。

7. ［**ポリシープロファイル有効化ルール**］ウィンドウで、作成しているポリシープロファイルの有効化に作用する条件に隣接するチェックボックスをオンにします：

- **ポリシープロファイルの有効化に対する全般ルール**

  このチェックボックスをオンにすると、デバイスのオフラインモードのステータス、管理サーバーへの接続ルール、デバイスに割り当てられているタグに応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

- **Active Directory 使用のルール**

  このチェックボックスをオンにすると、Active Directory 組織単位（OU）内にデバイスが属しているか、または Active Directory セキュリティグループにデバイス（またはその所有者）が属しているかに応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

- **特定のデバイス所有者向けのルール**

  このチェックボックスをオンにすると、デバイスの所有者に応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

- **ハードウェア仕様のルール**

  このチェックボックスをオンにすると、メモリサイズと論理プロセッサの数に応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

ウィザードで表示されるウィンドウ数は、最初のステップで選択した設定によります。ポリシープロファイルの有効化ルールは後で変更することができます。

8. ［**全般条件**］ウィンドウで、次の設定を指定します：

- ［**オフラインのデバイス**］のドロップダウンリストで、ネットワーク上のデバイスの有無に関する条件を指定します：

  - **はい**

    デバイスは外部ネットワーク内にあるため、管理サーバーは使用できません。

  - **いいえ**

    デバイスはネットワーク内にあるため、管理サーバーを使用できます。

  - **値を選択しない**

    基準は適用されません。

- 管理サーバー接続ルールがデバイス上で実行済みまたは未実行の場合、［**デバイスが指定されたネットワークの場所に存在**］で、ドロップダウンリストを使用してポリシープロファイルの有効化を設定します。

  - **実行済み / 未実行**

ポリシーのプロファイルを有効化する条件（ルールが実行されるかどうか）

- **ルール名**

  管理サーバーへの接続に関するデバイスのネットワークロケーションの説明。ポリシープロファイルを有効にするためにネットワークロケーションの説明の条件を満たす（または満たさない）必要があります。

  管理サーバーへの接続に関するデバイスのネットワークロケーションの説明は、ネットワークエージェント切り替えルールで作成または設定できます。

［**ポリシープロファイルの有効化に対する全般ルール**］をオンにすると、［**全般条件**］ウィンドウが表示されます。

9. ［**タグを使用している条件**］ウィンドウで、次の設定を指定します：

   - **タグリスト**

     このタグのリストで、目的のタグのチェックボックスをオンにすると、ポリシーのプロファイルにデバイスを含めるためのルールを指定できます。

     リストの上のフィールドに新しいタグを入力して、［**追加**］をクリックすると、新しいタグをリストに追加できます。

     選択したタグのすべてを説明に含むデバイスがポリシーのプロファイルに含まれます。チェックボックスをオフにすると、基準は適用されません。既定では、これらのチェックボックスはオフです。

   - **指定したタグのないデバイスに適用する**

     タグの選択状態を反転させる必要がある場合は、このオプションをオンにします。

     このオプションをオンにすると、選択されたタグのいずれも説明に含まないデバイスがポリシープロファイルに含まれます。このオプションをオフにすると、基準が適用されません。

     既定では、このオプションはオフです。

［**タグを使用している条件**］ウィンドウは、［**ポリシープロファイルの有効化に対する全般ルール**］をオンにすると表示されます。

10. ［**Active Directory を使用した条件**］ウィンドウで、次の設定を指定します：

    - **デバイス所有者が属している Active Directory セキュリティグループ**

      このオプションを有効にすると、所有者が指定されたセキュリティグループに所属しているデバイスで、ポリシーのプロファイルが有効化されます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

    - **デバイスが属している Active Directory セキュリティグループ**

      このオプションを有効にすると、デバイスでポリシープロファイルが有効化されます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **デバイスが割り当てられている Active Directory 組織単位**

  このオプションを有効にすると、指定された Active Directory 組織単位（OU）に属するデバイスで、ポリシーのプロファイルが有効化されます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。

  既定では、このオプションはオフです。

［**Active Directory 使用のルール**］をオンにすると、［**Active Directory を使用した条件**］ウィンドウが表示されます。

11. ［**デバイス所有者を使用した条件**］ウィンドウで、次の設定を指定します：

- **デバイスの所有者**

  このオプションをオンにして、デバイスの所有者に応じたプロファイルの有効化ルールを設定を有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

  - デバイスが特定の所有者のものである（「=」記号）
  - デバイスが特定の所有者のものでない（「#」記号）

    このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。このオプションをオンにすると、デバイスの所有者を指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **デバイスの所有者が属する内部セキュリティグループ**

  このオプションをオンにして、デバイスの所有者の Kaspersky Security Center の内部セキュリティグループの所属に応じたプロファイルの有効化ルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

  - デバイスの所有者が特定のセキュリティグループのメンバーである（「=」記号）
  - デバイスの所有者が特定のセキュリティグループのメンバーでない（「?」記号）

    このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。Kaspersky Security Center のセキュリティグループを指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **デバイス所有者のロールに応じてポリシープロファイルを有効化する**

  このオプションをオンにすると、デバイスの所有者のロールに応じたプロファイルの有効化ルールを設定し、オンにすることができます。既存のロールのリストからロールを手動で選択して追加します。

  このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。

［**デバイス所有者を使用した条件**］ウィンドウは、［**特定のデバイス所有者向けのルール**］をオンにすると表示されます。

12. ［**機器の特性を使用した条件**］ウィンドウで、次の設定を指定します：

- **RAM サイズ（MB）**

  このオプションをオンにして、デバイスで使用可能な RAM サイズに応じたプロファイルの有効化のルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

  - デバイスの RAM サイズは指定された値以下である（「<」記号）。
  - デバイスの RAM サイズは指定された値以上である（「>」記号）。

  このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。デバイスの RAM ボリュームを指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **論理プロセッサの数**

  このオプションをオンにして、デバイスの論理プロセッサの数に応じたプロファイルの有効化ルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

  - デバイスの論理プロセッサの数は指定された値以下である（「<」記号）。
  - デバイスの論理プロセッサの数は指定された値以上である（「>」記号）。

  このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。デバイス上の論理プロセッサの数を指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

［**ハードウェア仕様のルール**］をオンにすると、［**機器の特性を使用した条件**］ウィンドウが表示されます。

13. ［**ポリシープロファイル有効化ルールの名前**］ウィンドウの［**ルール名**］で、ルールの名前を指定します。

プロファイルが保存されます。プロファイルは、有効化ルールが適合すると、デバイスで有効になります。

プロファイル用に作成したポリシープロファイルの有効化ルールが、［**有効化ルール**］セクションのポリシープロファイルのプロパティに表示されます。ポリシープロファイルの有効化ルールはいずでも変更または削除することができます。

複数の有効化ルールを同時に適合させることができます。

デバイス移動ルール

*デバイス移動ルール*を使用して、管理グループにデバイスへの割り当てを自動化することを推奨します。デバイス移動ルールは、3 つのメイン部分から構成されます：それは、名前、実行条件（デバイス属性を使用した論理式）、および対象管理グループです。デバイス属性がルールの実行条件を満たしている場合は、このルールによりデバイスが対象管理グループに移動されます。

デバイス移動ルールにはすべて優先度が設定されています。管理サーバーは優先度の昇順に従って、デバイス属性が各ルールの実行条件を満たしているかどうかを確認します。デバイス属性がルールの実行条件を満たしている場合、そのデバイスは対象グループに移動され、このデバイスに対するルール処理が完了します。デバイス属性が複数のルールの条件を満たしている場合、そのデバイスは優先度が最も高いルールの対象グループに移動されます（つまり、ルールのリスト内で最高ランク）。

デバイス移動ルールは暗黙的に作成できます。たとえば、インストールパッケージまたはリモートインストールタスクのプロパティで、ネットワークエージェントをデバイスにインストールした後にそのデバイス移動先の管理グループを指定できます。さらに、移動ルールのリスト内で Kaspersky Security Center の管理者が、デバイス移動ルールを明示的に作成できます。このリストは、管理コンソールの［**未割り当てデバイス**］グループのプロパティ内に置かれています。

既定では、デバイス移動ルールは、管理グループに対してデバイスを最初にワンタイムで割り当てることを目的としています。このルールにより、［**未割り当てデバイス**］グループから一度だけデバイスが移動されます。デバイスがこのルールによって一度移動されている場合は、デバイスを手動で［**未割り当てデバイス**］グループに戻したとしても、このデバイスが再度移動されることはありません。これは移動ルールを適用する際に推奨される方法です。

一部の管理グループに割り当て済みであるデバイスを移動できます。これを実行するには、ルールのプロパティで［**どの管理グループにも属していないデバイスのみ移動する**］をオフにします。

一部の管理グループに割り当て済みのデバイスに対して移動ルールを適用すると、管理サーバーの負荷が大幅に増大します。

［**どの管理グループにも属していないデバイスのみ移動する**］は、自動的に作成された移動ルールのプロパティでロックされています。このようなルールは、［*アプリケーションをリモートでインストールする*］タスクを追加するか、スタンドアロンインストールパッケージを作成する時に作成されます。

単一のデバイスに繰り返し適用される移動ルールを作成することができます。

単一のデバイスをあるグループから別のグループに繰り返し移動させないでください（たとえば、該当するデバイスに特別なポリシーを適用するために、特別なグループタスクを実行するか、または特定のディストリビューションポイントを使用してデバイスをアップデートする）。

このような処理は、管理サーバーとネットワークのトラフィックの負荷を極端に増大させるため、サポートされていません。また、Kaspersky Security Center の操作原理と競合する可能性もあります（特に、アクセス権限、イベント、レポートの分野において）。ポリシーのプロファイル、デバイスの抽出のタスク、標準シナリオに従ったネットワークエージェントの割り当てなどを使用して、別のソリューションを見つける必要があります。

デバイス移動ルールの複製

デバイス移動ルールを、ほとんど同じ設定で複数作成する必要がある場合、既存のルールを複製してから設定を変更できます。この操作は、デバイス移動ルールを、IP アドレス範囲と対象グループだけ変更してそれ以外は同一の設定で複数作成しなければいけない場合などに便利です。

デバイス移動ルールを複製するには：

1. メインウィンドウを開きます。

2. ［**未割り当てデバイス**］フォルダーで、［**ルールの設定**］をクリックします。
   ［**プロパティ：割り当てデバイス**］ウィンドウが表示されます。

3. ［**デバイスの移動**］セクションで、複製するデバイス移動ルールを選択します。

4. ［**ルールの複製**］をクリックします。

   選択したデバイス移動ルールが複製され、リストの末尾に追加されます。

新しく作成されたルールは既定では無効になっています。ルールはいつでも編集したり、有効にすることができます。

ソフトウェアのカテゴリ分け

アプリケーションの実行状態を監視する主なツールは、*カスペルスキーのカテゴリ*です（以下、*KL カテゴリ*と表記）。KL カテゴリを使用することで、Kaspersky Security Center 管理者によるソフトウェアのカテゴリ分けのサポートを簡略化でき、管理対象デバイスへのトラフィックを最小化できます。

アプリケーションカテゴリは、既存の KL カテゴリのいずれかには分類できないアプリケーションに対してのみ作成する必要があります（たとえば、カスタムメイドソフトウェア用）。また、アプリケーションカテゴリは、アプリケーションのインストールパッケージ（MSI）またはインストールパッケージの置かれているフォルダーに基づいて作成されます。

KL カテゴリによりカテゴリ化されていない大規模セットのソフトウェアが提供されている場合は、自動的に更新されるカテゴリを作成するのが便利です。実行ファイルのチェックサムは、配布パッケージを含むフォルダーが変更されるたびに、自動的にこのカテゴリに追加されます。

My Documents、%windir%、%ProgramFiles%、および %ProgramFiles(x86)% フォルダーに対して、ソフトウェアの自動アップデートカテゴリを作成しないでください。これらのフォルダーにあるファイルのプールは頻繁に変更する必要がありますが、これにより管理サーバーの負荷とネットワークのトラフィックが増大します。この場合、一連のソフトウェアを格納する専用フォルダーを作成し、このフォルダーに定期的に新しい項目を追加する必要があります。

クライアント組織のデバイスにアプリケーションをインストールする場合の前提条件

クライアント組織のデバイスにアプリケーションをリモートインストールするプロセスは、企業内でのリモートインストールプロセスと同じです。

クライアント組織のデバイス上にアプリケーションをインストールするには、次を実行する必要があります：

- クライアント組織のデバイス上に、アプリケーションをインストールする前にネットワークエージェントをインストールします。

  ネットワークエージェントのインストールパッケージを Kaspersky Security Center のサービスプロバイダーが設定する場合は、インストールパッケージのプロパティウィンドウで次の設定を指定します：

  - ［**接続**］セクションの［**管理サーバー**］で、ディストリビューションポイントにネットワークエージェントをローカルでインストールする時に指定した仮想管理サーバーのアドレスを指定します。

- ［**詳細**］セクションで、［**接続ゲートウェイを使用して管理サーバーに接続する**］をオンにします。［**接続ゲートウェイアドレス**］で、ディストリビューションポイントのアドレスを指定します。デバイスの IP アドレスまたは Windows ネットワークでのデバイス名を使用できます。

- ネットワークエージェントインストールパッケージのダウンロード方法として、［**ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**］をオンにします。ダウンロード方法は次の手順で選択します：

  - リモートインストールタスクを使用してアプリケーションをインストールする場合は、以下のいずれかの方法でダウンロード方法を指定できます：

    - リモートインストールタスクの作成時に［**設定**］ウィンドウで選択

    - リモートインストールタスクのプロパティウィンドウの［**設定**］セクションで選択

  - リモートインストールウィザードを用いてアプリケーションをインストールする場合は、このウィザードの［**設定**］ウィンドウでダウンロード方法を選択できます。

- ディストリビューションポイントのデバイスで使用するアカウントには、すべてのクライアントデバイスの Admin$ へのアクセス権が必要です。

ローカルアプリケーション設定の表示と変更

Kaspersky Security Center の管理システムでは、管理コンソールを使用して、デバイス上のローカルアプリケーション設定をリモート管理できます。

*ローカルアプリケーション*設定は、デバイス固有のアプリケーション設定です。Kaspersky Security Center を使用すると、管理グループに含まれるデバイスのローカルアプリケーション設定を指定できます。

カスペルスキー製品の詳細については、各製品のガイドを参照してください。

アプリケーションのローカル設定を表示または変更するには：

1. 目的のデバイスが属するグループの作業領域で、［**デバイス**］タブを選択します。

2. デバイスのプロパティウィンドウの［**アプリケーション**］セクションで、関連するアプリケーションを選択します。

3. アプリケーション名をダブルクリックするか、［**プロパティ**］をクリックして、アプリケーションのプロパティウィンドウを開きます。

   選択したアプリケーションのローカル設定ウィンドウが開き、それらの設定を表示および編集できます。

グループポリシーによって変更がブロックされていない設定（ポリシーで鍵アイコン（🔒）が付いていない設定）の値を変更できます。

Kaspersky Security Center と管理対象アプリケーションのアップデート

このセクションでは Kaspersky Security Center と管理対象アプリケーションのアップデートに必要となる手順について説明します。

シナリオ：定義データベースとカスペルスキー製品の定期的なアップデート

このセクションでは、定義データベース、ソフトウェアモジュール、カスペルスキー製品の定期的なアップデートを行う手順について説明します。ネットワーク保護の設定手順の完了後、管理サーバーと管理対象デバイスがウイルス、ネットワーク攻撃、フィッシング攻撃などの様々な脅威から常に保護されるよう、保護システムの信頼性を維持する必要があります。

ネットワーク保護を最新の状態に維持する定期的なアップデートは次の通りです：

- 定義データベースとソフトウェアモジュール
- インストール済みのカスペルスキー製品（Kaspersky Security Center コンポーネントとセキュリティ製品を含む）

この手順を完了すると、次の状態を実現できます：

- ネットワークが最新のカスペルスキー製品（Kaspersky Security Center コンポーネントとセキュリティ製品を含む）で保護されている。
- ネットワークのセキュリティレベルにとって重要な定義データベースとその他のカスペルスキーのデータベースが常に最新である。

必須条件

管理対象デバイスが管理サーバーに接続している必要があります。接続していない場合は、定義データベース、ソフトウェアモジュール、カスペルスキー製品の手動アップデート、またはカスペルスキーのアップデートサーバーからの直接アップデートを検討してください。

管理サーバーはインターネットに接続している必要があります。

導入を開始する前に、次が完了していることを確認してください：

1. Kaspersky Security Center Web コンソールを使用したカスペルスキー製品の導入手順に従って、カスペルスキーのセキュリティ製品を管理対象デバイスに導入した。
2. ネットワーク保護の設定手順に従って、必要なすべてのポリシー、ポリシーのプロファイル、タスクを作成して設定した。
3. 管理対象デバイスの数とネットワークトポロジーに従って、適切な数のディストリビューションポイントを割り当てた。

定義データベースとカスペルスキー製品のアップデート手順は次の通りです：

1 アップデートスキームの選択

Kaspersky Security Center コンポーネントとセキュリティ製品に対するアップデートのインストールには、複数のスキームを使用できます。ネットワークの要件に最も合致するスキームを選択してください（複数のスキームを組み合わせることもできます）。

2 ［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの作成

このタスクは、Kaspersky Security Center のクイックスタートウィザードによって自動的に作成されます。ウィザードを実行していない場合は、次の手順に進む前にタスクを作成してください。

カスペルスキーのアップデートサーバーから管理サーバーのリポジトリへのアップデートのダウンロード、および定義データベースと Kaspersky Security Center のソフトウェアモジュールのアップデートには、このタスクが必要です。アップデートのダウンロード後、管理対象デバイスにこれらのアップデートを配信できます。

ネットワークにディストリビューションポイントが割り当てられている場合、アップデートは管理サーバーのリポジトリからディストリビューションポイントのリポジトリに自動的にダウンロードされます。この場合、ディストリビューションポイントの範囲に含まれる管理対象デバイスは、管理サーバーのリポジトリではなくディストリビューションポイントのリポジトリからアップデートをダウンロードします。

実行手順の説明：

- 管理コンソール：［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの作成
- Kaspersky Security Center Web コンソール：管理サーバーのリポジトリへのアップデートのダウンロードタスクの作成

3 ［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの作成（オプション）

既定では、管理サーバーからディストリビューションポイントにアップデートがダウンロードされます。カスペルスキーのアップデートサーバーからディストリビューションポイントにアップデートを直接ダウンロードするように Kaspersky Security Center を設定できます。ディストリビューションポイントのリポジトリへのダウンロードが推奨されるのは、管理サーバーとディストリビューションポイント間の通信の方がディストリビューションポイントとカスペルスキーのアップデートサーバー間の通信よりも費用がかかる場合や、管理サーバーがインターネットにアクセスできない場合などです。

ネットワークにディストリビューションポイントが割り当てられており、*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクが作成されている場合、ディストリビューションポイントは、管理サーバーのリポジトリではなくカスペルスキーのアップデートサーバーからアップデートをダウンロードします。

実行手順の説明：

- 管理コンソール：ディストリビューションポイントのリポジトリにアップデートをダウンロードタスクの作成
- Kaspersky Security Center Web コンソール：ディストリビューションポイントのリポジトリにアップデートをダウンロードタスクの作成

4 ディストリビューションポイントの設定

ネットワークにディストリビューションポイントが割り当てられている場合、設定が必要なすべてのディストリビューションポイントのプロパティで［**アップデートの配信**］がオンになっていることを確認します。ディストリビューションポイントでこのオプションがオフになっていると、ディストリビューションポイントの範囲に含まれるデバイスは管理サーバーのリポジトリからアップデートをダウンロードします。

管理対象デバイスがディストリビューションポイントからのみアップデートを受信するようにする場合は、ネットワークエージェントポリシーで［**ディストリビューションポイント経由でのみファイルを配信する**］をオンにします。

5 オフライン方式のアップデートのダウンロードまたは差分ファイルの使用によるアップデート処理の最適化（オプション）

オフライン方式のアップデートのダウンロード（既定で有効）または差分ファイルを使用して、アップデート処理を最適化できます。これら 2 つの機能は同時に使用できないため、各ネットワークセグメントでどちらを有効にするか選択する必要があります。

オフライン方式のアップデートのダウンロードを有効にした場合、アップデートが管理サーバーのリポジトリにダウンロードされると、セキュリティ製品がアップデートを要求する前にネットワークエージェントが管理対象デバイスに必要なアップデートをダウンロードします。これによりアップデート処理の信頼性が向上します。この機能を使用するには、［**アップデートと定義データベースをあらかじめ管理サーバーからダウンロードする（推奨）**］をネットワークエージェントのポリシーでオンにします。

オフライン方式のアップデートのダウンロードを使用しない場合は、差分ファイルを使用して管理サーバーと管理対象デバイス間のトラフィックを最適化できます。この機能を有効にすると、管理サーバーまたはディストリビューションポイントは定義データベースまたはソフトウェアモジュールのファイル全体ではなく差分ファイルをダウンロードします。差分ファイルには、定義データベースファイルまたはソフトウェアモジュールファイルの異なる 2 バージョン間の変更点のみが含まれています。したがって、差分ファイルの方がファイル全体より容量が小さくなります。これにより、管理サーバーと管理対象デバイス間またはディストリビューションポイントと管理対象デバイス間のトラフィックを削減できます。この機能を使用するには、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクや、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスク、またはその両方のプロパティで［**差分ファイルのダウンロード**］をオンにします。

実行手順の説明：

- カスペルスキー製品の定義データベースとソフトウェアモジュールのアップデートでの差分ファイルの使用
- 管理コンソール：オフライン方式のアップデートのダウンロードの有効化と無効化
- Kaspersky Security Center Web コンソール：オフライン方式のアップデートのダウンロードの有効化と無効化

6 ダウンロードされたアップデートの検証（オプション）

ダウンロードされたアップデートをインストールする前に、*アップデート検証*タスクを使用してアップデートを検証できます。このタスクでは、設定で指定したテストデバイスを対象に、デバイスアップデートタスクとマルウェアスキャンタスクを順番に実行します。タスクの実行結果に基づいて、管理サーバーは残りのデバイスに対するアップデートの配信を開始またはブロックします。

*アップデート検証*タスクは、*管理サーバーのリポジトリへのアップデートのダウンロード*タスクの一部として実行できます。*管理サーバーのリポジトリへのアップデートのダウンロード*タスクのプロパティで、［**配信前にアップデートを検証する**］（管理コンソールの場合）または［**アップデートの検証の実行**］（Kaspersky Security Center Web コンソールの場合）をオンにします。

実行手順の説明：

- 管理コンソール：ダウンロードされたアップデートの検証
- Kaspersky Security Center Web コンソール：ダウンロードされたアップデートの検証

7 ソフトウェアアップデートの拒否と承認

既定では、ダウンロードされたソフトウェアアップデートのステータスは「*未定義*」です。ステータスは「*承認*」または「*拒否*」に変更できます。承認されたアップデートは常にインストールされます。使用許諾契約書の条項の確認と同意がアップデートに必要な場合は、最初に条項に同意する必要があります。その後、アップデートを管理対象デバイスに配信できます。未定義のアップデートは、ネットワークエージェントポリシーの設定に従って、ネットワークエージェントとその他の Kaspersky Security Center コンポーネントにのみインストールできます。「*拒否*」のステータスを設定したアップデートはデバイスにインストールされません。拒否に設定したセキュリティ製品のアップデートが以前にインストールされている場合、Kaspersky Security Center はすべてのデバイスからのアップデートのアンインストールを試行します。Kaspersky Security Center コンポーネントのアップデートはアンインストールできません。

実行手順の説明：

- 管理コンソール：ソフトウェアアップデートの拒否と承認
- Kaspersky Security Center Web コンソール：ソフトウェアアップデートの拒否と承認

8. **Kaspersky Security Center コンポーネントのアップデートとパッチの自動インストールの設定**

   ネットワークエージェントとその他の Kaspersky Security Center コンポーネント用にダウンロードされたアップデートとパッチは自動的にインストールされます。ネットワークエージェントのプロパティで［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオンのままにした場合、アップデートはすべて、リポジトリにダウンロードされた後に自動的にインストールされます。このオプションをオフにすると、ダウンロードされたパッチのうちステータスが「*未定義*」のものは、管理者がステータスを「*承認*」に変更しない限りインストールされません。

   実行手順の説明：

   - 管理コンソール：Kaspersky Security Center コンポーネントの自動アップデートおよびパッチ適用の有効化と無効化
   - Kaspersky Security Center Web コンソール：Kaspersky Security Center コンポーネントの自動アップデートおよびパッチ適用の有効化と無効化

9. **管理サーバーのアップデートのインストール**

   管理サーバーのソフトウェアアップデートはアップデートのステータスに依存しません。これらのアップデートは自動的にインストールされず、事前に管理コンソールの［**監視**］タブ（［**管理サーバー** <サーバー名>］→［**監視**］）または Kaspersky Security Center Web コンソールの［**通知**］セクション（［**監視とレポート**］→［**通知**］）で管理者によって承認されている必要があります。その後、管理者が明示的にアップデートのインストールを実行する必要があります。

10. **セキュリティ製品のアップデートとパッチの自動インストールの設定**

    管理対象アプリケーションの*アップデート*タスクを作成して、製品、ソフトウェアモジュール、および定義データベースをタイムリーにアップデートします。タイムリーなアップデートを確実に実行するために、タスクスケジュールの設定時に、［**新しいアップデートがリポジトリにダウンロードされ次第**］をオンにすることを推奨します。

    ネットワークに IPv6 のみのデバイスが含まれていて、それらのデバイス上にインストールされているセキュリティ製品を定期的にアップデートする場合、管理対象デバイス上にバージョン 14 以降の管理サーバーとバージョン 14 以降のネットワークエージェントがインストールされていることを確認してください。

    既定では、アップデートのステータスを*承認*に変更した後にのみ、Kaspersky Endpoint Security for Windows と Kaspersky Endpoint Security for Linux のアップデートがインストールされます。アップデートの設定は、*アップデート*タスクで変更することができます。

    使用許諾契約書の条項の確認と同意がアップデートに必要な場合は、最初に条項に同意する必要があります。その後、アップデートを管理対象デバイスに配信できます。

    実行手順の説明：

    - 管理コンソール：Kaspersky Endpoint Security のアップデートをデバイスに自動インストール
    - Kaspersky Security Center Web コンソール：Kaspersky Endpoint Security のアップデートをデバイスに自動インストール

結果

すべての手順を完了すると、管理サーバーのリポジトリまたはディストリビューションポイントのリポジトリにアップデートがダウンロードされた後で、定義データベースとインストール済みのカスペルスキー製品をアップデートするように Kaspersky Security Center が設定されます。続いて、ネットワークステータスの監視を設定できます。

定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデートの概要

管理サーバーと管理対象デバイスの保護が最新の状態であるようにするには、次の項目のタイムリーなアップデートが必要です：

- 定義データベースとソフトウェアモジュール

  Kaspersky Security Center は、カスペルスキーのデータベースとソフトウェアをダウンロードする前にカスペルスキーのサーバーがアクセス可能かどうかをチェックします。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。これは、定義データベースを最新の状態に保ち、管理対象デバイスのセキュリティレベルを確実に管理するために必要です。

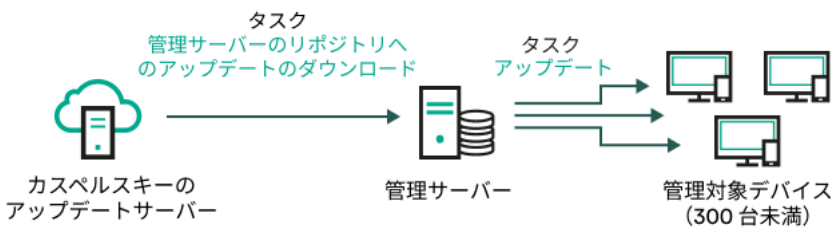
- インストール済みのカスペルスキー製品（Kaspersky Security Center コンポーネントとセキュリティ製品を含む）

ネットワークの設定に応じて、管理対象デバイスへの必要なアップデートのダウンロードと配信に次のスキームを使用できます：

- 単一のタスク［*管理サーバーのリポジトリへのアップデートのダウンロード*］の使用
- 次の 2 つのタスクの使用：
  - *［管理サーバーのリポジトリへのアップデートのダウンロード］タスク*
  - *ディストリビューションポイントのリポジトリにアップデートをダウンロードタスク*
- ローカルフォルダー、共有フォルダー、または FTP サーバーを使用して手動で実行
- カスペルスキーのアップデートサーバーから管理対象デバイスの Kaspersky Endpoint Security を直接アップデート
- 管理サーバーがインターネットに接続されていない場合は、ローカルまたはネットワークフォルダー経由

管理サーバーのリポジトリへのアップデートのダウンロードタスクの使用

このスキームでは、Kaspersky Security Center は *管理サーバーのリポジトリへのアップデートのダウンロード* タスクを使用してアップデートをダウンロードします。単一のネットワークセグメントで構成され管理対象デバイスが 300 台未満、または複数のセグメントに分かれているが各ネットワークセグメントに含まれる管理対象デバイスが 10 台未満の小規模ネットワークでは、管理サーバーのリポジトリから管理対象デバイスにアップデートが直接配信されます（次の図を参照）。

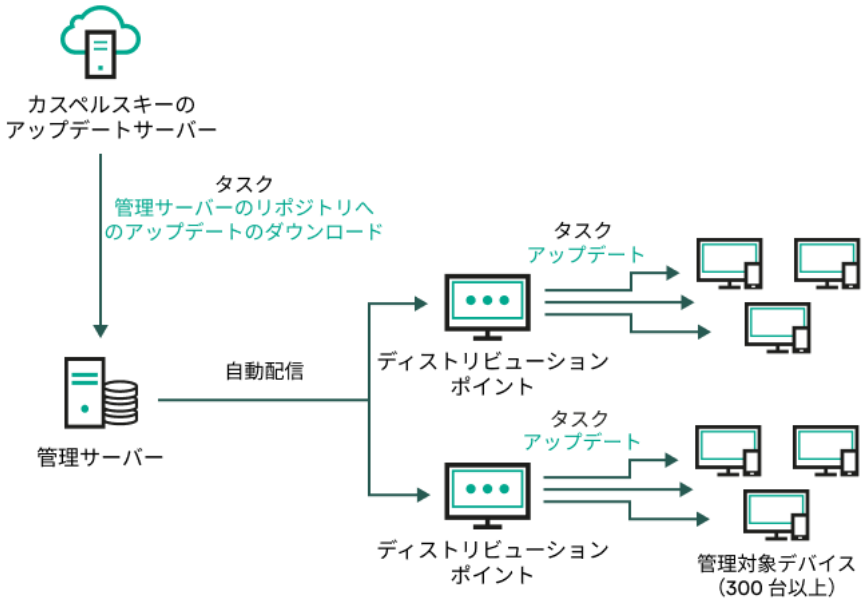


ディストリビューションポイントを使用しない、管理サーバーのリポジトリへのアップデートのダウンロードタスクによるアップデート

既定では、管理サーバーは HTTPS プロトコルを使用してカスペルスキーのアップデートサーバーに接続し、アップデートをダウンロードします。必要に応じて、管理サーバーで HTTPS プロトコルの代わりに HTTP プロトコルを使用するように設定を編集できます。

単一のネットワークセグメントで構成され管理対象デバイスが 300 台以上、または複数のセグメントに分かれていて各ネットワークセグメントに含まれる管理対象デバイスが 10 台以上のネットワークの場合は、ディストリビューションポイントを使用して管理対象デバイスにアップデートを配信することを推奨します（次の図を参照）。ディストリビューションポイントは管理サーバーの負荷を低減し、管理サーバーと管理対象デバイス間のトラフィックを最適化します。ネットワークに必要なディストリビューションポイントの数と設定を計算できます。

このスキームでは、アップデートは管理サーバーのリポジトリからディストリビューションポイントのリポジトリに自動的にダウンロードされます。ディストリビューションポイントの範囲に含まれる管理対象デバイスは、管理サーバーのリポジトリではなくディストリビューションポイントのリポジトリからアップデートをダウンロードします。



ディストリビューションポイントを使用した、管理サーバーのリポジトリへのアップデートのダウンロードタスクによるアップデート

*管理サーバーのリポジトリへのアップデートのダウンロード*タスクが完了すると、管理サーバーのリポジトリに次のアップデートがダウンロードされます：

- 定義データベースと Kaspersky Security Center のソフトウェアモジュール

  これらのアップデートは自動的にインストールされます。

- 管理対象デバイスのセキュリティ製品用の定義データベースとソフトウェアモジュール

  これらのアップデートは、Kaspersky Endpoint Security for Windows のアップデートタスクを使用してインストールされます。

- 管理サーバー用のアップデート

  これらのアップデートは自動的にインストールされません。管理者が明示的にアップデートのインストールを承認して実行する必要があります。

  管理サーバーへのパッチのインストールにはローカル管理者権限が必要です。

- Kaspersky Security Center のコンポーネント用のアップデート

既定では、これらのアップデートは自動的にインストールされます。ネットワークエージェントポリシーで設定を変更できます。

- セキュリティ製品用のアップデート

  既定では、Kaspersky Endpoint Security for Windows はこれらの承認されたアップデートのみをインストールします（管理コンソールまたは Kaspersky Security Center Web コンソールを使用してアップデートを承認できます）。アップデートは*アップデート*タスクを使用してインストールされ、このタスクのプロパティで設定することができます。

仮想管理サーバーでは［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクは利用できません。仮想管理サーバーのリポジトリには、プライマリ管理サーバーにダウンロードされたアップデートが表示されます。

テストデバイスを指定してアップデートの動作とエラーが検証されるように設定できます。検証に成功すると、アップデートが他の管理対象デバイスに配信されます。

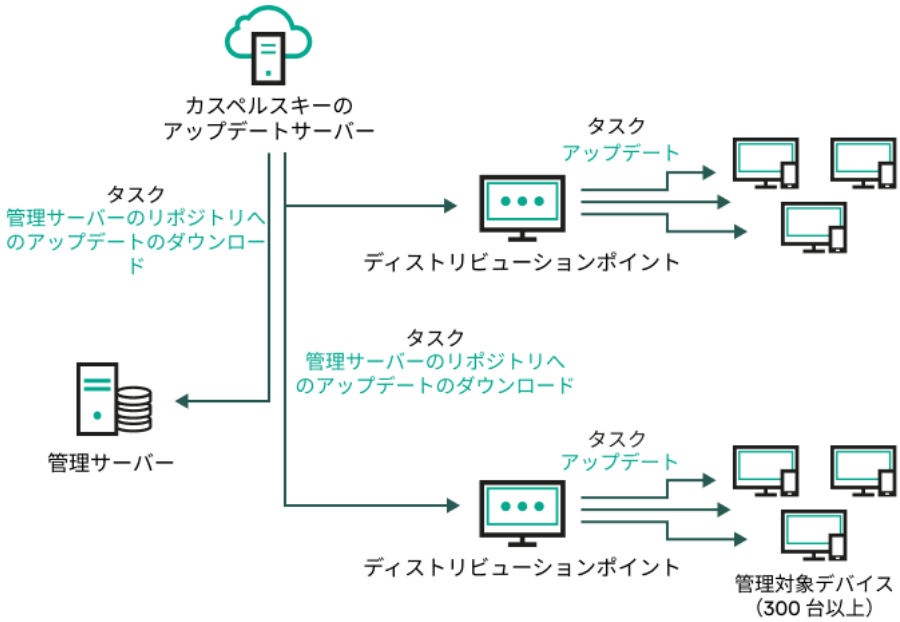
各カスペルスキー製品は、管理サーバーに必要なアップデートを要求します。管理サーバーはこれらの要求を集計した上で、いずれかの製品で要求されたアップデートのみをダウンロードします。これにより、同一のアップデートが複数回ダウンロードされたり、不必要なアップデートがダウンロードされることを防ぐことができます。［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを実行中、関連するバージョンの定義データベースとソフトウェアモジュールを確実にダウンロードする目的で、次の情報が管理サーバーからカスペルスキーのアップデートサーバーに自動的に送信されます：

- 製品 ID およびバージョン
- アプリケーションのインストール ID
- 現在のライセンス ID
- ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの実行 ID

送信される情報には、個人データや機密データは含まれません。カスペルスキーでは、法律で定められた要件に従って情報を保護しています。

2 つのタスク（［管理サーバーのリポジトリへのアップデートのダウンロード］タスクおよび［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスク）の使用

管理サーバーのリポジトリを経由させずに、カスペルスキーのアップデートサーバーからディストリビューションポイントのリポジトリにアップデートを直接ダウンロードして、管理対象デバイスにアップデートを配信できます（次の図を参照）。ディストリビューションポイントのリポジトリへのダウンロードが推奨されるのは、管理サーバーとディストリビューションポイント間の通信の方がディストリビューションポイントとカスペルスキーのアップデートサーバー間の通信よりも費用がかかる場合や、管理サーバーがインターネットにアクセスできない場合などです。



管理サーバーのリポジトリへのアップデートのダウンロードタスクおよびディストリビューションポイントのリポジトリにアップデートをダウンロードタスクによるアップデート

既定では、管理サーバーとディストリビューションポイントは HTTPS プロトコルを使用してカスペルスキーのアップデートサーバーに接続し、アップデートをダウンロードします。必要に応じて、管理サーバー、ディストリビューションポイント、またはその両方で HTTPS プロトコルの代わりに HTTP プロトコルを使用するように設定を編集できます。

このスキームを実装するには、*［管理サーバーのリポジトリへのアップデートのダウンロード］*タスクに加えて *［ディストリビューションポイントのリポジトリにアップデートをダウンロード］*タスクを作成します。その後、ディストリビューションポイントは、管理サーバーのリポジトリではなくカスペルスキーのアップデートサーバーからアップデートをダウンロードします。

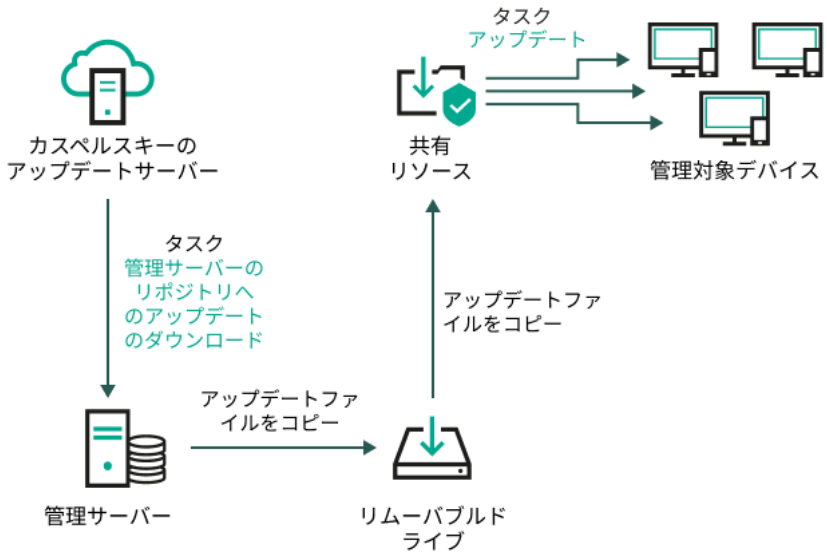
macOS を実行しているディストリビューションポイントデバイスでは、カスペルスキーのアップデートサーバーからアップデートをダウンロードできません。

*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクの対象範囲に macOS を実行しているデバイスが 1 台以上含まれている場合、すべての Windows デバイスでタスクが正常に完了した場合でも、タスクには「*失敗*」ステータスが付与されます。

定義データベースと Kaspersky Security Center のソフトウェアモジュールは *［管理サーバーのリポジトリへのアップデートのダウンロード］*タスクを使用してダウンロードされるため、このスキームでもこのタスクが必要です。

ローカルフォルダー、共有フォルダー、または FTP サーバーを使用して手動で実行

クライアントデバイスが管理サーバーに接続できない場合、ローカルフォルダーまたは共有リソースを使用して定義データベース、ソフトウェアモジュール、カスペルスキー製品をアップデートできます。このスキームでは、管理サーバーのリポジトリからリムーバブルドライブに必要なアップデートをコピーして、Kaspersky Endpoint Security の設定でアップデート元として指定したローカルフォルダーまたは共有リソースにアップデートをコピーする必要があります（次の図を参照）。



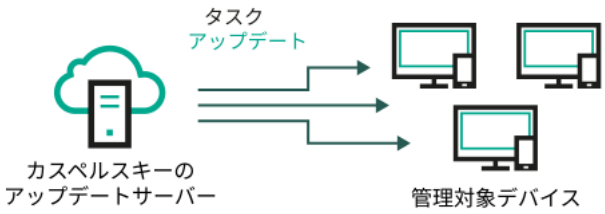
ローカルフォルダー、共有フォルダー、または FTP サーバーを使用したアップデート

Kaspersky Endpoint Security のアップデート元の詳細については、次のヘルプを参照してください：

- Kaspersky Endpoint Security for Windows のヘルプ
- Kaspersky Endpoint Security for Linux のヘルプ

カスペルスキーのアップデートサーバーから管理対象デバイスの Kaspersky Endpoint Security を直接アップデート

管理対象デバイスで、カスペルスキーのアップデートサーバーから直接アップデートを受信するように Kaspersky Endpoint Security を設定できます（次の図を参照）。



カスペルスキーのアップデートサーバーからセキュリティ製品を直接アップデート

このスキームでは、セキュリティ製品は Kaspersky Security Center が提供するリポジトリを使用しません。カスペルスキーのアップデートサーバーからアップデートを直接受信するには、セキュリティ製品のインターフェイスでカスペルスキーのアップデートサーバーをアップデート元として指定します。これらの設定の詳細については、次のヘルプを参照してください：

- Kaspersky Endpoint Security for Windows のヘルプ
- Kaspersky Endpoint Security for Linux のヘルプ

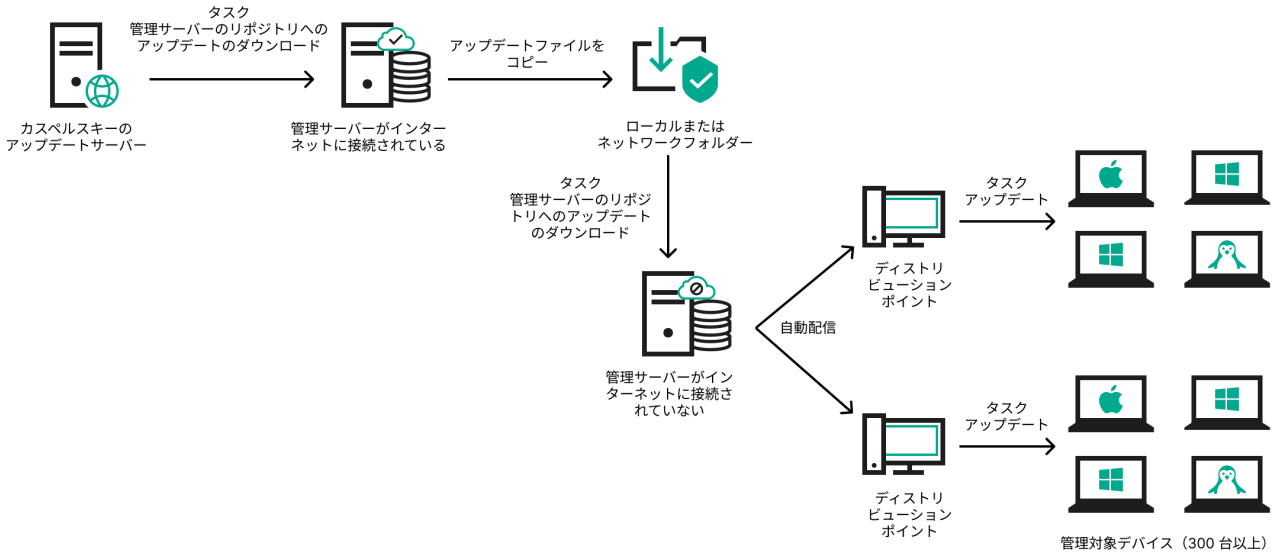
管理サーバーがインターネットに接続されていない場合は、ローカルまたはネットワークフォルダー経由

管理サーバーがインターネットに接続されていない場合は、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを設定して、ローカルまたはネットワークフォルダーからアップデートをダウンロードできます。この場合、指定したフォルダーに必要なアップデートファイルを定期的にコピーする必要があります。たとえば、次のいずれかのソースから、必要なアップデートファイルをコピーできます：

- インターネットに接続されている管理サーバー（下図を参照）

  管理サーバーは、セキュリティ製品が要求したアップデートのみをダウンロードするため、管理サーバーによって管理されるセキュリティ製品のセット（インターネット接続があるものとないもの）が一致している必要があります。

  アップデートのダウンロードに使用する管理サーバーのバージョンが 13.2 以前の場合、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクのプロパティを開き、［**旧スキームを使用してアップデートをダウンロード**］オプションをオンにします。



管理サーバーがインターネットに接続されていない場合のローカルまたはネットワーク フォルダー経由のアップデート

- Kaspersky Update Utility

  このユーティリティは旧スキームを使用してアップデートをダウンロードするため、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクのプロパティを開き、［**旧スキームを使用してアップデートをダウンロード**］オプションをオンにします。

カスペルスキー製品の定義データベースとソフトウェアモジュールのアップデートでの差分ファイルの使用

Kaspersky Security Center がカスペルスキーのアップデートサーバーからアップデートをダウンロードする時、差分ファイルを使用することでトラフィックが最適化されます。また、ネットワーク内の他のデバイスからアップデートを取得するデバイス（管理サーバー、ディストリビューションポイント、クライアントデバイス）についても、差分ファイルの使用を有効化できます。

差分ファイルのダウンロード機能の概要

差分ファイルには、定義データベースファイルまたはソフトウェアモジュールファイルの異なる 2 バージョン間の変更点のみが含まれています。完全な定義データベースファイルまたはソフトウェアモジュールファイルよりも差分ファイルの方が容量が小さいため、差分ファイルを使用することで社内ネットワークのトラフィック量を軽減できます。管理サーバーまたはディストリビューションポイントで［*差分ファイルのダウンロード*］機能が有効になっている場合、該当する管理サーバーまたはディストリビューションポイントに差分ファイルが保存されます。これにより、この管理サーバーまたはディストリビューションポイントからアップデートを取得するデバイスでは、保存されている差分ファイルを使用して定義データベースとソフトウェアモジュールのアップデートを実行できます。

差分ファイルをより効果的に使用するには、デバイス側でのアップデートスケジュールを、アップデートの取得元となる管理サーバーやディストリビューションポイント側のアップデートスケジュールと同期することを推奨します。ただし、このような設定を行わなくても、デバイス側のアップデート頻度がアップデートの取得元となる管理サーバーやディストリビューションポイント側のアップデート頻度より低いだけでもトラフィックの軽減につながります。

差分ファイルのダウンロード機能は、バージョン 11 以降の管理サーバーとディストリビューションポイントでのみ有効にできます。それ以前のバージョンの管理サーバーとディストリビューションポイントで差分ファイルの保存を行うには、バージョン 11 以降へのアップグレードを先に実行してください。

差分ファイルのダウンロード機能は、オフライン方式でのアップデートのダウンロードではサポートされません。ネットワークエージェントへのアップデートの配信を行う管理サーバーまたはディストリビューションポイントで差分ファイルのダウンロードが有効になっていても、オフライン方式でアップデートのダウンロードを行う設定のネットワークエージェントは差分ファイルをダウンロードしません

ディストリビューションポイントは差分ファイルの自動配信に IP マルチキャストを使用しません。

差分ファイルのダウンロード機能の有効化

必須条件

事前に満たすべき要件は次の通りです：

- 管理サーバーとディストリビューションポイントがバージョン 11 以降にアップグレードされています。
- ネットワークエージェントのポリシーでオフライン方式でのアップデートのダウンロードがオフになっている。

実行するステップ

1. **管理サーバーでこの機能を有効にする**

   管理サーバーのリポジトリへのアップデートのダウンロードタスクの設定でこの機能を有効にします。

2. **ディストリビューションポイントでこの機能を有効にする**

   ディストリビューションポイントのリポジトリにアップデートをダウンロードタスクを使用してアップデートを取得するディストリビューションポイントでこの機能を有効にします。

   管理サーバーからアップデートを取得するディストリビューションポイントでこの機能を有効にします。

ネットワークエージェントのポリシー設定と（ディストリビューションポイントを手動で割り当てていてポリシー設定を上書きしたい場合）管理サーバーのプロパティの［**ディストリビューションポイント**］セクションで機能を有効にできます。

［差分ファイルのダウンロード］機能が有効になっているかどうかを確認する方法としては、これらの手順を実行する前後での内部トラフィックを測定することができます。

［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの作成

管理サーバー上の*管理サーバーのリポジトリへのアップデートのダウンロード*タスクは、Kaspersky Security Center のクイックスタートウィザードによって自動的に作成されます。*管理サーバーのリポジトリへのアップデートのダウンロード*タスクは1つだけ作成できます。したがって、このタスクが管理サーバーのタスク リストから削除された場合にのみ、*管理サーバーのリポジトリへのアップデートのダウンロード*のタスクを作成することができます。

管理サーバーのリポジトリへアップデートをダウンロードするタスクを作成するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. 次のいずれかの方法で、タスクの作成を開始します：
   - コンソールツリーの［**タスク**］フォルダーのコンテキストメニューで、［**新規**］→［**タスク**］の順に選択します。
   - ［**タスク**］フォルダーの作業領域で［**タスクの作成**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. ウィザードの［**タスク種別の選択**］ウィンドウで、［**管理サーバーのリポジトリへのアップデートのダウンロード**］を選択します。
4. ウィザードの［**設定**］ウィンドウで、タスクを次のように設定します：
   - **アップデート元**

管理サーバーのアップデート元として、使用できるものは次のとおりです：

- カスペルスキーのアップデートサーバー

  カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。既定では、管理サーバーは HTTPS プロトコルを使用してカスペルスキーのアップデートサーバーに接続し、アップデートをダウンロードします。必要に応じて、管理サーバーで HTTPS プロトコルの代わりに HTTP プロトコルを使用するように設定を編集できます。

  既定では、この項目が選択されます。

- プライマリ管理サーバー

  セカンダリ管理サーバーまたは仮想管理サーバーを対象とするタスクに適用されます。

- ローカルまたはネットワークフォルダー

  最新のアップデートが保存されたローカルフォルダーまたはネットワークフォルダー：ネットワークフォルダーとしては FTP サーバー、HTTP サーバー、または SMB 共有を指定できます。ネットワークフォルダーに認証が必要な場合、SMB プロトコルのみがサポートされています。ローカルフォルダーの選択時には、管理サーバーがインストールされているデバイスのフォルダーを指定する必要があります。

  > アップデート元で使用される FTP/HTTP サーバーまたはネットワークフォルダーは、アップデートを含み、フォルダーの構造がカスペルスキーのアップデートサーバーの使用時に作成された構造と一致する必要があります。

- **その他の設定**

  - **セカンダリ管理サーバーの強制アップデート**

    このオプションをオンにすると、管理サーバーは、新しいアップデートがダウンロードされるとすぐに、セカンダリ管理サーバーのアップデートタスクを開始します。アップデートタスクは、セカンダリ管理サーバーのタスクプロパティで構成されているアップデートソースを使用して開始されます。

    このオプションをオフにすると、セカンダリ管理サーバーのアップデートタスクは、スケジュールに従って開始されます。

    既定では、このオプションはオフです。

  - **ダウンロード済みのアップデートを追加のフォルダーにコピー**

管理サーバーがアップデートを受信すると、指定されたフォルダーにコピーします。ネットワークでのアップデートの配信を手動で管理する場合は、このオプションをオンにします。

このオプションの使用を検討する状況としては、たとえば、組織のネットワークが複数の独立したサブネットワークで構成され、各サブネットワークに属するデバイスは別のサブネットワークへのアクセス権を付与されていない場合があります。ただし、すべてのサブネットワークのデバイスは共通のネットワーク共有へのアクセス権は付与されています。この場合、いずれかのサブネットワークの管理サーバーでカスペルスキーのアップデートサーバーからアップデートをダウンロードするように設定した後、このオプションをオンにし、ネットワーク共有をコピー先に指定します。他の管理サーバーでは、リポジトリへのアップデートのダウンロードタスクのアップデート元として、このネットワーク共有を指定します。

既定では、このオプションはオフです。

- **アップデートのコピーが完了していない場合はデバイスおよびセカンダリ管理サーバーを強制アップデートしない**

  クライアントデバイスとセカンダリ管理サーバーでのアップデートのダウンロードタスクは、元のネットワークフォルダーから追加のアップデートフォルダーにアップデートがコピーされるまで開始されません。

  クライアントデバイスとセカンダリ管理サーバーが、追加のネットワークフォルダーからアップデートをダウンロードする場合は、このオプションをオンにする必要があります。

  既定では、このオプションはオフです。

- **旧スキームを使用してアップデートをダウンロード**

  Kaspersky Security Center のバージョン 14 から、データベースのアップデートとソフトウェアモジュールのダウンロードには新しいスキームが使用されるようになりました。新しいスキームを使用してアップデートをダウンロードするには、アップデート元に、新しいスキームと互換性のあるメタデータを持つアップデートファイルが含まれている必要があります。アップデート元のアップデートファイルのメタデータが旧スキームのみと互換性がある場合は、［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。オフにした場合、アップデートのダウンロードタスクは失敗します。

  例えば、アップデート元としてローカルまたはネットワークフォルダーが指定されており、そのフォルダー内のアップデートファイルが次のアプリケーションによってダウンロードされた場合にはこのオプションをオンにする必要があります：

  - Kaspersky Update Utility

    このユーティリティは旧スキームを使用してアップデートをダウンロードします。

  - Kaspersky Security Center 13.2 以前のバージョン

    例えば、管理サーバー 1 はインターネットに接続していないものとします。この場合、インターネットに接続できる管理サーバー 2 を使用してアップデートをダウンロードし、このアップデートを管理サーバー 1 のアップデート元として使用するために、ローカルまたはネットワークフォルダーに保存します。管理サーバー 2 に Kaspersky Security Center のバージョン 13.2 以前のバージョンがインストールされていた場合、管理サーバー 1 向けのタスクでは［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。

  既定では、このオプションはオフです。

5. ウィザードの［**タスクスケジュールの設定**］ページで、タスク開始のスケジュールを作成できます。必要に応じて、次の設定を指定します：

   - **実行予定：**

タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

- **N 時間ごと**

  指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

  既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

- **N 日ごと**

  日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

  既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

- **N 週間ごと**

  指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

  既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

- **N 分ごと**

  タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

  既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

- **毎日（サマータイムはサポートしていません）**

  日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を 1 時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

  このスケジュールの使用は推奨されません。Kaspersky Security Center の旧バージョンとの後方互換性を維持するために用意されているオプションとなります。

  既定では、毎日、現在のシステム時刻にタスクが実行されます。

- **毎週**

  毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

毎月、指定した日付の指定した時刻にタスクを定期的に実行します。
指定した日付が存在しない月には、月の最終日にタスクを実行します。
既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。
  規定では、日付は選択されていません。規定の開始時間は18:00 です。

- **ウイルスアウトブレイク検知次第**

  ［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：
  - ワークステーションとファイルサーバー向けアンチウイルス製品
  - 境界防御向けアンチウイルス製品
  - メールサーバー向けアンチウイルス製品

  既定では、すべてのアプリケーション種別がオンです。
  ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

  他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

  テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

  必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

  - タスク名で検索するには、検索フィールドにタスク名を入力します。
  - 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。
    既定では、タスクはアルファベットの昇順で並べ替えられます。
  - フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる(分)**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

既定では、このオプションはオフです。既定の時間は1分です。

6. ウィザードの［**タスク名の定義**］ウィンドウで、作成中のタスク名を指定します。タスク名は100文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

7. ［**タスク作成の終了**］ウィンドウで、［**終了**］をクリックしてウィザードを終了します。

   ウィザード終了後にすぐにタスクを開始するには、［**ウィザードの終了後にタスクを実行**］をオンにします。

ウィザードが完了すると、作業領域の管理サーバータスクのリストに［**管理サーバーのリポジトリへのアップデートのダウンロード**］タスクが表示されます。

タスクの作成時に指定した設定およびタスクのその他のプロパティは、いつでも変更できます。

管理サーバーが*管理サーバーのリポジトリへのアップデートのダウンロード*のタスクを実行すると、アップデート元から定義データベースとソフトウェアモジュールのアップデートがダウンロードされ、管理サーバーの共有フォルダーに保存されます。管理グループに対してこのタスクを作成すると、指定された管理グループにあるネットワークエージェントにのみ適用されます。

アップデートは管理サーバーの共有フォルダーからクライアントデバイスとセカンダリ管理サーバーに配信されます。

［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの作成

macOS を実行しているディストリビューションポイントデバイスでは、カスペルスキーのアップデートサーバーからアップデートをダウンロードできません。

*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクの対象範囲に macOS を実行しているデバイスが 1 台以上含まれている場合、すべての Windows デバイスでタスクが正常に完了した場合でも、タスクには「*失敗*」ステータスが付与されます。

*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを管理グループに対して作成できます。このタスクは、指定の管理グループ内のディストリビューションポイントに対して実行されます。

このタスクの使用例としては、管理サーバーとディストリビューションポイント間の通信の方が、ディストリビューションポイントとカスペルスキーのアップデートサーバー間の通信よりも費用がかかる場合や、管理サーバーがインターネットにアクセスできない場合などがあります。

ディストリビューションポイントのリポジトリにアップデートをダウンロードタスクを、選択した管理グループに対して作成するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. このフォルダーの作業領域で［**新規タスク**］をクリックします。
   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. ウィザードの［**タスク種別の選択**］ページで［**Kaspersky Security Center 管理サーバー**］ノードを選択し、［**詳細**］フォルダーを開いて**ディストリビューションポイントのリポジトリにアップデートをダウンロード**タスクを選択します。
4. ウィザードの［**設定**］ページで、タスクを次のように設定します：
   - **アップデート元**

ディストリビューションポイントのアップデート元として、使用できるものは次の通りです：

- カスペルスキーのアップデートサーバー

  カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。

  既定ではこのオプションが選択されます。

- プライマリ管理サーバー

  セカンダリ管理サーバーまたは仮想管理サーバーを対象とするタスクに適用されます。

- ローカルまたはネットワークフォルダー

  最新のアップデートが保存されたローカルフォルダーまたはネットワークフォルダー：ネットワークフォルダーとしては FTP サーバー、HTTP サーバー、または SMB 共有を指定できます。ネットワークフォルダーに認証が必要な場合、SMB プロトコルのみがサポートされています。ローカルフォルダーの選択時には、管理サーバーがインストールされているデバイスのフォルダーを指定する必要があります。

  > アップデート元で使用される FTP/HTTP サーバーまたはネットワークフォルダーは、アップデートを含み、フォルダーの構造がカスペルスキーのアップデートサーバーの使用時に作成された構造と一致する必要があります。

- **アップデート保存先フォルダー**

  保存したアップデートを保管するためのフォルダーのパス。指定したフォルダーのパスをクリップボードにコピーすることができます。グループタスクに対して指定されたフォルダーのパスを変更することはできません。

- **旧スキームを使用してアップデートをダウンロード**

Kaspersky Security Center のバージョン 14 から、データベースのアップデートとソフトウェアモジュールのダウンロードには新しいスキームが使用されるようになりました。新しいスキームを使用してアップデートをダウンロードするには、アップデート元に、新しいスキームと互換性のあるメタデータを持つアップデートファイルが含まれている必要があります。アップデート元のアップデートファイルのメタデータが旧スキームのみと互換性がある場合は、［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。オフにした場合、アップデートのダウンロードタスクは失敗します。

たとえば、アップデート元としてローカルまたはネットワークフォルダーが指定されており、そのフォルダー内のアップデートファイルが次のアプリケーションによってダウンロードされた場合にはこのオプションをオンにする必要があります：

- Kaspersky Update Utility

  このユーティリティは旧スキームを使用してアップデートをダウンロードします。

- Kaspersky Security Center 13.2 以前のバージョン

  たとえば、ディストリビューションポイントがローカルまたはネットワークフォルダーからアップデートを取得するように設定されているものとします。この場合、インターネットに接続できる管理サーバーを使用してアップデートをダウンロードし、このアップデートをディストリビューションポイントのローカルフォルダーに配置します。管理サーバーに Kaspersky Security Center 13.2 以前のバージョンがインストールされている場合、*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクで［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。

既定では、このオプションはオフです。

5. ウィザードの［**管理グループの選択**］ウィンドウで［**参照**］をクリックして、タスクを適用する管理グループを選択します。

6. ウィザードの［**タスクスケジュールの設定**］ページで、タスク開始のスケジュールを作成できます。必要に応じて、次の設定を指定します：

- **実行予定：**

  タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

  - **N 時間ごと**

    指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

    既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

  - **N 日ごと**

    日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

    既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

  - **N 週間ごと**

指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。
既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

- **N 分ごと**

  タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。
  既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

- **毎日（サマータイムはサポートしていません）**

  日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を 1 時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。
  このスケジュールの使用は推奨されません。Kaspersky Security Center の旧バージョンとの後方互換性を維持するために用意されているオプションとなります。
  既定では、毎日、現在のシステム時刻にタスクが実行されます。

- **毎週**

  毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。
  既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。
  指定した日付が存在しない月には、月の最終日にタスクを実行します。
  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。
  規定では、日付は選択されていません。規定の開始時間は18:00 です。

- **ウイルスアウトブレイク検知次第**

［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

- ワークステーションとファイルサーバー向けアンチウイルス製品
- 境界防御向けアンチウイルス製品
- メールサーバー向けアンチウイルス製品

既定では、すべてのアプリケーション種別がオンです。

ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

- タスク名で検索するには、検索フィールドにタスク名を入力します。
- 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。

  既定では、タスクはアルファベットの昇順で並べ替えられます。
- フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる(分)**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  既定では、このオプションはオフです。既定の時間は1分です。

7. ウィザードの［**タスク名の定義**］ウィンドウで、作成中のタスク名を指定します。タスク名は100文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

8. ［**タスク作成の終了**］ウィンドウで、［**終了**］をクリックしてウィザードを終了します。

   ウィザード終了後にすぐにタスクを開始するには、［**ウィザードの終了後にタスクを実行**］をオンにします。

ウィザードが完了すると、［**ディストリビューションポイントのリポジトリにアップデートをダウンロード**］タスクが、コンソールの対象の管理グループのネットワークエージェントタスクのリストと［**タスク**］作業領域に表示されます。

タスクの作成時に指定した設定およびタスクのその他のプロパティは、いつでも変更できます。

*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを実行すると、定義データベースとソフトウェアモジュールのアップデートがアップデート元からダウンロードされ、共有フォルダーに保存されます。指定の管理グループに含まれていて、ディストリビューションポイントタスクが明示的に設定されていないディストリビューションポイントにしか、ダウンロードされたアップデートは使用されません。

管理サーバーのプロパティウィンドウの［**セクション**］ペインで、［**ディストリビューションポイント**］を選択します。各ディストリビューションポイントのプロパティの［**アップデート元**］セクションでは、アップデート元を指定できます（［**管理サーバーから取得**］または［**アップデートの強制ダウンロードタスクを使用**］）。手動または自動的に割り当てられたディストリビューションポイントでは、［**管理サーバーから取得**］があらかじめ選択されています。これらのディストリビューションポイントは、*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクの結果を使用します。

各ディストリビューションポイントのプロパティによって、そのディストリビューションポイント用に個別に設定されたネットワークフォルダーが指定されます。フォルダー名はそのディストリビューションポイントによって異なる場合があります。そのため、デバイスのグループ用のタスクを作成する場合、タスクプロパティでネットワークフォルダーを変更しないでください。

1台のデバイス用のローカルタスクを作成する場合、*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクのプロパティでアップデートを格納するネットワークフォルダーを変更できます。

［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの設定

管理サーバーのリポジトリへのアップデートのダウンロードタスクを設定するには

1. コンソールツリーの［**タスク**］フォルダーの作業領域で、タスクリストから［**管理サーバーのリポジトリへのアップデートのダウンロード**］を選択します。
2. 次のいずれかの方法で、タスクのプロパティウィンドウを開きます：
   - タスクのコンテキストメニューで［**プロパティ**］を選択します。
   - 選択したタスクの情報ボックスで、［**タスクの設定**］をクリックします。

*管理サーバーのリポジトリへのアップデートのダウンロード*タスクのプロパティウィンドウが開きます。このウィンドウでは、アップデートを管理サーバーのリポジトリにダウンロードする方法を設定できます。

ダウンロードされたアップデートの検証

管理対象デバイスにアップデートをインストールする前に、*アップデートの検証*タスクを使用してアップデートの動作およびエラーがないかどうかを検証することができます。*アップデートの検証*タスクは、*管理サーバーのリポジトリへのアップデートのダウンロード*のタスクの一部として自動的に実行されます。アップデート元からアップデートがダウンロードされて、一時リポジトリに保存された後、*アップデートの検証*タスクが実行されます。タスクが正常に完了すると、一時リポジトリから管理サーバーの共有フォルダー（<Kaspersky Security Center のインストールフォルダー>\Share\Updates）にアップデートがコピーされます。アップデートのコピーは、管理サーバーがアップデート元として指定されているすべてのクライアントデバイスに配信されます。

*アップデートの検証*タスクの結果、一時リポジトリにあるアップデートが正しくないことが判明した場合、または*アップデートの検証*タスクがエラーで終了した場合、それらのアップデートは共有フォルダーにコピーされません。管理サーバーでは、以前のアップデートが維持されます。また、スケジュール種別として［**新しいアップデートがリポジトリにダウンロードされ次第**］が指定されたタスクも開始されません。新しいアップデートのスキャンが正常に完了した場合、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの次の開始時に、それらのタスクが実行されます。

少なくとも1台のテストデバイスで次のいずれかの条件が当てはまる場合、アップデートは正しくないと判断されます：

- アップデートタスクエラーが発生した
- セキュリティ製品のリアルタイム保護のステータスがアップデートの適用後に変更された
- オンデマンドスキャンタスクの実行中に、感染したオブジェクトが検知された
- カスペルスキー製品の実行時にエラーが発生した

すべてのテストデバイスの場合に挙げられた条件が当てはまらない場合、そのアップデートは正常とみなされ、*アップデートの検証*タスクは正常に終了したと判断されます。

*アップデートの検証*タスクを作成する前に、次の前提条件を実行してください：

1. 複数のテストデバイスで管理グループを作成する。このグループでアップデートを検証します。

   ネットワーク内で、最も信頼性の高い保護が適用されており、最も一般的なアプリケーション設定が行われているデバイスを使用してください。このアプローチにより、スキャン中のウイルス検知の精度が向上し、誤検知のリスクを最小限に抑えます。テストデバイスでウイルスが検知された場合、*アップデート検証*タスクは失敗と判断されます。

2. Kaspersky Endpoint Security for Windows や Kaspersky Security for Windows Server など、Kaspersky Security Center のサポート対象のアプリケーション向けに*アップデートおよびマルウェアスキャンタスクを作成します*。*アップデート*および*マルウェアスキャン*タスクの作成時に、テストデバイスの管理グループを指定します。

   *アップデートの検証*タスクは順次テストデバイスで*アップデート*と*マルウェアスキャン*タスクを実行し、すべてのアップデートが有効であることを確認します。また、*アップデートの検証*タスクの作成中に*アップデート*および*マルウェアスキャン*タスクを指定する必要があります。

3. *［管理サーバーのリポジトリへのアップデートのダウンロード］タスクを作成します*。

ダウンロードしたアップデートを、クライアントデバイスに配信する前に Kaspersky Security Center で検証するには：

1. ［**タスク**］フォルダーの作業領域で、タスクリストから*管理サーバーのリポジトリへのアップデートのダウンロード*タスクを選択します。

2. 次のいずれかの方法で、タスクのプロパティウィンドウを開きます：

   - タスクのコンテキストメニューで［**プロパティ**］を選択します。
   - 選択したタスクの情報ボックスで、［**タスクの設定**］をクリックします。

3. *アップデートの検証*タスクがある場合は、［**参照**］をクリックします。表示されるウィンドウで、テストデバイスの管理グループで*アップデートの検証*タスクを選択します。

4. 事前に*アップデートの検証*タスクを作成していなかった場合は、［**作成**］をクリックします。

   *アップデートの検証*タスクウィザードが起動します。ウィザードの指示に従ってください。

5. ［**OK**］をクリックして、*管理サーバーのリポジトリへのアップデートのダウンロード*タスクのプロパティウィンドウを閉じます。

アップデートの自動的な検証が有効になります。これで、*管理サーバーのリポジトリへのアップデートのダウンロード*タスクを実行できるようになりました。タスクはアップデート検証から開始します。

テストポリシーと予備タスクの設定

*アップデートの検証*タスクの作成時に、テストポリシーと予備のグループアップデートタスクおよびオンデマンドスキャンタスクが管理サーバーで生成されます。

予備のグループアップデートタスクとオンデマンドスキャンタスクの実行には少し時間がかかります。これらのタスクは、*アップデート検証*タスクの実行時に実行されます。*アップデート検証*タスクは、*リポジトリへのアップデートのダウンロード*タスクの一部として実行されます。［*リポジトリへのアップデートのダウンロード*］タスクの実行時間には、予備のグループアップデートタスクとオンデマンドスキャンタスクの実行時間も含まれています。

テストポリシーと予備タスクの設定を変更することができます。

テストポリシーまたは予備タスクの設定を変更するには：

1. コンソールツリーで、*アップデート検証*タスクを作成したグループを選択します。
2. グループの作業領域で、次のいずれかのタブを選択します：
   - **ポリシー**：テストポリシーの設定を編集する場合
   - **タスク**：予備タスクの設定を変更する場合
3. タブの作業領域で、設定を変更するポリシーまたはタスクを選択します。
4. 次のいずれかの方法で、ポリシー（タスク）のプロパティウィンドウを開きます：
   - ポリシー（タスク）のコンテキストメニューで［**プロパティ**］を選択します。
   - 選択したポリシー（タスク）の情報ボックスで、［**ポリシーの設定**］（［**タスクの設定**］）をクリックします。

アップデートを正しく検証するには、テストポリシーと予備タスクの変更に次の制限を適用します：

- 予備タスクの設定：
  - 管理サーバーで、すべてのタスクを［**緊急**］および［**機能エラー**］の重要度で保存する。管理サーバーはこれらの種別のイベントを使用して、アプリケーションの動作を分析します。
  - 管理サーバーをアップデート元として使用する。
  - タスクのスケジュール種別を［**手動**］に指定する。
- テストポリシーの設定：
  - iChecker および iSwift スキャン加速技術を無効にします（［**脅威対策**］→［**ファイル脅威対策**］→［**設定**］→［**詳細**］→［**スキャン技術**］）。
  - 感染したオブジェクトの処理を選択します：**駆除する。駆除できない場合は削除する / 駆除する。駆除できない場合はブロックする / ブロック**（［**脅威対策**］→［**ファイル脅威対策**］→［**脅威の検知時の処理**］）。
- テストポリシーと予備タスクの設定：

  ソフトウェアモジュールのアップデートのインストール後、デバイスで再起動が必要な場合は、ただちに再起動する必要があります。デバイスを再起動しないと、この種別のアップデートをテストすることはできません。一部のアプリケーションでは、再起動が必要なアップデートのインストールは禁止されているか、またはユーザーへまず確認を要求するように設定されています。テストポリシーと予備タスクの設定では、これらの制限を無効にする必要があります。

ダウンロードされたアップデートの表示

ダウンロードされたアップデートのリストを表示するには：

コンソールツリーで、［**リポジトリ**］フォルダーの［**定義データベースとカスペルスキー製品モジュールのアップデート**］サブフォルダーを選択します。

［**定義データベースとカスペルスキー製品モジュールのアップデート**］フォルダーの作業領域に、管理サーバーに保存されているアップデートのリストが表示されます。

Kaspersky Endpoint Security のアップデートをデバイスに自動インストール

クライアントデバイスでの Kaspersky Endpoint Security の定義データベースとソフトウェアモジュールの自動アップデートを設定できます。

デバイスでの Kaspersky Endpoint Security アップデートのダウンロードおよび自動インストールを設定するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. 次のいずれかの方法で、**アップデート**タスクを作成します：
   - コンソールツリーの［**タスク**］フォルダーのコンテキストメニューで、［**新規作成**］→［**タスク**］の順に選択します。
   - ［**タスク**］フォルダーの作業領域の［**新規タスク**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. ウィザードの［**タスク種別の選択**］ページで、タスクの種別として［**Kaspersky Endpoint Security**］を選択し、その下の［**アップデート**］を選択します。
4. 引き続きウィザードの指示に従って操作します。

   ウィザードが終了したら、Kaspersky Endpoint Security のアップデートタスクが作成されます。新規作成されたタスクが、［**タスク**］フォルダーの作業領域のタスクのリストに表示されます。
5. ［**タスク**］フォルダーの作業領域で、作成したアップデートタスクを選択します。
6. タスクのコンテキストメニューで［**プロパティ**］を選択します。
7. タスクのプロパティウィンドウが開いたら、［**セクション**］ペインで［**オプション**］を選択します。

   ［**オプション**］セクションでは、ローカルモードまたはモバイルモードで、アップデートタスクを設定できます：
   - **ローカルモードのアップデート設定**：管理サーバーとデバイスの間で接続が確立されている場合。
   - **モバイルモードのアップデート設定**：Kaspersky Security Center とデバイスの間で接続が確立されていない場合（たとえば、デバイスがインターネットに接続されていない場合）。

8. ［**設定**］をクリックして、アップデート元を選択します。

9. ［**ソフトウェアモジュールのアップデートをダウンロード**］をオンにして、定義データベースとともに、ソフトウェアモジュールのアップデートをダウンロードおよびインストールします。

   このチェックボックスをオンにすると、Kaspersky Endpoint Security によって適用可能なソフトウェアモジュールのアップデートについてユーザーに通知され、アップデートタスクの実行中に、アップデートパッケージにソフトウェアモジュールのアップデートが追加されます。アップデートモジュール使用を設定するには：

   - **重要なアップデートおよび承認済みのアップデートをインストール**：ソフトウェアモジュールのアップデートが適用可能な場合、Kaspersky Endpoint Security は「*緊急*」ステータスのアップデートのみを自動的にインストールし、残りのアップデートは承認後にインストールします。

   - **承認されたアップデートのみをインストール**：ソフトウェアモジュールのアップデートが適用可能な場合、Kaspersky Endpoint Security はインストールが承認されたアップデートのみインストールします。ローカルへのインストールは、製品インターフェイスまたは Kaspersky Security Center を経由して実行されます。

   ソフトウェアモジュールのアップデートで使用許諾契約書とプライバシーポリシーの条項を確認して同意する必要がある場合、カスペルスキー製品では、使用許諾契約書とプライバシーポリシーの条項をユーザーが同意した後にアップデートがインストールされます。

10. ダウンロード済みのアップデートをフォルダーに保存するために［**アップデートをフォルダーにコピー**］をオンにし、［**参照**］をクリックしてフォルダーを指定します。

11. ［**OK**］をクリックします。

［**アップデート**］タスクの実行時、製品からカスペルスキーのアップデートサーバーにリクエストが送信されます。

アップデートによっては、最新バージョンの管理プラグインをインストールする必要があります。

オフライン方式のアップデートのダウンロード

管理対象デバイス上のネットワークエージェントが管理サーバーに接続していないためアップデートを受信できない場合があります。たとえば、ネットワークエージェントがノート PC にインストールされており、インターネットにもローカルネットワークにも接続されていないことがあります。また、デバイスのネットワーク接続時間が管理者によって制限されている場合もあります。このような場合、ネットワークエージェントがインストールされたデバイスはスケジュールに従って管理サーバーからアップデートを受信することができません。ネットワークエージェントを使用して管理対象のアプリケーション（Kaspersky Endpoint Security など）のアップデートを設定している場合、アップデートには管理サーバーとの接続が必要です。ネットワークエージェントと管理サーバーとの間に接続が確立されていない場合、アップデートはできません。ネットワークエージェントが指定された時間間隔で管理サーバーに接続するようにネットワークエージェントと管理サーバーとの接続を設定する場合があります。指定した時間間隔に接続がなかった場合、定義データベースはアップデートされません。さらに、複数の管理対象アプリケーションが同時にアップデートを受信しようとして管理サーバーにアクセスする可能性があります。その場合、管理サーバーが応答を停止する場合があります（DDoS 攻撃と類似しているため）。

上述のような問題を回避するため、管理対象アプリケーションのオフライン方式によるアップデートのダウンロードが Kaspersky Security Center に実装されています。この方式は、管理サーバー通信チャネルにアクセスできないことによる一時的な問題があっても、アップデート配信のためのメカニズムを提供します。また、管理サーバーの負荷も低減できます。

オフライン方式によるアップデートのダウンロード

管理サーバーは、アップデートの受信時に、管理対象アプリケーションに必要なアップデートを、該当するアプリケーションがインストールされたデバイス上のネットワークエージェントに通知します。ネットワークエージェントは、アップデートに関する情報を受け取ると、適切なファイルを管理サーバーからあらかじめダウンロードします。具体的には、管理サーバーは、ネットワークエージェントが次に接続された時にアップデートのダウンロードを開始します。ネットワークエージェントによってすべてのアップデートがクライアントデバイスにダウンロードされると、そのデバイスのアプリケーションでこれらのアップデートが利用可能になります。

クライアントデバイス上の管理対象アプリケーションがアップデートのためにネットワークエージェントにアクセスしようとすると、ネットワークエージェントは必要なアップデートがあるかどうか確認します。管理対象アプリケーションから要求された時点で、管理サーバーからアップデートを受信してから経過した時間が 25 時間以内の場合、ネットワークエージェントは管理サーバーと接続せずに、ローカルキャッシュからアップデートを管理対象アプリケーションに渡します。ネットワークエージェントからクライアントデバイス上のアプリケーションへアップデートを配信する際には、アップデートのために管理サーバーへの接続を確立する必要はありません。

ネットワークエージェントは、管理サーバーの負荷を分散するため、管理サーバーへの接続とアップデートのダウンロードを、管理サーバーが指定する時間間隔の中でランダムに実行します。この間隔は、アップデートをダウンロードするネットワークエージェントがインストールされたデバイスの数とアップデートの容量で決まります。管理サーバーの負荷を軽減するため、ネットワークエージェントをディストリビューションポイントとして使用できます。

オフライン方式でのアップデートのダウンロードが無効になっている場合、アップデートはアップデートのダウンロードタスクのスケジュール設定に基づいて配信されます。

既定では、オフライン方式でのアップデートのダウンロードは有効です。

オフライン方式でのアップデートのダウンロードは、管理対象製品がアップデートを受け取るためのタスクのスケジュール種別で［**新しいアップデートがリポジトリにダウンロードされ次第**］が選択されている管理対象デバイスでのみ使用されます。その他の管理対象デバイスでは、標準スキームを使用して、リアルタイムモードで管理サーバーからアップデートを取得します。

管理対象製品が管理サーバーからではなくカスペルスキーサーバーまたはネットワークフォルダーから取得したアップデートを持っており、なおかつアップデートダウンロードタスクがスケジュール種別として［**新しいアップデートがリポジトリにダウンロードされ次第**］を選択している場合、関係する管理グループのネットワークエージェントポリシーの設定を使用して、オフライン方式でのアップデートのダウンロードを無効にしてください。

オフライン方式のアップデートのダウンロードの有効化と無効化

オフライン方式でのアップデートのダウンロードを無効にすることは推奨されません。無効にすると、デバイスにアップデートが提供されません。場合によっては、カスペルスキーのテクニカルサポート担当者が、［**アップデートと定義データベースをあらかじめ管理サーバーからダウンロードする**］をオフにすることを推奨する場合もあります。次に、カスペルスキー製品のアップデートを受信するためのタスクが設定されていることを確認する必要があります。

管理グループでオフライン方式のアップデートのダウンロードを有効または無効にするには：

1. コンソールツリーで、オフライン方式のアップデートのダウンロードを有効化する必要がある管理グループを選択します。
2. グループの作業領域で、［**ポリシー**］タブを開きます。
3. ［**ポリシー**］タブで、ネットワークエージェントポリシーを選択します。
4. ポリシーのコンテキストメニューで［**プロパティ**］を選択します。
   ネットワークエージェントポリシーのプロパティウィンドウを表示します。
5. ポリシーのプロパティウィンドウで［**パッチとアップデートの管理**］セクションを選択します。
6. ［**アップデートと定義データベースをあらかじめ管理サーバーからダウンロードする（推奨）**］を、オフライン方式のアップデートのダウンロードを有効にする場合はオン、無効にする場合はオフにします。
   既定では、オフライン方式でのアップデートのダウンロードは有効です。

オフライン方式でのアップデートのダウンロードが有効または無効になります。

Kaspersky Security Center コンポーネントの自動アップデートおよびパッチ適用

既定では、ダウンロードされたあらゆるアップデートとパッチが、次のアプリケーションコンポーネントに自動インストールされます：

- Windows 用のネットワークエージェント
- 管理コンソール
- iOS MDM サーバー

Kaspersky Security Center コンポーネントの自動アップデートおよびパッチ適用は Windows を実行しているデバイスでのみ使用できます。これらのコンポーネントの自動アップデートとパッチを無効にできます。この場合、ダウンロードされたあらゆるアップデートとパッチは、アップデートとパッチのステータスを［*承認*］へ変更した後にインストールされます。［*未定義*］ステータスのアップデートとパッチはインストールされません。

Kaspersky Security Center コンポーネントの自動アップデートおよびパッチ適用の有効化と無効化

Kaspersky Security Center コンポーネントのアップデートとパッチの自動インストールは、デバイスにネットワークエージェントをインストールする際に既定値で有効化されます。ネットワークエージェントのインストール中、あるいはインストール後にポリシーを使用して無効化することができます。

ネットワークエージェントをデバイスのローカルにインストール中、Kaspersky Security Center コンポーネントの自動アップデートとパッチを無効にするには：

1. デバイスへのネットワークエージェントのローカルインストールを開始します。

2. **詳細設定**ステップで、［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオフにします。

3. ウィザードの指示に従ってください。

Kaspersky Security Center コンポーネントの自動アップデートとパッチが無効にされたネットワークエージェントが、デバイスにインストールされます。ポリシーを使用して、自動アップデートとパッチを有効にできます。

インストールパッケージを介してネットワークエージェントをデバイスにインストール中に、Kaspersky Security Center コンポーネントの自動アップデートとパッチを無効にするには：

1. コンソールツリーで、［**リモートインストール**］→［**インストールパッケージ**］フォルダーの順に選択します。

2. 「**Kaspersky Security Center ネットワークエージェント <バージョン番号>**」パッケージのコンテキストメニューで、［**プロパティ**］を選択します。

3. インストールパッケージ内の［**設定**］セクションで、［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオフにします。

Kaspersky Security Center コンポーネントの自動アップデートとパッチが無効にされたネットワークエージェントが、このパッケージからインストールされます。ポリシーを使用して、自動アップデートとパッチを有効にできます。

デバイスにネットワークエージェントをインストール中に、このチェックボックスをオンにすると（またはオフにすると）、その後ネットワークエージェントポリシーを使用して自動アップデートを有効（または無効）にできます。

ネットワークエージェントポリシーを使用して、Kaspersky Security Center コンポーネントの自動アップデートとパッチを有効または無効にするには：

1. コンソールツリーで、自動アップデートとパッチを有効または無効にする管理グループを選択します。

2. グループの作業領域で、［**ポリシー**］タブを開きます。

3. ［**ポリシー**］タブで、ネットワークエージェントポリシーを選択します。

4. ポリシーのコンテキストメニューで［**プロパティ**］を選択します。
   ネットワークエージェントポリシーのプロパティウィンドウを表示します。

5. ポリシーのプロパティウィンドウで［**パッチとアップデートの管理**］セクションを選択します。

6. ［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオンまたはオフにして、自動アップデートとパッチを有効または無効にします。

7. このチェックボックスに「ロック」を設定します。

選択したデバイスにポリシーが適用され、Kaspersky Security Center コンポーネントの自動アップデートとパッチがデバイス上で有効（または無効）になります。

アップデートの自動配信

Kaspersky Security Center では、クライアントデバイスとセカンダリ管理サーバーにアップデートを自動的に配信してインストールすることができます。

クライアントデバイスへのアップデートの自動配信

特定のアプリケーションのアップデートが管理サーバーのリポジトリにダウンロードされた直後に、そのアップデートをクライアントデバイスに配信するには：

1. クライアントデバイスを管理する管理サーバーに接続します。
2. 次のいずれかの方法で、選択したクライアントデバイスにアップデートを配信するタスクを作成します：
   - 特定の管理グループに属するクライアントデバイスにアップデートを配信する必要がある場合は、特定のグループのタスクを作成します。
   - いくつかの管理グループにまたがるクライアントデバイスまたはどの管理グループにも属さないクライアントデバイスにアップデートを配信する必要がある場合は、特定のデバイスのタスクを作成します。

   新規タスクウィザードが起動します。指示に従って、次の操作を実行します：
   a. ［**タスク種別**］ウィザードウィンドウで、目的のアプリケーションのフォルダーにあるアップデート導入タスクを選択します。

      ［**タスク種別の選択**］ウィンドウに表示されるアップデート配信タスクの名前は、そのタスクを作成するアプリケーションによって異なります。選択したカスペルスキー製品のアップデートタスク名の詳細については、該当するガイドを参照してください。

   b. ［**スケジュール**］ウィザードウィンドウの［**実行予定**］で、［**新しいアップデートがリポジトリにダウンロードされ次第**］を選択します。

   アップデートが管理サーバーのリポジトリにダウンロードされるたびに、選択したデバイスに対して作成されたアップデート配信タスクが実行されます。

特定のデバイス向けに目的のアプリケーションのアップデートを配信するタスクが既に作成されている場合、アップデートをクライアントデバイスに自動的に配信するには、そのタスクのプロパティウィンドウの［**スケジュール**］セクションにある［**実行予定**］で、［**新しいアップデートがリポジトリにダウンロードされ次第**］を選択します。

セカンダリ管理サーバーへのアップデートの自動配信

選択したアプリケーションのアップデートがプライマリ管理サーバーのリポジトリにダウンロードされた直後に、そのアップデートをセカンダリ管理サーバーに配信するには：

1. コンソールツリーで、プライマリ管理サーバーのフォルダーにある［**タスク**］フォルダーを選択します。
2. 作業領域にあるタスクのリストで、管理サーバーでの管理サーバーのリポジトリへのアップデートのダウンロードタスクを選択します。
3. 次のいずれかの方法で、選択したタスクの［**設定**］セクションを開きます：

- タスクのコンテキストメニューで［**プロパティ**］を選択します。
- 選択したタスクの情報ボックスで、［**設定の編集**］をクリックします。

4. タスクのプロパティウィンドウの［**設定**］セクションで、［**その他の設定**］サブセクションを選択してから［**設定**］をクリックします。
5. ［**その他の設定**］ウィンドウが表示されたら、［**セカンダリ管理サーバーの強制アップデート**］をオンにします。

管理サーバーのアップデートダウンロードタスクの設定で、タスクのプロパティウィンドウの［**設定**］タブにある［**セカンダリ管理サーバーの強制アップデート**］をオンにします。

プライマリ管理サーバーがアップデートを取得すると、設定されたスケジュールに関係なく、アップデートのダウンロードタスクがセカンダリ管理サーバーで自動的に開始されます。

ディストリビューションポイントの自動的な割り当て

ディストリビューションポイント用デバイスは、自動的に割り当てることを推奨します。自動で行う場合、ディストリビューションポイントに指定するデバイスを Kaspersky Security Center が選択します。

ディストリビューションポイントを自動的に割り当てるには：

1. メインウィンドウを開きます。
2. コンソールツリーで、ディストリビューションポイントを自動的に割り当てる必要がある管理サーバーの名前が付けられたフォルダーを選択します。
3. 管理サーバーのコンテキストメニューから［**プロパティ**］をクリックします。
4. 管理サーバーのプロパティウィンドウの［**セクション**］ペインで、［**ディストリビューションポイント**］を選択します。
5. ウィンドウの右側で、［**ディストリビューションポイントを自動的に割り当て**］をオンにします。

ディストリビューションポイントとしてのデバイスの自動割り当てが有効な場合、手動でディストリビューションポイントを設定したりディストリビューションポイントのリストを編集したりすることはできません。

6. ［**OK**］をクリックします。

管理サーバーが自動的にディストリビューションポイントを割り当てて設定します。

ディストリビューションポイントとして動作するデバイスを手動で割り当てる

Kaspersky Security Center で、ディストリビューションポイントとして動作するデバイスを指定できます。

ディストリビューションポイント用デバイスは、自動的に割り当てることを推奨します。自動的に割り当てる場合、ディストリビューションポイントに指定するデバイスを Kaspersky Security Center が選択します。何らかの理由（たとえば、この用途専用で割り当てられたサーバーを使用する、など）により自動割り当てが選択できない場合、ディストリビューションポイント数の計算と設定を行った後に、手動でディストリビューションポイントを割り当てることができます。

ディストリビューションポイントとして動作するデバイスについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

ディストリビューションポイントとして動作するデバイスを手動で指定するには：

1. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウで、［**ディストリビューションポイント**］セクションを選択し、［**追加**］をクリックします。［**ディストリビューションポイントを手動で割り当て**］がオンになっていると、このボタンを使用できます。

   ［**ディストリビューションポイントの追加**］ウィンドウが表示されます。
4. ［**ディストリビューションポイントの追加**］ウィンドウで、次の操作を実行します：

   a. ディストリビューションポイントとして動作するデバイスを選択します（管理グループ内のデバイスを選択するか、デバイスの IP アドレスを指定します）。デバイスを選択する際は、ディストリビューションポイントの動作とディストリビューションポイントとして動作するデバイスの要件を確認してください。

   b. ディストリビューションポイントがアップデートを配信するデバイスを指定します。管理グループまたはネットワークロケーションの説明を指定できます。
5. ［OK］をクリックします。

   追加されたディストリビューションポイントが、［**ディストリビューションポイント**］セクションのディストリビューションポイントのリストに表示されます。
6. 新しく追加したディストリビューションポイントをリストから選択し、［**プロパティ**］をクリックして、プロパティウィンドウを開きます。
7. プロパティウィンドウでディストリビューションポイントを設定します。

   - ［**全般**］セクションには、ディストリビューションポイントとクライアントデバイスの間の通信の設定があります。
     - **SSL ポート**

       SSL を使用したクライアントデバイスとディストリビューションポイントの間の暗号化接続で使用する SSL ポートの番号。

       既定では、ポート 13000 が使用されます。
     - **マルチキャストを使用する**

このオプションをオンにすると、グループ内にあるクライアントデバイスへのインストールパッケージの自動配布に IP マルチキャストが使用されます。

IP マルチキャストを使用すると、インストールパッケージからクライアントデバイスのグループに製品をインストールするのに必要な時間が短縮されます。一方で、1 台のクライアントデバイスに製品をインストールする場合は、インストールの時間は長くなります。

- **マルチキャスト IP アドレス**

  マルチキャストで使用される IP アドレス。224.0.0.0 ～ 239.255.255.255 の範囲で IP アドレスを定義できます。

  既定では、Kaspersky Security Center は定められた範囲内で一意の IP マルチキャストアドレスを自動的に割り当てます。

- **IP マルチキャストポート番号**

  IP マルチキャストのポート番号。

  既定では、ポート番号は 15001 です。管理サーバーがインストールされたデバイスがディストリビューションポイントとして指定された場合、既定では SSL 接続でポート 13001 が使用されます。

- **アップデートの配布**

  アップデートは、次のアップデート元から管理対象デバイスに配布されます：

  - このオプションがオンの場合は、このディストリビューションポイントです。
  - このオプションがオフの場合は、管理サーバーやカスペルスキーのアップデートサーバーなどその他のディストリビューションポイントです。

  アップデートの配信にディストリビューションポイントを使用している場合は、ダウンロード数を減らすため、トラフィックを節約できます。また、管理サーバーの負荷を軽減し、ディストリビューションポイント間の負荷を移動することもできます。ネットワークのディストリビューションポイントの数を計算して、トラフィックと負荷を最適化できます。

  このオプションをオフにすると、アップデートのダウンロード数が増えて管理サーバーの負荷が増加する可能性があります。既定では、このオプションはオンです。

- **インストールパッケージの配布**

  インストールパッケージは、次の配布元から管理対象デバイスに配布されます：

  - このオプションがオンの場合は、このディストリビューションポイントです。
  - このオプションがオフの場合は、管理サーバーやカスペルスキーのアップデートサーバーなどその他のディストリビューションポイントです。

  インストールパッケージの配信にディストリビューションポイントを使用すると、ダウンロード数を減らすため、トラフィックを節約できます。また、管理サーバーの負荷を軽減し、ディストリビューションポイント間の負荷を移動することもできます。ネットワークのディストリビューションポイントの数を計算して、トラフィックと負荷を最適化できます。

  このオプションをオフにすると、アップデートのダウンロード数が増えて管理サーバーの負荷が増加する可能性があります。既定では、このオプションはオンです。

- **ディストリビューションポイントをプッシュサーバーとして使用する**

Kaspersky Security Center で、ディストリビューションポイントをモバイルプロトコルを使用して管理されているデバイスのプッシュサーバーとして動作させることができます。たとえば、KasperskyOS デバイスと管理サーバー間の強制同期を実行可能にする時に、プッシュサーバーを有効にする必要があります。プッシュサーバーの管理デバイスの範囲は、プッシュサーバーを有効にするディストリビューションポイントの範囲と同じです。同一の管理グループに複数のディストリビューションポイントを割り当てている場合は、各ディストリビューションポイントに対してプッシュサーバーを有効に設定できます。この場合、管理サーバーはディストリビューション間の負荷を分散します。

KasperskyOS をデバイスにインストール済みか、インストールする予定がある場合、ディストリビューションポイントをプッシュサーバーとして使用する必要があります。クライアントデバイスへプッシュ通知を送信する場合も、ディストリビューションポイントをプッシュサーバーとして使用できます。

- **プッシュサーバーのポート**

  クライアントデバイスが接続に使用するディストリビューションポイントのポート。既定では、ポート 13295 が使用されます。

- ［**範囲**］セクションで、ディストリビューションポイントがアップデートを配信する範囲を指定します（管理グループまたはネットワークロケーション）。

- ［**KSN プロキシ**］セクションでは、ディストリビューションポイントを使用して管理対象デバイスからの KSN リクエストを転送するようにアプリケーションを設定できます：

  - **ディストリビューションポイントで KSN プロキシを有効にする**

    ディストリビューションポイントとして使用しているデバイス上で KSN プロキシサービスが実行されます。この機能を使用することで、ネットワーク上でトラフィックを分配しなおし、最適化できます。

    ディストリビューションポイントは、Kaspersky Security Network に関する声明に記載されている KSN の統計情報をカスペルスキーに送信します。既定では、KSN 声明は「%ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula」にあります。

    既定では、このオプションはオフです。管理サーバーのプロパティウィンドウで、［**管理サーバーをプロキシサーバーとして使用する**］と［**Kaspersky Security Network への参加に同意する**］がオンになっている場合にのみ使用できます。

    アクティブ / パッシブモードのクラスターのノードをディストリビューションポイントに割り当て、ノード上で KSN プロキシサーバーを有効にできます。

  - **KSN リクエストを管理サーバーに転送する**

    ディストリビューションポイントは管理対象デバイスからの KSN リクエストを管理サーバーに転送します。

    既定では、このオプションはオンです。

  - **インターネット経由で直接 KSN クラウド / KPSN にアクセスする**

ディストリビューションポイントは管理対象デバイスからの KSN リクエストを KSN クラウドまたは KPSN に転送します。ディストリビューションポイント自体で生成された KSN リクエストも、KSN クラウドまたは KPSN に直接送信されます。

バージョン 11 以前のネットワークエージェントをインストールしているディストリビューションポイントでは、KPSN に直接アクセスできません。これらのディストリビューションポイントで KPSN リクエストを KPSN に送信するように設定を編集するには、各ディストリビューションポイントで［**KSN リクエストを管理サーバーに転送する**］をオンにします。

バージョン 12 以降のネットワークエージェントをインストールしているディストリビューションポイントでは、KPSN に直接アクセスできません。

- **KPSN への接続時に プロキシサーバーの設定を無視する**

  ディストリビューションポイントのプロパティまたはネットワークエージェントのポリシーでプロキシサーバー設定が構成済みであるにも関わらず、ネットワークアーキテクチャで KPSN を直接使用する必要がある場合は、このオプションをオンにします。このオプションをオンにしないと、管理対象アプリケーションからのリクエストが KPSN に到達できません。

  このオプションは［**インターネット経由で直接 KSN クラウド / KPSN にアクセスする**］をオンにした場合に使用できます。

- **TCP ポート**

  管理対象デバイスが KSN プロキシサーバーへの接続に使用する TCP ポートの番号。既定のポート番号は 13111 です。

- **UDP ポート**

  ネットワークエージェントが UDP ポートを経由して管理サーバーを接続する場合は、［**UDP ポートを使用**］をオンにして、［**UDP ポート番号**］を指定します。既定では、このオプションはオンです。管理サーバーに接続するための既定の UDP ポートは 15000 です。

- **HTTPS ポート**

  管理対象デバイスが HTTPS ポート経由で KSN プロキシサーバーに接続する必要がある場合は、［**HTTPS を使用する**］をオンにし、［**HTTPS の使用時に経由するポート**］の番号を指定します。HTTPS プロキシサーバーに接続する既定のポートは 17111 です。

- ［**デバイスの検索**］セクションで、ディストリビューションポイントによる、Windows ドメイン、Active Directory、および IP アドレス範囲のポーリングを設定します。

  - **Windows ドメイン**

    Windows ドメインに対するデバイスの検索を有効にし、スケジュールを設定できます。

  - **Active Directory**

Active Directory に対するネットワークのポーリングを有効にし、ポーリングのスケジュールを設定できます。

Windows ディストリビューションポイントを使用する場合は、次のオプションのいずれかをオンにできます：

- **現在の Active Directory ドメインのポーリング**
- **Active Directory ドメインフォレストのポーリング**
- **指定した Active Directory ドメインのみポーリング**：このオプションを選択した場合、1つ以上の Active Directory ドメインをリストに追加してください

ネットワークエージェント 15 がインストールされた Linux ディストリビューションポイントを使用する場合は、アドレスとユーザー資格情報を指定した Active Directory ドメインのみをポーリングできます。現在の Active Directory ドメインと Active Directory ドメインフォレストのポーリングは使用できません。

- **IP アドレス範囲**

デバイスの検索は IPv4 範囲および IPv6 ネットワークで有効にできます。

［**IP アドレス範囲のポーリングを有効にする**］をオンにすると、対象範囲を追加して実行スケジュールを設定できます。スキャン対象範囲のリストに IP アドレス範囲を追加できます。

［**Zeroconf を使用して IPv6 ネットワークのポーリングを実行する**］をオンにすると、ディストリビューションポイントは自動的にゼロコンフィギュレーションネットワーキング（「*Zeroconf*」とも表記）を使用して IPv6 ネットワークのポーリングを行います。この場合、ディストリビューションポイントはネットワーク全体を検索するため、指定した IP 範囲は無視されます。ディストリビューションポイントが Linux を実行している場合は、［**Zeroconf を使用して IPv6 ネットワークのポーリングを実行する**］を使用できます。Zeroconf IPv6 ポーリングを使用するには、ディストリビューションポイントで avahi-browse ユーティリティをインストールする必要があります。

- ［**詳細**］セクションで、配信されたデータの格納用にディストリビューションポイントが使用するフォルダーを指定します。
  - **既定のフォルダーを使用する**

このオプションをオンにすると、ディストリビューションポイント上でネットワークエージェントがインストールされているフォルダーが使用されます。

  - **指定したフォルダーを使用する**

このオプションをオンにすると、この下のフィールドで、フォルダーのパスを指定できます。ディストリビューションポイントのローカルフォルダーまたは組織ネットワーク内の任意のデバイス上にあるフォルダーを指定できます。

ネットワークエージェントの実行時にディストリビューションポイントで使用されるユーザーアカウントには、指定したフォルダーへの読み取りおよび書き込みアクセス権限が必要です。

選択されたデバイスがディストリビューションポイントとして使用されます。

Windows オペレーティングシステムが実行されているデバイスのみが、ネットワークロケーションを判別できます。他のオペレーティングシステムが実行されているデバイスのネットワークロケーションを判別することはできません。

ディストリビューションポイントのリストからデバイスを削除する

ディストリビューションポイントのリストからデバイスを削除するには：

1. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウの［**ディストリビューションポイント**］セクションで、ディストリビューションポイントとして動作するデバイスを選択して、［**削除**］をクリックします。

   デバイスがディストリビューションポイントのリストから削除され、ディストリビューションポイントとしてのデバイスの動作を停止します。

管理サーバーによって自動的に割り当てられたデバイスは、ディストリビューションポイントのリストから削除できません。

ディストリビューションポイントによるアップデートのダウンロード

Kaspersky Security Center では、ディストリビューションポイントはアップデートを管理サーバー、カスペルスキーのサーバー、ローカルまたはネットワークフォルダーから取得できます。

アップデート元を指定する必要がない場合は、管理グループの「*ディストリビューションポイントのリポジトリにアップデートをダウンロードする*」タスクを使用することを推奨します。詳細については、次のトピックを参照してください：ディストリビューションポイントのリポジトリへのアップデートプログラムのダウンロードタスクの作成。

ディストリビューションポイントによるアップデートのダウンロードを設定するには：

1. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウの［**ディストリビューションポイント**］セクションで、グループ内のクライアントデバイスにアップデートを配信するディストリビューションポイントを選択します。
4. ［**プロパティ**］をクリックして、選択したディストリビューションポイントのプロパティウィンドウを開きます。
5. ディストリビューションポイントのプロパティウィンドウで、［**アップデート元**］セクションを選択します。
6. ディストリビューションポイントのアップデート元を選択します：

- ディストリビューションポイントが管理サーバーからアップデートを取得できるようにするには、［**管理サーバーから取得**］をオンにします。
  - **差分ファイルのダウンロード**

    このオプションで差分ファイルのダウンロードを有効にすることができます。

    既定では、このオプションはオンです。

- このタスクを使用してディストリビューションポイントがアップデートを受信できるようにするには、［**アップデートの強制ダウンロードタスクを使用**］をオンにします：
  - そのようなタスクが既にデバイスに存在している場合、［**参照**］をクリックし、表示される一覧でタスクを選択します。
  - そのようなタスクがデバイスに存在しない場合、［**新規タスク**］をクリックし、タスクを作成します。新規タスクウィザードが起動します。ウィザードの指示に従ってください。

  ［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクはローカルタスクです。ディストリビューションポイントとして動作するデバイスごとに新規のタスクを作成する必要があります。

ディストリビューションポイントは指定されたアップデート元からアップデートを取得します。

リポジトリからのソフトウェアのアップデートの削除

管理サーバーのリポジトリからソフトウェアのアップデートを削除するには：

1. コンソールツリーの［**詳細**］フォルダーで、［**アプリケーションの管理**］フォルダーから［**ソフトウェアのアップデート**］サブフォルダーを選択します。
2. ［**ソフトウェアのアップデート**］フォルダーの作業領域で、削除するアップデートを選択します。
3. アップデートのコンテキストメニューで、［**アップデートファイルを削除**］を選択します。

ソフトウェアのアップデートが管理サーバーのリポジトリから削除されます。

クラスターモードでのカスペルスキー製品のパッチのインストール

Kaspersky Security Center のクラスターモードでは、カスペルスキー製品のパッチは手動インストールのみがサポートされます。

カスペルスキー製品のパッチをインストールするには：

1. クラスターのそれぞれのノードにパッチをダウンロードします。
2. アクティブなノードでパッチのインストールを実行します。

3. パッチが正常にインストールされるまで待ちます。

4. クラスターのすべてのサブノードで順にパッチを実行します。

   コマンドラインからパッチを実行する場合、 `-CLUSTER_SECONDARY_NODE` キーを使用します。

   パッチがクラスターの全ノードにインストールされます。

5. カスペルスキーのクラスターサービスを手動で実行します。

クラスターのすべてのノードが、ネットワークエージェントがインストールされたデバイスとして管理コンソールに表示されます。

インストールされたパッチの情報は、［**ソフトウェアのアップデート**］フォルダーか、カスペルスキー製品のソフトウェアモジュールに対するアップデートのバージョンに関するレポートで確認できます。

クライアントデバイス上のサードパーティ製品の管理

Kaspersky Security Center では、クライアントデバイスにインストールされたカスペルスキー製品とその他の製造元のアプリケーションを管理できます。

次の操作を実行できます：

- 指定した基準に基づいたアプリケーションカテゴリの作成
- 特別に作成したルールを使用したアプリケーションカテゴリの管理
- デバイス上のアプリケーション実行の管理
- デバイスにインストールされているソフトウェアのインベントリおよびレジストリの保守
- デバイスにインストールされているソフトウェアの脆弱性の修正
- Windows Update およびその他のソフトウェア開発元のアップデートのデバイスへのインストール
- ライセンス認証済みアプリケーショングループによるライセンス使用状況の監視

サードパーティ製ソフトウェアのアップデートのインストール

Kaspersky Security Center では、クライアントデバイスにインストールされたソフトウェアのアップデートを管理し、Microsoft 製アプリケーションや他のソフトウェア会社の製品に含まれる脆弱性を、必要なアップデートをインストールすることで修正できます。

Kaspersky Security Center は、アップデート検索タスクでアップデートを検索し、アップデートリポジトリにダウンロードします。アップデートの検索の完了後、適用可能なアップデートとそのアップデートによって修正できるアプリケーションの脆弱性に関する情報が管理者に提供されます。

Microsoft Windows の使用可能な更新プログラムの情報は、Windows Update サービスによって提供されます。管理サーバーは Windows Server Update Service（WSUS）サーバーとして使用できます。管理サーバーを WSUS サーバーとして使用するには、更新プログラムと Windows Update との同期を設定する必要があります。Windows Update とのデータの同期の設定が終わると、管理サーバーは一元管理モードで、また設定された頻度で、デバイス上の Windows Update サービスにアップデートを提供します。

また、ネットワークエージェントポリシーを使用してソフトウェアのアップデートを管理することもできます。これを行うには、新規ポリシーウィザードの対応するウィンドウで、ネットワークエージェントポリシーを作成し、ソフトウェアのアップデートを設定する必要があります。

［**アプリケーションの管理**］フォルダーの［**ソフトウェアのアップデート**］サブフォルダーで、適用可能なアップデートのリストを表示できます。このフォルダーには、管理サーバーが取得した、デバイスへ配信可能なMicrosoft アプリケーションやその他のソフトウェア会社の製品のアップデートのリストが含まれます。適用可能なアップデートの情報を確認した後、それらをデバイスにインストールできます。

Kaspersky Security Center はいくつかのアプリケーションについて、古いバージョンを削除して新しいバージョンをインストールして更新します。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

プライマリおよびセカンダリ管理サーバーの［**インターフェイスの設定**］ウィンドウで［**脆弱性とパッチ管理の表示**］がオンになっていることを確認します。それ以外の場合、アップデート検索タスクは WSUS アップデートのみを処理します。

セキュリティ上の理由から、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートすべてに対して、カスペルスキーの技術によるマルウェアのスキャンが自動的に実行されます。この技術は自動的なファイルのチェックに使用され、ウイルススキャン、Sandbox 環境における静的分析、動的分析、ふるまい分析、機械学習が含まれます。

カスペルスキーは、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートを手動で分析することはありません。さらに、カスペルスキーの専門家は脆弱性（既知または未知）や文書化されていないアップデートの機能について確認したり、上記で指定されているもの以外のアップデートの分析を行ったりすることはありません。

アップデートをすべてのデバイスにインストールする前に、テストインストールを実施して、インストールするアップデートによってデバイス上のアプリケーションの動作に異常が起きないかを確認できます。

Kaspersky Security Center を使用してアップデートできるサードパーティ製ソフトウェアの詳細情報は、テクニカルサポートサイトの Kaspersky Security Center ページにある「サーバー管理」セクションで確認できます。

シナリオ：サードパーティ製ソフトウェアのアップデート

このセクションでは、クライアントデバイスにインストールされているサードパーティ製ソフトウェアをアップデートするシナリオについて説明します。「サードパーティ製ソフトウェア」とは、Microsoft およびその他の製造元が提供しているアプリケーションを指します。Microsoft 製品のアップデートの情報は、Windows Update サービスによって提供されます。

必須条件

Microsoft 製品以外のサードパーティ製ソフトウェアのアップデートをインストールするには、管理サーバーはインターネットに接続している必要があります。

既定では、管理サーバーが管理対象デバイスに Microsoft 製品のアップデートをインストールするためにインターネット接続は必要ありません。たとえば、管理対象デバイスは、Microsoft Update サーバーから直接、または組織のネットワークに展開されている Microsoft Windows Server Update Services（WSUS）を使用して WindowsServer から、Microsoft ソフトウェアのアップデートをダウンロードできます。管理サーバーを WSUS サーバーとして使用する場合は、管理サーバーがインターネットに接続されている必要があります。

実行するステップ

サードパーティ製ソフトウェアのアップデートは段階的に進行します：

1. **必要なアップデートの検索**

   管理対象デバイスに必要なサードパーティ製ソフトウェアのアップデートを検索するには、［*脆弱性とアプリケーションのアップデートの検索*］タスクを実行します。タスクが完了すると、Kaspersky Security Center はタスクのプロパティで指定したデバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。

   ［*脆弱性とアプリケーションのアップデートの検索*］タスクは、管理サーバークイックスタートウィザードによって自動的に作成されます。ウィザードを実行していない場合は、次の手順に進む前にタスクを手動で作成するか、クイックスタートウィザードを実行してください。

   実行手順の説明：

   - 管理コンソール：アプリケーションの脆弱性スキャン、脆弱性とアプリケーションのアップデートの検索タスクのスケジュール設定
   - Kaspersky Security Center Web コンソール：脆弱性とアプリケーションのアップデートの検索タスクの作成、脆弱性とアプリケーションのアップデートの検索タスクの設定

2. **検出されたアップデートのリストの分析**

   ［**ソフトウェアのアップデート**］リストを確認して、どのアップデートをインストールするかを決定します。それぞれのアップデートの詳細情報を確認するには、リスト内のアップデートの名前をクリックします。リスト内のそれぞれのアップデートについて、クライアントデバイスへのアップデートのインストールに関する統計情報を表示することもできます。

   実行手順の説明：

   - 管理コンソール：適用可能なアップデートに関する情報の表示
   - Kaspersky Security Center Web コンソール：サードパーティ製品の使用可能なアップデートに関する情報の表示

3. **アップデートのインストールの設定**

   Kaspersky Security Center でサードパーティ製ソフトウェアのアップデートのリストの取得が完了すると、*アップデートのインストールと脆弱性の修正タスク*または *Windows Update 更新プログラムのインストール*タスクを使用して、クライアントデバイスにアップデートをインストールできます。いずれかのタスクを作成してください。［**タスク**］タブまたは［**ソフトウェアのアップデート**］リストを使用してこれらのタスクを作成できます。

   *アップデートのインストールと脆弱性の修正*タスクは、Windows Update サービス経由で提供される場合も含めた Microsoft アプリケーションのアップデートとその他の製造元の製品のアップデートのインストールに使用されます。このタスクは、脆弱性とパッチ管理機能を使用できるライセンスを使用している場合にのみ作成できます。

   ［*Windows Update 更新プログラムのインストール*］タスクを使用するために、特別なライセンスは必要ありません。ただし、インストールできるのは Windows Update の更新プログラムのみです。

   一部のソフトウェアのアップデートのインストールでは、インストールするために使用許諾契約書に同意する必要があります。使用許諾契約書に同意しない場合、アップデートはインストールされません。

アップデートのインストールタスクをスケジュールを指定して開始できます。タスクのスケジュールを指定する場合は、［*脆弱性とアプリケーションのアップデートの検索*］タスクが完了してからアップデートのインストールタスクが開始されるようにしてください。

実行手順の説明：

- 管理コンソール：アプリケーションの脆弱性の修正、適用可能なアップデートに関する情報の表示
- Kaspersky Security Center Web コンソール：の作成アップデートのインストールと脆弱性の修正タスク、Windows Update 更新プログラムのインストールタスクの作成、サードパーティ製品の使用可能なアップデートに関する情報の表示

4 タスクのスケジュール設定

アップデートのリストを最新の状態に維持するため、［*脆弱性とアプリケーションのアップデートの検索*］タスクが定期的に自動で実行されるようにスケジュールを指定してください。既定では、*脆弱性とアプリケーションのアップデートの検索*タスクは手動で開始するように設定されています。

*アップデートのインストールと脆弱性の修正*タスクを作成している場合は、実行頻度が*脆弱性とアプリケーションのアップデートの検索*タスクの実行頻度以下となるようにスケジュールを設定します。*Windows Update 更新プログラムのインストール*タスクのスケジュールを設定する場合は、タスクを実行する前に毎回、インストールするアップデートのリストを指定する必要があることに注意してください。

タスクのスケジュールを指定する場合は、*脆弱性とアプリケーションのアップデートの検索*タスクが完了してからアップデートのインストールタスクが開始されるようにしてください。

5 ソフトウェアアップデートの拒否と承認（必要に応じて実施）

アップデートのインストールと脆弱性の修正タスクを作成している場合は、タスクのプロパティでアップデートのインストールルールを指定できます。Windows Update 更新プログラムのインストールタスクを作成している場合は、この手順はスキップしてください。

それぞれのルールで、アップデートの次のようなステータスに応じて、インストールするアップデートを指定できます：*未定義*、*承認*、*拒否*。たとえば、サーバー向けのタスクとして、「*承認*」ステータスの Windows Update 更新プログラムのインストールのみを許可するようにルールを設定したタスクを設定するなどの使用方法が考えられます。この場合、インストールするアップデートに手動で「*承認*」ステータスを設定します。このように設定すると、Windows Update 更新プログラムでもステータスが「*未定義*」または「*拒否*」のアップデートは、タスクでインストール先に指定したサーバーにインストールされません。

アップデートのインストールを管理するための「*承認*」ステータスの使用は、アップデート量が少ない場合に効率的です。複数のアップデートをインストールするには、［*アップデートのインストールと脆弱性の修正*］タスクで構成できるルールを使用します。ルールで指定された基準を満たさない特定のアップデートに対してのみ、「*承認*」ステータスを設定することを推奨します。大量のアップデートを手動で承認すると、管理サーバーのパフォーマンスが低下し、サーバーが過負荷状態になる場合があります。

既定では、ダウンロードされたソフトウェアアップデートのステータスは「*未定義*」です。［**ソフトウェアのアップデート**］リストで、アップデートのステータスを「*承認*」または「*拒否*」に変更できます（［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動して操作）。

実行手順の説明：

- 管理コンソール：ソフトウェアアップデートの拒否と承認
- Kaspersky Security Center Web コンソール：サードパーティ製ソフトウェアのアップデートの拒否と承認

6 管理サーバーが Windows Server Update Service（WSUS）サーバーとして動作するように設定（省略可能）

既定では、Windows Update 更新プログラムは Microsoft のサーバーから管理対象デバイスにダウンロードされます。この設定を変更して、管理サーバーを WSUS サーバーとして使用するように設定できます。この場合、管理サーバーは指定した頻度で、Windows Update サービスとアップデートに関するデータの同期を実行し、ネットワークデバイスに一元的に Windows Update の更新プログラムを提供します。

管理サーバーを WSUS サーバーとして使用するには、Windows Update の同期の実行タスクを作成し、ネットワークエージェントのポリシーで［**管理サーバーを WSUS サーバーとして使用する**］をオンにする必要があります。

実行手順の説明：

- 管理コンソール：Windows Update の更新プログラムと管理サーバーとの同期、ネットワークエージェントポリシーでの Windows アップデートの設定
- Kaspersky Security Center Web コンソール：Windows Update の同期の実行タスクの作成

7. **アップデートのインストールタスクの実行**

   アップデートのインストールと脆弱性の修正タスクまたは *Windows Update 更新プログラムのインストール* タスクを開始します。これらのタスクを開始すると、管理対象デバイスにアップデートがダウンロードされインストールされます。タスクが完了したら、タスクリストでのタスクのステータスが［*正常終了*］になっていることを確認します。

8. **サードパーティ製ソフトウェアのアップデートのインストール結果のレポートの作成（省略可能）**

   アップデートのインストールに関する詳細な統計情報を確認するには、［**サードパーティ製ソフトウェアのアップデートのインストール結果に関するレポート**］を作成します。

   実行手順の説明：

   - 管理コンソール：レポートの作成と表示
   - Kaspersky Security Center Web コンソール：レポートの生成と表示

結果

*アップデートのインストールと脆弱性の修正*タスクを作成し設定した場合は、管理対象デバイスにアップデートが自動的にインストールされます。新しいアップデートが管理サーバーのリポジトリにダウンロードされると、Kaspersky Security Center はそのアップデートがアップデートルールで指定されている条件を満たすかどうかをチェックします。条件を満たす新しいアップデートはすべて、次回のタスク実行時に自動的にインストールされます。

*Windows Update 更新プログラムのインストール*タスクを作成した場合は、*Windows Update 更新プログラムのインストール*タスクのプロパティで指定したアップデートのみがインストールされます。タスクの作成後、管理サーバーのリポジトリにダウンロードされた新しいアップデートをインストールする場合は、既存のタスクに目的のアップデートを追加するか、新たに *Windows Update 更新プログラムのインストール*タスクを作成する必要があります。

サードパーティ製品で利用可能なアップデートに関する情報の表示

クライアントデバイスにインストールされたサードパーティ製ソフトウェアに対して適用可能なアップデートのリストを表示するには、

コンソールツリーの［**詳細**］→［**アプリケーションの管理**］フォルダーで、［**ソフトウェアのアップデート**］サブフォルダーを選択します。

フォルダーの作業領域に、デバイスにインストールされたアプリケーションに対して適用可能なアップデートのリストが表示されます。

アップデートのプロパティを表示するには：

［**ソフトウェアのアップデート**］フォルダーの作業領域で、アップデートのコンテキストメニューから［**プロパティ**］を選択します。

アップデートのプロパティウィンドウには、次の情報が表示されます：

- ［**全般**］セクションで、［**アップデート承認の状況**］を表示できます。：
  - **未定義** - アップデートはアップデートのリストにありますが、インストールは承認されていません。
  - **承認** - アップデートはアップデートのリストで使用可能であり、インストールが承認されています。
  - **承認却下** - アップデートのインストールが拒否されています。
- ［**属性**］セクションでは、［**自動的にインストール**］フィールドの値を表示できます：
  - *アップデートのインストールと脆弱性の修正*タスクがそのアプリケーションのアップデートをインストールできる場合には、［**自動**］が表示されます。タスクは製造元またはサードパーティ製品が提供するWebアドレスから新しいアップデートを自動的にインストールします。
  - Kaspersky Security Centerがそのアプリケーションのアップデートを自動的にインストールできない場合は[**手動**]が表示されます。アップデートを手動でインストールしてください。

  Windowsアプリケーションのアップデートに[**自動的にインストール**]は表示されません。
- アップデート対象のクライアントデバイスのリスト
- アップデート前にインストールする必要がある必須システムコンポーネントのリスト（存在する場合）
- アップデートにより修正されるソフトウェアの脆弱性

ソフトウェアアップデートの拒否と承認

アップデートのインストールタスクの設定によっては、インストールするアップデートの承認が必要な場合があります。インストールする必要のあるアップデートを承認し、インストールしないアップデートを拒否します。

たとえば、最初にテスト環境にアップデートをインストールしてデバイスのオペレーティングシステムとの互換性の問題が生じないかを確認してから、クライアントデバイスへのこれらのアップデートのインストールを許可することができます。

サードパーティのアップデートのインストールを管理するための「*承認*」ステータスの使用は、アップデート量が少ない場合に効率的です。複数のサードパーティのアップデートをインストールするには、*アップデートのインストールと脆弱性の修正*タスクで設定できるルールを使用します。ルールで指定された基準を満たさない特定のアップデートに対してのみ、「*承認*」ステータスを設定することを推奨します。大量のアップデートを手動で承認すると、管理サーバーのパフォーマンスが低下し、サーバーが過負荷状態になる場合があります。

1つ以上のアップデートを承認または拒否するには：

1. コンソールツリーで、［**詳細**］→［**アプリケーションの管理**］→［**ソフトウェアのアップデート**］フォルダーの順に選択します。

2. ［**ソフトウェアのアップデート**］フォルダーの作業領域で、右上端の［**更新**］をクリックします。アップデートリストが表示されます。

3. 承認または拒否するアップデートを選択します。

   作業領域の右側に選択したオブジェクトの情報ボックスが表示されます。

4. ［**アップデート承認の状況**］ドロップダウンリストで、選択したアップデートを承認する場合は［**承認**］を、拒否する場合は［**承認却下**］を選択します。

   既定値は **未定義** です。

［**承認**］ステータスを設定したアップデートは、インストールを待機するキューに置かれます。

［**承認却下**］が設定されたアップデートは、アップデートをインストール済みのすべてのデバイスからアンインストールされます（可能な場合）。また、今後これらのアップデートは他のデバイスに新規にインストールされません。

カスペルスキー製品の一部のアップデートはアンインストールできません。［**承認却下**］を設定した場合、Kaspersky Security Center は、これらのアップデートを、インストール済みのデバイスからアンインストールしません。しかし、今後これらのアップデートが他のデバイスに新規にインストールされることはありません。カスペルスキー製品のアップデートがアンインストールできない場合、アップデートのプロパティウィンドウの、［**セクション**］ペインの［**全般**］タブの作業領域で、［**インストールの要件**］にそのことが表示されます。サードパーティ製のソフトウェアアップデートに［**承認却下**］を設定すると、これらのアップデートは、アップデートのインストールを予定しているがまだインストールしていないデバイスにはインストールされません。このアップデートは、アップデートをインストール済みのデバイスにはそのまま残ります。アップデートを削除する時は、手動でローカル削除できます。

Windows Update の更新プログラムと管理サーバーとの同期

クイックスタートウィザードの［**アップデート管理設定**］ウィンドウで［**管理サーバーを WSUS サーバーとして使用する**］を選択した場合、［Windows Update の同期の実行］タスクが自動的に作成されます。作成されたタスクは、［**タスク**］フォルダーで実行できます。Microsoft ソフトウェアのアップデート機能は、**Windows Update の同期の実行**タスクが正常に完了した後にのみ使用可能になります。

Microsoft ソフトウェアのアップデートは 10 GB を超える場合があります。管理サーバーのデータベースがそのようなボリュームに対応できることを確認してください。そうしないと、［**Windows Update の同期の実行**］タスクが失敗します。Microsoft SQL Express データベースは、［**Windows Update の同期の実行**］タスクではサポートされていません。

Windows Update の同期の実行タスクは、メタデータのみを Microsoft のサーバーからダウンロードします。ネットワークで WSUS サーバーが使用されていない場合は、個々のクライアントデバイスが外部のサーバーから Microsoft のアップデートを個別にダウンロードします。

Windows Update と管理サーバーとを同期するタスクを作成するには：

1. コンソールツリーの［**詳細**］→［**アプリケーションの管理**］フォルダーで、［**ソフトウェアのアップデート**］サブフォルダーを選択します。

2. ［**その他の操作**］をクリックして、ドロップダウンリストで［**Windows Update との同期の設定**］を選択します。

   このウィザードは、［**タスク**］フォルダーに表示される **Windows Update の同期の実行**タスクを作成します。

Windows Update Center データ取得タスク作成ウィザードが起動します。ウィザードの指示に従ってください。

［**タスク**］フォルダーで［**タスクの作成**］をクリックして、［Windows Update の同期の実行］タスクを作成することもできます。

Microsoft 社では、古くなったアップデートを定期的に自社サーバーから削除し、現行のアップデートの数が常に 200,000 から 300,000 の間で保たれるようになっています。ディスク使用領域とデータベースサイズの削減を目的として、Kaspersky Security Center は、Microsoft Update サーバー上に存在しない古くなったアップデートを削除します。

Windows Update の同期の実行タスクの実行時に、本製品は Microsoft Update サーバーから現行のアップデート一覧を受信します。その後、本製品は古くなったアップデートの一覧を作成します。次に**脆弱性とアプリケーションのアップデートの検索**タスクを開始する時に、本製品はすべての古くなったアップデートにフラグを付け、削除までの時間を設定します。次に **Windows Update の同期の実行**タスクを開始する時に、30 日前に削除フラグが付けられたアップデートはすべて削除されます。また、フラグを付けてから 181 日以上経過しているアップデートの有無を確認し、あれば削除します。

Windows Update の同期の実行タスクが完了し、古くなったアップデートが削除されても、削除されたアップデートのファイルに属するハッシュコードがデータベース上に残っていることがあります。同様に、%AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles にある対応するファイルもデータベース上に残っていることがあります（それ以前にダウンロードされていた場合）。［**管理サーバーのメンテナンス**］タスクを実行して、定義データベースと対応するファイルからこれらの古いレコードを削除できます。

ステップ 1：トラフィックを削減するかどうかの定義

Kaspersky Security Center が Microsoft Windows Update Server のアップデートと同期すると、全ファイルに関する情報が管理サーバーのデータベースに保存されます。Windows Update エージェントとのやり取りの間、アップデートに必要なファイルもすべてドライブにダウンロードされます。具体的には、Kaspersky Security Center によって、高速インストールファイルに関する情報がデータベースに保存され、必要な時にこれらのファイルがダウンロードされます。高速インストールファイルをダウンロードすると、ドライブの空き容量が減少します。

ディスクの空き容量の減少を避け、トラフィックを減らすには、［**高速インストールファイルをダウンロード**］を無効にします。

このオプションを選択すると、タスクの実行時に高速インストールファイルがダウンロードされます。既定では、このオプションはオフです。

ステップ 2：アプリケーション

このセクションでは、アップデートをダウンロードする対象アプリケーションを選択できます。

［**全製品**］をオンにすると、すべての既存のアプリケーション、および今後リリースされる可能性のあるすべてのアプリケーションのアップデートがダウンロードされます。

既定では、［**全製品**］はオンになっています。

ステップ 3：アップデートのカテゴリ

このセクションでは、管理サーバーにダウンロードするアップデートのカテゴリを選択できます。

［**全カテゴリ**］をオンにすると、すべての既存のアップデートカテゴリ、および今後生じる可能性のあるすべてのカテゴリのアップデートがダウンロードされます。

既定では、［**全カテゴリ**］はオンになっています。

ステップ 4：アップデートの言語

このウィンドウでは、管理サーバーにダウンロードするアップデートの言語を選択できます。アップデートのローカリゼーション言語をダウンロードするために、次のオプションのいずれかを選択します：

- **新しい言語を含むすべての言語をダウンロード**

  このオプションをオンにすると、使用可能なすべての言語のアップデートを管理サーバーにダウンロードできます。既定では、このオプションがオンです。

- **特定の言語をダウンロード**

  このオプションをオンにすると、管理サーバーにダウンロードするアップデートの言語をリストから選択できます。

ステップ 5：タスクを開始するアカウントの選択

［**タスクを実行するアカウントの選択**］ウィンドウで、タスクの実行時に使用するアカウントを指定できます。次のいずれかのオプションをオンにします：

- **既定のアカウント**

  タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。

  既定では、このオプションがオンです。

- **アカウントの指定**

  ［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

  - **アカウント**

    タスクを実行するアカウント。

  - **パスワード**

タスクが実行されるアカウントのパスワード。

ステップ 6：タスク開始スケジュールの設定

［**タスクスケジュールの設定**］ウィザードウィンドウで、タスク開始のスケジュールを作成できます。必要に応じて、次の設定を指定します：

- **実行予定：**

  タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

  - **N 時間ごと**

    指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

    既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

  - **N 日ごと**

    日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

    既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

  - **N 週間ごと**

    指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

    既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

  - **N 分ごと**

    タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

    既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

  - **毎日（サマータイムはサポートしていません）**

    日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を 1 時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

    このスケジュールの使用は推奨されません。Kaspersky Security Center の旧バージョンとの後方互換性を維持するために用意されているオプションとなります。

    既定では、毎日、現在のシステム時刻にタスクが実行されます。

  - **毎週**

毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。
  既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。
  指定した日付が存在しない月には、月の最終日にタスクを実行します。
  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **1回**

  タスクは、指定された日時に 1 回実行されます (既定では、タスクが作成された日)。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。
  規定では、日付は選択されていません。規定の開始時間は18:00 です。

- **ウイルスアウトブレイク検知次第**

  ［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：
  - ワークステーションとファイルサーバー向けアンチウイルス製品
  - 境界防御向けアンチウイルス製品
  - メールサーバー向けアンチウイルス製品

  既定では、すべてのアプリケーション種別がオンです。
  ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

- タスク名で検索するには、検索フィールドにタスク名を入力します。
- 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。
  既定では、タスクはアルファベットの昇順で並べ替えられます。
- フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

  このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

  このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

  このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

  既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる(分)**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

既定では、このオプションはオフです。既定の時間は1分です。

ステップ7：タスク名の定義

［**タスク名の定義**］ウィンドウで、作成中のタスク名を指定します。タスク名は100文字以下で、特殊文字（**"*<>?\:|**）を含めることはできません。既定値は「*Windows Update の同期の実行*」です。

ステップ8：タスクの作成完了

［**タスク作成の終了**］ウィンドウで、［**終了**］をクリックしてウィザードを終了します。

ウィザード終了後にすぐにタスクを開始するには、［**ウィザードの終了後にタスクを実行**］をオンにします。

新しく作成したWindows Updateの同期タスクは、コンソールツリーの［**タスク**］フォルダーのタスクのリストに表示されます。

デバイスでの手動によるアップデートのインストール

クイックスタートウィザードの［**アップデート管理設定**］ページで［**必要なアップデートの検索とインストール**］を選択した場合、*アップデートのインストールと脆弱性の修正*タスクが自動的に作成されます。［**管理対象デバイス**］フォルダーの［**タスク**］タブでタスクの実行または停止を行うことができます。

クイックスタートウィザードで［**必要なアップデートの検索**］を選択した場合、［*アップデートのインストールと脆弱性の修正*］タスクによりクライアントデバイスでソフトウェアのアップデートをインストールできます。

次の操作を実行できます：

- アップデートのインストールタスクを作成する。
- 既存のアップデートインストールタスクにアップデートのインストールのルールを追加する。
- 既存のアップデートインストールタスクの設定で、アップデートのテストインストールを設定する。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

インストールタスクの作成によるアップデートのインストール

次の操作を実行できます：

- 特定のアップデートのインストールタスクを作成する。
- アップデートを選択し、同一および類似のアップデートのインストールタスクを作成する。

特定のアップデートをインストールするには：

1. コンソールツリーの［**詳細**］→［**アプリケーションの管理**］フォルダーで、［**ソフトウェアのアップデート**］サブフォルダーを選択します。
2. 作業領域で、インストールするアップデートを選択します。
3. 次のいずれかの手順を実行します：
   - 選択したアップデートのリストからいずれかを右クリックし、［**アップデートのインストール**］→［**新規タスク**］の順に選択する。
   - 選択したアップデートの情報ボックスで、［**アップデートのインストール（タスクの作成）**］をクリックする。
4. アプリケーションの以前のアップデートをインストールするかを確認するダイアログで、いずれかを選択します。選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、［**はい**］をクリックします。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、［**いいえ**］をクリックします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

   アップデートのインストールと脆弱性修正タスク作成ウィザードが起動します。ウィザードの指示に従ってください。
5. ウィザードの［**オペレーティングシステムの再起動のオプションを選択**］ウィンドウで、タスク完了後にクライアントデバイスのオペレーティングシステムの再起動が必要になった場合の処理を選択します。
   - **デバイスを再起動しない**

     操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。
   - **デバイスを再起動する**

     インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。
   - **ユーザーに処理を確認する**

手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

既定では、このオプションがオンです。

- **通知の繰り返し間隔（分）**

  このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

  既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

  このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

- **再起動するまでの時間（分）**

  ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

  既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

6. ウィザードの［**タスクスケジュールの設定**］ページで、タスク開始のスケジュールを作成できます。必要に応じて、次の設定を指定します：

- **実行予定：**

  タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

- **N 時間ごと**

  指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

  既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

- **N 日ごと**

日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

既定では、現在のシステム日時から、1日ごとにタスクが実行されます。

- **N週間ごと**

  指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

  既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

- **N分ごと**

  タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

  既定では、現在のシステム時刻から、30分ごとにタスクが実行されます。

- **毎日（サマータイムはサポートしていません）**

  日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を1時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

  このスケジュールの使用は推奨されません。Kaspersky Security Centerの旧バージョンとの後方互換性を維持するために用意されているオプションとなります。

  既定では、毎日、現在のシステム時刻にタスクが実行されます。

- **毎週**

  毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後6時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。

  指定した日付が存在しない月には、月の最終日にタスクを実行します。

  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。

  規定では、日付は選択されていません。規定の開始時間は18:00 です。

- **ウイルスアウトブレイク検知次第**

  ［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

  - ワークステーションとファイルサーバー向けアンチウイルス製品
  - 境界防御向けアンチウイルス製品
  - メールサーバー向けアンチウイルス製品

  既定では、すべてのアプリケーション種別がオンです。

  ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

  他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

  テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

  必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

  - タスク名で検索するには、検索フィールドにタスク名を入力します。
  - 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。

    既定では、タスクはアルファベットの昇順で並べ替えられます。
  - フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

  このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

  このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

  このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

  既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる(分)**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  既定では、このオプションはオフです。既定の時間は1分です。

7. ウィザードの［**タスク名の定義**］ウィンドウで、作成中のタスク名を指定します。タスク名は100文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

8. ［**タスク作成の終了**］ウィンドウで、［**終了**］をクリックしてウィザードを終了します。

   ウィザード終了後にすぐにタスクを開始するには、［**ウィザードの終了後にタスクを実行**］をオンにします。

ウィザードが完了すると、［**アップデートのインストールと脆弱性の修正**］タスクが［**タスク**］フォルダーに表示されます。

*アップデートのインストールと脆弱性の修正*タスクのプロパティで、アップデートのインストール前にシステムコンポーネント（前提条件）の自動インストールを有効にすることができます。このオプションがオンになっていると、アップデートの前にすべての必須システムコンポーネントがインストールされます。必須コンポーネントのリストは、アップデートのプロパティで確認できます。

*アップデートのインストールと脆弱性の修正*タスクのプロパティでは、製品を新しいバージョンにアップグレードするアップデートのインストールを許可することができます。

タスクの設定で、サードパーティ製品のアップデートをインストールするルールが設定されている場合、管理サーバーは必要なアップデートをそれぞれの開発元のWebサイトからダウンロードします。アップデートは管理サーバーのリポジトリに保存され、適用可能なデバイスに配信されてインストールされます。

タスクの設定で、Microsoft製品のアップデートをインストールするルールが設定されており、管理サーバーがWSUSサーバーとして動作するよう設定されている場合、管理サーバーが必要なすべてのアップデートをリポジトリにダウンロードし、管理対象デバイスに配信します。ネットワークでWSUSサーバーが使用されていない場合は、個々のクライアントデバイスが外部のサーバーからMicrosoftのアップデートを個別にダウンロードします。

特定のアップデートおよび類似のアップデートをインストールするには：

1. コンソールツリーの［**詳細**］→［**アプリケーションの管理**］フォルダーで、［**ソフトウェアのアップデート**］サブフォルダーを選択します。

2. 作業領域で、インストールするアップデートを選択します。

3. ［**アップデートのインストールウィザードを実行**］をクリックします。
   アップデートのインストールウィザードが起動します。

   > アップデートのインストールウィザードは、脆弱性とパッチ管理 ライセンスがある場合のみ使用できます。

   ウィザードの指示に従ってください。

4. ［**既存のアップデートインストールタスクを検索する**］ウィンドウで、次の設定を指定します：

   - **このアップデートをインストールするタスクを検索する**

     このオプションをオンにすると、アップデートのインストールウィザードで、選択したアップデートをインストールする既存のタスクが検索されます。

     このオプションがオフまたは該当するタスクが見つからなかった場合、アップデートのインストールウィザードで、アップデートをインストールするルールまたはタスクを作成するように要求されます。

     既定では、このオプションはオンです。

   - **アップデートのインストールを承認する**

     選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

     既定では、このオプションはオフです。

5. ［既存のアップデートインストールタスクを検索する］をオンにして、該当するタスクが見つかった場合、これらのタスクのプロパティを表示したり手動で開始することができます。追加の操作は必要ありません。
   これが当てはまらない場合は、［**新しいアップデートインストールタスク**］をクリックします。

6. 新しいタスクに追加するインストールルールの種別を選択し、［**終了**］をクリックします。

7. アプリケーションの以前のアップデートをインストールするかを確認するダイアログで、いずれかを選択します。選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、［**はい**］をクリックします。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、［**いいえ**］をクリックします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。
   アップデートのインストールと脆弱性修正タスク作成ウィザードが起動します。ウィザードの指示に従ってください。

8. ウィザードの［**オペレーティングシステムの再起動のオプションを選択**］ウィンドウで、タスク完了後にクライアントデバイスのオペレーティングシステムの再起動が必要になった場合の処理を選択します。

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

  - **通知の繰り返し間隔（分）**

    このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

    既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

    このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

  - **再起動するまでの時間（分）**

    ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

    既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

9. ウィザードの［**タスクを割り当てるデバイスの選択**］ページで、次のいずれかのオプションをオンにします：

- **ネットワークの管理サーバーによって検出されたデバイスを選択する**

  タスクを特定のデバイスに割り当てます。特定のデバイスには、管理グループに属するデバイスと管理グループが割り当てられていないデバイスの両方を含めることができます。

  たとえば、未割り当てデバイスでネットワークエージェントのインストールタスクを実行する時に、このオプションを使用すると便利です。

- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

  タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

  特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

- **デバイスの抽出にタスクを割り当てる**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

- **管理グループにタスクを割り当てる**

  任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

  たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

  タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

10. ウィザードの［**タスクスケジュールの設定**］ページで、タスク開始のスケジュールを作成できます。必要に応じて、次の設定を指定します：

- **実行予定：**

  タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

  - **N 時間ごと**

    指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

    既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

  - **N 日ごと**

日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

既定では、現在のシステム日時から、1日ごとにタスクが実行されます。

- **N週間ごと**

  指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

  既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

- **N分ごと**

  タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

  既定では、現在のシステム時刻から、30分ごとにタスクが実行されます。

- **毎日（サマータイムはサポートしていません）**

  日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を1時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

  このスケジュールの使用は推奨されません。Kaspersky Security Centerの旧バージョンとの後方互換性を維持するために用意されているオプションとなります。

  既定では、毎日、現在のシステム時刻にタスクが実行されます。

- **毎週**

  毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後6時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。

  指定した日付が存在しない月には、月の最終日にタスクを実行します。

  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **手動**（既定で選択）

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。

  規定では、日付は選択されていません。規定の開始時間は18:00 です。

- **ウイルスアウトブレイク検知次第**

  ［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

  - ワークステーションとファイルサーバー向けアンチウイルス製品
  - 境界防御向けアンチウイルス製品
  - メールサーバー向けアンチウイルス製品

  既定では、すべてのアプリケーション種別がオンです。

  ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

  他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

  テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

  必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

  - タスク名で検索するには、検索フィールドにタスク名を入力します。
  - 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。

    既定では、タスクはアルファベットの昇順で並べ替えられます。
  - フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

  このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

  このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

  このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

  既定では、このオプションはオフです。

- **タスクの開始を次の時間範囲内でランダムに遅延させる(分)**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる(分)**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  既定では、このオプションはオフです。既定の時間は1分です。

11. ウィザードの［**タスク名の定義**］ウィンドウで、作成中のタスク名を指定します。タスク名は100文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

12. ［**タスク作成の終了**］ウィンドウで、［**終了**］をクリックしてウィザードを終了します。

    ウィザード終了後にすぐにタスクを開始するには、［**ウィザードの終了後にタスクを実行**］をオンにします。

ウィザードが完了すると、［**アップデートのインストールと脆弱性の修正**］タスクが作成され、［**タスク**］フォルダーに表示されます。

タスクの作成時に指定した設定およびタスクのその他のプロパティは、いつでも変更できます。

本製品を新しいバージョンにアップデートすることにより、デバイス上の本製品に依存するアプリケーションが正しく動作しなくなることがあります。

既存のインストールタスクへのルールの追加によるアップデートのインストール

既存のインストールタスクにルールを追加してアップデートをインストールするには：

1. コンソールツリーの［**詳細**］→［**アプリケーションの管理**］フォルダーで、［**ソフトウェアのアップデート**］サブフォルダーを選択します。

2. 作業領域で、インストールするアップデートを選択します。

3. ［**アップデートのインストールウィザードを実行**］をクリックします。

   アップデートのインストールウィザードが起動します。

アップデートのインストールウィザードは、脆弱性とパッチ管理 ライセンスがある場合のみ使用できます。

ウィザードの指示に従ってください。

4. ［**既存のアップデートインストールタスクを検索する**］ウィンドウで、次の設定を指定します：

   - **このアップデートをインストールするタスクを検索する**

     このオプションをオンにすると、アップデートのインストールウィザードで、選択したアップデートをインストールする既存のタスクが検索されます。

     このオプションがオフまたは該当するタスクが見つからなかった場合、アップデートのインストールウィザードで、アップデートをインストールするルールまたはタスクを作成するように要求されます。

     既定では、このオプションはオンです。

   - **アップデートのインストールを承認する**

     選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

     既定では、このオプションはオフです。

5. ［既存のアップデートインストールタスクを検索する］をオンにして、該当するタスクが見つかった場合、これらのタスクのプロパティを表示したり手動で開始することができます。追加の操作は必要ありません。

   いずれも該当しない場合は、［**アップデートのインストールルールを追加する**］をクリックします。

6. ルールを追加するタスクを選択し、［**ルールの追加**］をクリックします。

   既存のタスクのプロパティを表示したり、タスクを手動で作成したり、新規タスクを作成することもできます。

7. 選択したタスクに追加するルールの種別を選択し、［**終了**］をクリックします。

8. アプリケーションの以前のアップデートをインストールするかを確認するダイアログで、いずれかを選択します。選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、［**はい**］をクリックします。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、［**いいえ**］をクリックします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

既存の**アップデートのインストールと脆弱性の修正**タスクに新しいアップデートのインストールルールが追加されます。

アップデートのテストインストールの設定

アップデートのテストインストールを設定するには：

1. コンソールツリーで、［**管理対象デバイス**］フォルダーの［**タスク**］タブのアップデートのインストールと脆弱性の修正タスクを選択します。

2. タスクのコンテキストメニューで［**プロパティ**］を選択します。

   アップデートのインストールと脆弱性の修正タスクのプロパティウィンドウが開きます。

3. タスクのプロパティウィンドウの［**テストインストール**］セクションで、テストインストールに使用可能なオプションの1つを選択します。

   - **スキャンしない**：アップデートのテストインストールを実行しない場合は、このオプションを選択します。

   - **選択されたデバイスでスキャンを実行**：選択したデバイスでアップデートのインストールをテストする場合、このオプションを選択します。［**追加**］をクリックし、アップデートのテストインストールを実行するデバイスを選択します。

   - **指定されたグループのデバイスでスキャンを実行**：特定のグループ内のデバイスでアップデートのインストールをテストする場合、このオプションを選択します。［**テストグループの指定**］に、テストインストールを実行するデバイスのグループを指定します。

   - **指定された割合のデバイスにスキャンを実行**：デバイスの一部でアップデートのインストールをテストする場合、このオプションを選択します。［**対象の全デバイス内でテストデバイスが占める割合**］に、アップデートのテストインストールを実行するデバイスの割合をパーセントで指定します。

4. ［**スキャンしない**］以外のいずれかのオプションを選択する時には、［**インストールを続行するかどうかを判定する時間（時間）**］で、アップデートのテストインストールを行ってからすべてのデバイスに対してアップデートのインストールを開始するまでの待機時間を指定します。

ネットワークエージェントポリシーでの Windows アップデートの設定

ネットワークエージェントポリシーで Windows アップデートを設定するには：

1. コンソールツリーで、［**管理対象デバイス**］を選択します。

2. 作業領域で、［**ポリシー**］タブを選択します。

3. ネットワークエージェントのポリシーを選択します。

4. ポリシーのコンテキストメニューで［**プロパティ**］を選択します。

   ネットワークエージェントポリシーのプロパティウィンドウが表示されます。

5. ［**セクション**］ペインで、［**ソフトウェアのアップデートと脆弱性**］を選択します。

6. Windows アップデートを管理サーバーにダウンロードしてからネットワークエージェントを使用してクライアントデバイスに配信するには、［**管理サーバーを WSUS サーバーとして使用する**］をオンにします。

   このオプションをオフにすると、Windows 更新プログラムが管理サーバーにダウンロードされません。この場合、クライアントデバイスが Microsoft のサーバーから直接 Windows アップデートを受信します。

7. ユーザーが Windows Update サービスを使用してデバイスに手動でインストールできるアップデートを選択します。

Windows 10 を実行しているデバイスで、デバイスに適用可能な更新プログラムが Windows Update 内で既に検出されている場合、［**Kaspersky Security Center 11 がインストールされた管理サーバーデバイスが WSUS サーバーとして使用されている場合に、バージョン 11 以降のネットワークエージェントがインストールされたデバイス上で、Windows Update 更新プログラムのインストールをユーザーが管理することを許可する**］は、検出された更新プログラムがインストールされた後に適用されます。

ドロップダウンリストからオプションを選択します：

- **Windows Update のすべての適用可能な更新プログラムのインストールをユーザーに許可する**

  ユーザーは、デバイスに適用可能な Microsoft Windows Update のすべての更新プログラムをインストールできます。

  アップデートのインストールをブロックしない場合は、このオプションを選択します。

  ユーザーが Microsoft Windows Update の更新プログラムを手動でインストールする時、更新プログラムを管理サーバーからではなく Microsoft サーバーからダウンロードする場合があります。これは、管理サーバーが対象の更新プログラムをまだダウンロードしていない場合に起こります。Microsoft サーバーから更新プログラムをダウンロードすると、トラフィック量が増加します。

- **Windows Update の承認された更新プログラムのみのインストールをユーザーに許可する**

  ユーザーは、デバイスに適用可能で管理者に承認された Microsoft Windows Update のすべての更新プログラムをインストールできます。

  たとえば、最初にテスト環境にアップデートをインストールしてデバイスのオペレーティングシステムとの互換性の問題が生じないかを確認してから、クライアントデバイスへの承認されたアップデートのインストールを許可することができます。

  ユーザーが Microsoft Windows Update の更新プログラムを手動でインストールする時、更新プログラムを管理サーバーからではなく Microsoft サーバーからダウンロードする場合があります。これは、管理サーバーが対象の更新プログラムをまだダウンロードしていない場合に起こります。Microsoft サーバーから更新プログラムをダウンロードすると、トラフィック量が増加します。

- **Windows Update 更新プログラムのインストールをユーザーに許可しない**

  ユーザーは、デバイスに Microsoft Windows Update の更新プログラムを手動でインストールできません。すべての適用可能な更新プログラムは、管理者の設定に従ってインストールされます。

  アップデートのインストールを一元的に管理する場合は、このオプションをオンにします。

  たとえば、ネットワークの過負荷を避けるために、アップデートのスケジュールを最適化したい場合などです。ユーザーの業務に支障をきたさないように、業務時間外にアップデートをスケジュールすることができます。

8. Windows Update 検索モード：

- **アクティブ**

このオプションをオンにすると、管理サーバーがネットワークエージェントのサポートにより、クライアントデバイス上の Windows Update エージェントからアップデート元である Windows Update Server または WSUS への要求を開始します。次に、ネットワークエージェントが、Windows Update エージェントから受け取った情報を管理サーバーに渡します。

このオプションは、*脆弱性とアプリケーションのアップデートの検索*タスクで［**アップデートサーバーに接続してアップデートを取得**］が選択されている場合にのみ有効になります。

既定では、このオプションがオンです。

- **パッシブ**

  このオプションをオンにすると、ネットワークエージェントは、Windows Update エージェントとアップデート元との前回の同期で取得した更新プログラムの情報を定期的に管理サーバーに渡します。Windows Update エージェントとアップデート元が同期されない場合、管理サーバー上のアップデートの情報が最新ではなくなります。

  アップデート元のメモリキャッシュからアップデートを取得する場合は、このオプションを選択します。

- **無効**

  このオプションをオンにすると、管理サーバーは更新プログラムに関する情報を要求しません。

  このオプションは、たとえば手元のローカルデバイスで最初にアップデートをテストしたい場合などに選択します。

9. 実行ファイルの実行中に、そのファイルの脆弱性をスキャンする場合、［**実行ファイルの開始時に脆弱性をスキャンする**］をオンにします。
10. 変更したすべての設定で編集がロックされていることを確認してください。それ以外の場合、変更は適用されません。
11. ［**適用**］をクリックします。

サードパーティ製ソフトウェアの脆弱性の修正

このセクションでは、管理対象デバイスにインストールされているソフトウェアの脆弱性の修正に関連する Kaspersky Security Center の機能について説明します。

シナリオ：サードパーティ製ソフトウェアの脆弱性の検知と修正

このセクションでは Windows オペレーティングシステムを使用しているデバイスで、脆弱性を検知し修正する方法について説明しています。オペレーティングシステムとサードパーティ製ソフトウェア（Microsoft 製品を含む）の脆弱性の検知と修正を実行できます。

必須条件

- 組織内に Kaspersky Security Center が導入されている。

- 組織内に Windows を使用している管理対象デバイスが存在する。
- 管理サーバーで次のタスクを実行する場合は、インターネット接続が必要になります。
  - Microsoft ソフトウェアの脆弱性に対して推奨される修正のリストを作成する。このリストは、カスペルスキーのスペシャリストにより作成され、定期的に更新されます。
  - Microsoft ソフトウェア以外のサードパーティ製ソフトウェアで脆弱性を修正する。

実行するステップ

ソフトウェアの脆弱性の検知と修正は、次の手順で進みます：

1. **管理対象デバイスにインストールされているソフトウェアの脆弱性のスキャン**

   管理対象デバイスにインストールされているソフトウェアの脆弱性を検知するには、［*脆弱性とアプリケーションのアップデートの検索*］タスクを実行します。タスクが完了すると、Kaspersky Security Center はタスクのプロパティで指定したデバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。

   *脆弱性とアプリケーションのアップデートの検索*タスクは、Kaspersky Security Center のクイックスタートウィザードによって自動的に作成されます。ウィザードを実行していない場合は、次の手順に進む前にウィザードを実行するか手動でタスクを作成してください。

   実行手順の説明：

   - 管理コンソール：アプリケーションの脆弱性スキャン、脆弱性とアプリケーションのアップデートの検索タスクのスケジュール設定
   - Kaspersky Security Center Web コンソール：脆弱性とアプリケーションのアップデートの検索タスクの作成、脆弱性とアプリケーションのアップデートの検索タスクの設定

2. **検知されたソフトウェアの脆弱性の分析**

   ［**ソフトウェアの脆弱性**］リストを確認して、どの脆弱性を修正するかを決定します。それぞれの脆弱性の詳細情報を確認するには、リスト内の脆弱性の名前をクリックします。リスト内のそれぞれの脆弱性について、管理対象デバイス上の脆弱性に関する統計情報を表示することもできます。

   実行手順の説明：

   - 管理コンソール：ソフトウェアの脆弱性に関する情報の表示、管理対象デバイス上の脆弱性に関する統計情報の表示
   - Kaspersky Security Center Web コンソール：ソフトウェアの脆弱性に関する情報の表示、管理対象デバイス上の脆弱性に関する統計情報の表示

3. **脆弱性の修正の設定**

   管理対象デバイス上でソフトウェアの脆弱性が検知された場合、［*アップデートのインストールと脆弱性の修正*］タスクまたは［*脆弱性の修正*］タスクを使用して、ソフトウェア脆弱性を修正できます。

   ［*アップデートのインストールと脆弱性の修正*］タスクは、管理対象デバイス上で Microsoft 製品やその他のサードパーティ製ソフトウェアの脆弱性をアップデートによって修正するために使用します。このタスクを使用することで、一定のルールに従って複数のアップデートをインストールしたり、複数の脆弱性を修正したりすることができます。このタスクは、脆弱性とパッチ管理機能を利用できるライセンスを使用している場合にのみ作成できます。ソフトウェア脆弱性を修正するために、*アップデートのインストールと脆弱性の修正*タスクは推奨されるソフトウェアアップデートを使用します。

*脆弱性の修正*タスクは、脆弱性とパッチ管理機能を使用できるライセンスがなくても使用できます。このタスクを使用するには、タスクの設定で、サードパーティ製ソフトウェアの脆弱性を修正するために使用するユーザー修正を手動で指定する必要があります。*脆弱性の修正*タスクでは、Microsoft 製品に対しては推奨される修正を、その他のサードパーティ製ソフトウェアに対してはユーザー修正をインストールして脆弱性を修正します。

脆弱性修正ウィザードを起動すると、これらのタスクのいずれかを自動的に作成できます。または、手動でタスクを作成することもできます。

実行手順の説明：

- 管理コンソール：サードパーティ製ソフトウェアの脆弱性へのユーザー修正の選択、アプリケーションの脆弱性の修正
- Kaspersky Security Center Web コンソール：サードパーティ製ソフトウェアの脆弱性へのユーザー修正の選択、サードパーティ製ソフトウェアの脆弱性の修正、アップデートのインストールと脆弱性の修正タスクの作成

4 タスクのスケジュール設定

脆弱性のリストを最新の状態に維持するため、［*脆弱性とアプリケーションのアップデートの検索*］タスクが定期的に自動で実行されるようにスケジュールを指定してください。推奨される平均的なタスクの実行頻度は週に1回です。

［*アップデートのインストールと脆弱性の修正*］タスクを作成している場合は、実行頻度を［*脆弱性とアプリケーションのアップデートの検索*］と同じかそれよりも少なくします。*脆弱性の修正*タスクのスケジュールを設定する場合は、タスクを開始する前に、毎回 Microsoft 製品の修正を選択するか、サードパーティ製ソフトウェアのユーザー修正を指定する必要があることに注意してください。

タスクのスケジュールを指定する場合は、［*脆弱性とアプリケーションのアップデートの検索*］タスクが完了してからこれらのタスクが開始するようにしてください。

5 検知されたソフトウェアの脆弱性への非対応の判断（必要に応じて実施）

必要に応じて、すべてのデバイス上または選択した特定のデバイス上で、ソフトウェアの脆弱性を無視できます。

実行手順の説明：

- 管理コンソール：検知されたソフトウェアの脆弱性への非対応の判断
- Kaspersky Security Center Web コンソール：検知されたソフトウェアの脆弱性への非対応の判断

6 脆弱性の修正タスクの実行

*アップデートのインストールと脆弱性の修正*タスクまたは*脆弱性の修正*タスクを開始します。タスクが完了したら、タスクリストでのタスクのステータスが［*正常終了*］になっていることを確認します。

7 ソフトウェアの脆弱性の修正結果のレポートの作成（省略可能）

脆弱性の修正に関する詳細な統計情報を確認するには、脆弱性レポートを生成します。レポートには、修正されなかったソフトウェアの脆弱性に関する情報が表示されます。これにより、組織内での Microsoft 製品やその他のサードパーティ製ソフトウェアの脆弱性の検知と修正の状況を把握することができます。

実行手順の説明：

- 管理コンソール：レポートの作成と表示
- Kaspersky Security Center Web コンソール：レポートの生成と表示

8 サードパーティ製ソフトウェアの脆弱性の検知と修正に関する設定の確認

次の手順がすべて完了していることを確認してください：

- 管理対象デバイス上のソフトウェアの脆弱性のリストを作成して内容を確認した
- 必要に応じて、修正対応しないソフトウェアの脆弱性を選定した
- 脆弱性を修正するタスクを設定した
- タスクの実行順序として、ソフトウェアの脆弱性を検知するタスクが実行された後に脆弱性を修正するタスクが実行されるようにスケジュールを指定した
- ソフトウェアの脆弱性を修正するタスクが実行されたことを確認した

結果

［*アップデートのインストールと脆弱性の修正*］タスクを作成した場合、管理対象デバイス上の脆弱性が自動的に修正されます。タスクの実行時に、適用可能なソフトウェアアップデートのリストとタスクの設定で指定されたルールとが照合されます。ルールの条件に一致するすべてのソフトウェアアップデートが管理サーバーのリポジトリにダウンロードされ、ソフトウェアの脆弱性を修正するためにインストールされます。

［*脆弱性の修正*］タスクを作成した場合、Microsoft 製品のソフトウェア脆弱性のみが修正されます。

ソフトウェアの脆弱性の検知と修正

Kaspersky Security Center では、Microsoft Windows オペレーティングシステムを実行している管理対象デバイスのソフトウェア脆弱性を検知して修正することができます。オペレーティングシステムとサードパーティ製ソフトウェア（Microsoft 製品を含む）の脆弱性が検知されます。

アップデート機能（ウイルス対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

ソフトウェア脆弱性の検知

ソフトウェア脆弱性の検知では、Kaspersky Security Center は既知の脆弱性のデータベースに記録されている情報を使用します。このデータベースは、カスペルスキーのスペシャリストによって作成されています。データベースには、脆弱性の説明、脆弱性の検知日、脆弱性の深刻度などの情報が含まれています。アプリケーションの脆弱性に関する詳細情報は、カスペルスキーの Web サイトにあります。

Kaspersky Security Center は*脆弱性とアプリケーションのアップデートの検索*タスクを使用してソフトウェア脆弱性を検知します。

場合によっては、Microsoft Windows オペレーティングシステムで検知された脆弱性は、次のいずれかの方法を使用して修正できます：

- OS のアップデートをインストールしています。
- OS を新しいバージョンにアップグレードする（たとえば、Windows 10 から Windows 11 へ）。

このシナリオでは、KSC は同じ脆弱性に対して 2 つのエントリを表示します。

ソフトウェア脆弱性の修正

ソフトウェア脆弱性の修正では、Kaspersky Security Center はソフトウェアの製造元から提供されているソフトウェアのアップデートを使用します。次のタスクを実行すると、ソフトウェアアップデートのメタデータが管理サーバーのリポジトリにダウンロードされます：

- *管理サーバーのリポジトリへのアップデートのダウンロード*：このタスクは、カスペルスキー製品とサードパーティ製ソフトウェアのアップデートのメタデータをダウンロードするためのタスクです。このタスクは、Kaspersky Security Center のクイックスタートウィザードによって自動的に作成されます。管理サーバーのリポジトリへのアップデートのダウンロードタスクを手動で作成することもできます。

- *Windows Update の同期の実行*：このタスクは、Microsoft 製品のアップデートのメタデータをダウンロードするためのタスクです。

脆弱性を修正するためのソフトウェアのアップデートは、配布パッケージまたはパッチの形式で提供されます。ソフトウェアの脆弱性を修正するソフトウェアのアップデートは、「*修正*」という名称で呼ばれます。*推奨される修正*は、カスペルスキーのスペシャリストがインストールを推奨する修正です。*ユーザー修正*は、インストールするようにユーザーが手動で指定する修正です。ユーザー修正をインストールするには、修正を含むインストールパッケージを事前に作成する必要があります。

脆弱性とパッチ管理機能を使用できる Kaspersky Security Center ライセンスを使用している場合、ソフトウェア脆弱性の修正に*アップデートのインストールと脆弱性の修正*タスクを使用できます。このタスクでは、推奨される修正をインストールして、検知された複数の脆弱性を自動的に修正します。このタスクを使用する場合、脆弱性を修正するためのルールを手動で指定できます。

脆弱性とパッチ管理機能を使用できる Kaspersky Security Center ライセンスを使用していない場合、ソフトウェア脆弱性の修正に*脆弱性の修正*タスクを使用できます。このタスクを使用すると、Microsoft 製品に対して推奨される修正とその他のサードパーティ製ソフトウェアに対するユーザー修正をインストールして脆弱性を修正できます。

セキュリティ上の理由から、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートすべてに対して、カスペルスキーの技術によるマルウェアのスキャンが自動的に実行されます。この技術は自動的なファイルのチェックに使用され、ウイルススキャン、Sandbox 環境における静的分析、動的分析、ふるまい分析、機械学習が含まれます。

カスペルスキーは、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートを手動で分析することはありません。さらに、カスペルスキーの専門家は脆弱性（既知または未知）や文書化されていないアップデートの機能について確認したり、上記で指定されているもの以外のアップデートの分析を行ったりすることはありません。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

一部のソフトウェアに関する脆弱性の修正では、ソフトウェアのインストールについて使用許諾契約書（EULA）への同意を要求された場合、EULA に同意する必要があります。使用許諾契約書に同意しない場合、脆弱性は修正されません。

ソフトウェアの脆弱性に関する情報の表示

クライアントデバイスで検知された脆弱性のリストを表示するには：

コンソールツリーの［**詳細**］フォルダーで、［**アプリケーションの管理**］フォルダーから［**ソフトウェアの脆弱性**］サブフォルダーを選択します。

管理対象デバイスで検知されたソフトウェア脆弱性のリストが表示されます。

選択した脆弱性に関する情報を取得するには：

脆弱性のコンテキストメニューから［**プロパティ**］を選択します。

脆弱性のプロパティウィンドウに次の情報が表示されます：

- 脆弱性が検知されたアプリケーション
- 脆弱性が検知されたデバイスのリスト
- 脆弱性が修正されたどうかに関する情報

検知されたすべての脆弱性に関するレポートを表示するには：

［**ソフトウェアの脆弱性**］フォルダーの作業領域で［**脆弱性レポートの表示**］をクリックします。

デバイスにインストールされたソフトウェアの脆弱性に関するレポートが生成されます。このレポートは、該当する管理サーバーの名前のフォルダーで［**レポート**］タブを開くことで表示できます。

管理対象デバイス上の脆弱性に関する統計情報の表示

管理対象デバイス上でのそれぞれのソフトウェア脆弱性に関する統計情報を表示できます。統計情報は図表として表示されます。図表には、次のステータスごとに該当するデバイス数が表示されます：

- *無視：<デバイス数>*：脆弱性のプロパティでその脆弱性を無視するように手動で設定した場合に、このステータスが割り当てられます。
- *修正済み：<デバイス数>*：脆弱性を修正するためのタスクが正常に完了した場合に、このステータスが割り当てられます。
- *修正をスケジュール済み：<デバイス数>*：脆弱性を修正するためのタスクを作成済みだが、タスクがまだ実行されていない場合に、このステータスが割り当てられます。
- *パッチが適用済み：<デバイス数>*：脆弱性の修正をするためのソフトウェアのアップデートを手動で選択したが、そのソフトウェアのアップデートでは脆弱性が修正されていない場合に、このステータスが割り当てられます。
- *修正が必要：<デバイス数>*：脆弱性が一部の管理対象デバイスでのみ修正されており、さらに多くの管理対象デバイスで脆弱性を修正する必要がある場合に、このステータスが割り当てられます。

管理対象デバイス上の脆弱性に関する統計情報を表示するには：

1. コンソールツリーの［**詳細**］フォルダーで、［**アプリケーションの管理**］フォルダーから［**ソフトウェアの脆弱性**］サブフォルダーを選択します。

   管理対象デバイスで検知されたソフトウェア脆弱性のリストが表示されます。

2. 統計情報を表示する脆弱性を選択します。

   選択したオブジェクトに対する操作を実行できるボックス内に、脆弱性のステータスの図表が表示されます。それぞれのステータスをクリックすると、選択したステータスの脆弱性が存在するデバイスのリストが表示されます。

アプリケーションの脆弱性スキャン

クイックスタートウィザードを使用してアプリケーションを構成した場合は、*脆弱性スキャン*タスクが自動的に作成されます。［**管理対象デバイス**］フォルダーの［**タスク**］タブでこのタスクを確認できます。

クライアントデバイスにインストールされたソフトウェアの脆弱性をスキャンするタスクを作成するには：

1. コンソールツリーで、［**詳細**］→［**アプリケーションの管理**］フォルダー→［**ソフトウェアの脆弱性**］サブフォルダーの順に選択します。

2. 作業領域で［**その他の操作**］→［**脆弱性スキャンの設定**］の順に選択します。

   脆弱性スキャンタスクが既に存在する場合、該当する既存タスクが選択された状態で［**管理対象デバイス**］フォルダーの［**タスク**］タブが表示されます。既存のタスクがない場合、脆弱性とアプリケーションのアップデートの検索タスク作成ウィザードが起動します。ウィザードの指示に従ってください。

3. ［**タスク種別の選択**］ウィンドウで、［**脆弱性とアプリケーションのアップデートの検索**］を選択します。

4. ウィザードの［**設定**］ページで、タスクを次のように設定します：

   - **Microsoft による脆弱性とアップデートのリストを検索する**

     脆弱性とアップデートの検索時に、Kaspersky Security Center は、現時点で適用可能な Microsoft Update のアップデート元からの該当する Microsoft Update の情報を使用します。

     Microsoft Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

     既定では、このオプションはオンです。

   - **アップデートサーバーに接続してアップデートを取得**

管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元として指定した場所に接続します。以下のサーバーを Microsoft Update のアップデート元として動作させることができます：

- Kaspersky Security Center 管理サーバー（詳細は、「ネットワークエージェントのポリシーの設定」を参照してください）
- 組織ネットワーク内で Microsoft Windows Server Update Services（WSUS）として機能している Windows Server
- Microsoft Update サーバー

このオプションをオンにすると、管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元に接続して、該当する Microsoft Windows Update の情報を最新にします。

このオプションをオフにすると、管理対象デバイス上の Windows Update エージェントは Microsoft アップデートプログラムのソースから以前に受信した、該当する Microsoft Windows アップデートプログラムに関する情報を使用します。

Microsoft Update のアップデート元への接続は、多くのリソースを消費します。別のタスクまたはセクション［**ソフトウェアのアップデートと脆弱性**］のネットワークエージェントのポリシーのプロパティで、アップデート元へ定期的に接続するように設定している場合は、このオプションをオフにすることを検討してください。このオプションをオフにしない場合は、サーバーの負荷を下げるために、タスクの開始を 360 分以内でランダムに遅延させるようにタスクのスケジュールを設定できます。

既定では、このオプションはオンです。

ネットワークエージェントのポリシーの設定の各オプションの組み合わせに応じて、以下のようにアップデートの取得方法が異なります：

- 管理対象デバイス上の Windows Update エージェントがアップデートサーバーに接続してアップデートを取得するのは、［*脆弱性とアプリケーションのアップデートの検索*］タスクのプロパティでアップデートサーバーに［**アップデートサーバーに接続してアップデートを取得**］が有効になっており、ネットワークエージェントポリシーの設定で［**Windows Update 検索モード**］が［**アクティブ**］に設定されている場合のみです。
- *脆弱性スキャン*タスクを実行する時に、ネットワークエージェントが Microsoft Windows アップデート元への接続を開始して更新をダウンロードする必要がない場合は、［**Windows Update 検索モード**］を［**パッシブ**］に設定できますが、［**アップデートサーバーに接続してアップデートを取得**］は有効のままにする必要があります。これにより、リソースを節約し、以前に受信した Windows アップデートプログラムを使用して脆弱性をスキャンできるようになります。Microsoft Windows アップデートプログラムの受信を別の方法で構成する場合は、パッシブモードを使用できます。Microsoft Windows アップデートプログラムの受信が別の方法で構成されていない場合は、**Windows Update 検索モード**オプションを[**パッシブ**]に設定しないでください。この場合、アップデートプログラムに関する情報は受信されません。
- ［**アップデートサーバーに接続してアップデートを取得**］の状態（オンまたはオフ）に関係なく、［**Windows Update 検索モード**］が［**無効**］に設定されている場合、Kaspersky Security Center はアップデートプログラムに関する情報を要求しません。

- **カスペルスキーによるサードパーティ製品の脆弱性とアップデートのリストを検索する**

このオプションをオンにすると、Kaspersky Security Center は Windows のレジストリおよび［**ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**］で指定したフォルダーに存在するサードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）の脆弱性とアップデートを検索します。サポート対象のサードパーティ製品の全リストはカスペルスキーが管理しています。

このオプションをオフにすると、サードパーティ製品の脆弱性とアップデートの検索は行われません。Microsoft Windows Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

既定では、このオプションはオンです。

- **ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**

Kaspersky Security Center が脆弱性の修正とアップデートのインストールが必要なアプリケーションを検索する時に対象とするフォルダーです。システム変数を使用できます。

アプリケーションがインストールされているフォルダーを指定します。既定では、ほとんどのアプリケーションのインストール先となっているシステムフォルダーがリストに含まれます。

- **詳細な診断を有効にする**

このオプションをオンにすると、Kaspersky Security Center リモート診断ユーティリティでネットワークエージェントによるトレースがオフになっていても、ネットワークエージェントがトレースを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center リモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

既定では、このオプションはオフです。

- **詳細な診断ファイルの最大サイズ（MB）**

既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

5. ウィザードの［**タスクスケジュールの設定**］ページで、タスク開始のスケジュールを作成できます。必要に応じて、次の設定を指定します：

- **実行予定：**

タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

  - **N 時間ごと**

指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

- **N 日ごと**

  日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

  既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

- **N 週間ごと**

  指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

  既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

- **N 分ごと**

  タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

  既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

- **毎日（サマータイムはサポートしていません）**

  日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を 1 時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

  このスケジュールの使用は推奨されません。Kaspersky Security Center の旧バージョンとの後方互換性を維持するために用意されているオプションとなります。

  既定では、毎日、現在のシステム時刻にタスクが実行されます。

- **毎週**

  毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。

  指定した日付が存在しない月には、月の最終日にタスクを実行します。

  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。
  規定では、日付は選択されていません。規定の開始時間は 18:00 です。

- **新しいアップデートがリポジトリにダウンロードされ次第**

  アップデートのリポジトリへのダウンロードが完了すると、タスクが実行されます。たとえば、脆弱性とアプリケーションのアップデートの検索タスクのスケジュールを設定する時に、このオプションを使用すると便利です。

- **ウイルスアウトブレイク検知次第**

  ［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

  - ワークステーションとファイルサーバー向けアンチウイルス製品
  - 境界防御向けアンチウイルス製品
  - メールサーバー向けアンチウイルス製品

  既定では、すべてのアプリケーション種別がオンです。
  ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

  他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

  テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

  必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

  - タスク名で検索するには、検索フィールドにタスク名を入力します。
  - 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。
    既定では、タスクはアルファベットの昇順で並べ替えられます。
  - フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる(分)**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  既定では、このオプションはオフです。既定の時間は1分です。

6. ウィザードの［**タスク名の定義**］ウィンドウで、作成中のタスク名を指定します。タスク名は100文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

7. ［**タスク作成の終了**］ウィンドウで、［**終了**］をクリックしてウィザードを終了します。

   ウィザード終了後にすぐにタスクを開始するには、［**ウィザードの終了後にタスクを実行**］をオンにします。

このウィザードが完了すると、**脆弱性と必要なアップデートを検索**タスクが、［**管理対象デバイス**］フォルダーの［**タスク**］タブに表示されます。

タスクの作成時に指定した設定およびタスクのその他のプロパティは、いつでも変更できます。

*脆弱性と必要なアップデートを検索*タスクが完了すると、管理サーバーに、デバイスにインストールされているアプリケーションで検知された脆弱性のリストと、検知された脆弱性を修正するために必要なソフトウェアのすべてのアップデートも表示されます。

0x80240033「Windows Update エージェントエラー 80240033（「ライセンス条項がダウンロードできませんでした。」）」が表示された場合は、Windows レジストリを使用してこの問題を解決できます。

［*高速インストールファイルをダウンロード*］をオフにした **Windows Update の同期の実行**タスクと*脆弱性と必要なアップデートを検索*タスクをこの順序で連続して実行した場合、管理サーバーでは必要なソフトウェアのアップデートのリストが表示されません。必要なソフトウェアのアップデートのリストを表示するには、*脆弱性と必要なアップデートを検索*タスクを再実行する必要があります。

ネットワークエージェントは、適用可能な Windows アップデートおよび Microsoft 製品のアップデートに関する情報を、Windows Update から、または管理サーバーが WSUS サーバーとして動作する場合は管理サーバーから受信します。情報は、アプリケーションの起動時（ポリシーで規定されている場合）、およびクライアントデバイス上で*脆弱性と必要なアップデートを検索*タスクが定期的に実行されるたびに送信されます。

Kaspersky Security Center を使用してアップデートできるサードパーティ製ソフトウェアの詳細情報は、テクニカルサポートサイトの Kaspersky Security Center ページにある「**サーバー管理**」セクションで確認できます。

アプリケーションの脆弱性の修正

クイックスタートウィザードの［**アップデート管理設定**］ページで［**必要なアップデートの検索とインストール**］を選択した場合、*アップデートのインストールと脆弱性の修正*タスクが自動的に作成されます。このタスクは、［**管理対象デバイス**］フォルダーの［**タスク**］タブの作業領域に表示されます。

それ以外の場合、次の操作を実行できます：

- 適用可能なアップデートのインストールによる脆弱性の修正タスクを作成する。
- 脆弱性の修正の既存タスクに脆弱性の修正のルールを追加する。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

脆弱性の修正タスクの作成による脆弱性の修正

次の操作を実行できます：

- 一定のルールに合致する複数の脆弱性を修正するタスクを作成する。
- 脆弱性を選択し、同一および類似の脆弱性の修正タスクを作成する。

一定のルールに合致する脆弱性を修正するタスクを作成するには：

1. コンソールツリーで、脆弱性を修正するデバイスの管理サーバーを選択します。
2. メインウィンドウの［**表示**］メニューで、［**インターフェイスの設定**］を選択します。
3. 開いたウィンドウで、［**脆弱性とパッチ管理の表示**］をオンにし、［OK］をクリックします。

4. アプリケーションメッセージが表示されたウィンドウで、［**OK**］をクリックします。

5. 管理コンソールを再起動して、変更を有効にします。

6. コンソールツリーで、［**管理対象デバイス**］フォルダーを選択します。

7. 作業領域で、［**タスク**］タブを選択します。

8. ［**タスクの作成**］をクリックして、［新規タスクウィザード］を実行します。ウィザードの指示に従ってください。

9. ウィザードの［**タスク種別の選択**］ウィンドウで、［**アップデートのインストールと脆弱性の修正**］を選択します。

   タスクが表示されない場合は、［**システム管理**：**脆弱性とパッチ管理**］機能領域の**読み取り**、**変更**、および**実行**権限がアカウントに付与されていることを確認してください。これらのアクセス権がない場合、*アップデートのインストールと脆弱性の修正*タスクを作成および設定することはできません。

10. ウィザードの［**設定**］ページで、タスクを次のように設定します：

- **アップデートのインストールのルールを指定します**

  これらのルールはクライアントデバイスでのアップデートのインストールに適用されます。ルールが指定されていない場合、タスクはなにも実行しません。ルールの使用法については、「アップデートインストールのルール」を参照してください。

- **デバイスの再起動時またはシャットダウン時にインストールを開始する**

  このオプションをオンにすると、デバイスの再起動時またはシャットダウン時にアップデートがインストールされます。オプションがオフの場合、アップデートのインストールはスケジュールに従って実行されます。

  アップデートのインストールによりデバイスのパフォーマンスに影響を与える可能性がある場合は、このオプションを使用します。

  既定では、このオプションはオフです。

- **必要なシステムコンポーネントをインストールする**

  このオプションをオンにすると、アップデートのインストール前にインストールが必要な一般システムコンポーネントをすべて自動的にインストールします。インストールが必要な対象とは、たとえばオペレーティングシステムのアップデートなどです。

  このオプションをオフにすると、必須コンポーネントを手動でインストールすることが必要となる場合があります。

  既定では、このオプションはオフです。

- **アップデート中に新しい製品のバージョンのインストールを許可する**

このオプションをオンにすると、製品の新しいバージョンをインストールするアップデートを許可できます。

このオプションをオフにすると、製品はアップグレードされません。製品の新しいバージョンは手動でインストールするか、別のタスクを通してインストールできます。この設定は、所属企業のインフラストラクチャでソフトウェアの新しいバージョンがサポートされていなかったり、アップグレードをテスト環境で確認したい場合に使用します。

既定では、このオプションはオンです。

製品をアップデートすることにより、クライアントデバイスにインストールされた対象製品に依存するアプリケーションが正しく動作しなくなることがあります。

- **デバイスにアップデートをダウンロードするがインストールしない**

このオプションをオンにすると、アップデートをデバイスにダウンロードしますが、自動ではインストールしません。ダウンロードされたアップデートを手動でインストールできます。

Microsoft 製品のアップデートは、システム Windows フォルダーにダウンロードされます。サードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートは、［**アップデートのダウンロード先**］で指定したフォルダーにダウンロードされます。

このオプションをオフにすると、アップデートはデバイスに自動的にインストールされません。

既定では、このオプションはオフです。

  - **アップデートのダウンロード先**

このフォルダーはサードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートのダウンロードに使用されます。

- **詳細な診断を有効にする**

このオプションをオンにすると、Kaspersky Security Center リモート診断ユーティリティでネットワークエージェントによるトレースがオフになっていても、ネットワークエージェントがトレースを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center リモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

既定では、このオプションはオフです。

  - **詳細な診断ファイルの最大サイズ（MB）**

既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

11. ウィザードの［**オペレーティングシステムの再起動のオプションを選択**］ウィンドウで、タスク完了後にクライアントデバイスのオペレーティングシステムの再起動が必要になった場合の処理を選択します。

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

  - **通知の繰り返し間隔（分）**

    このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

    既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

    このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

  - **再起動するまでの時間（分）**

    ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

    既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

既定では、このオプションはオフです。

12. ウィザードの［**タスクスケジュールの設定**］ページで、タスク開始のスケジュールを作成できます。必要に応じて、次の設定を指定します：

- **実行予定：**

  タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

  - **N 時間ごと**

    指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

    既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

  - **N 日ごと**

    日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

    既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

  - **N 週間ごと**

    指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

    既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

  - **N 分ごと**

    タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

    既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

  - **毎日（サマータイムはサポートしていません）**

日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を1時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

このスケジュールの使用は推奨されません。Kaspersky Security Center の旧バージョンとの後方互換性を維持するために用意されているオプションとなります。

既定では、毎日、現在のシステム時刻にタスクが実行されます。

- **毎週**

  毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。

  指定した日付が存在しない月には、月の最終日にタスクを実行します。

  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。

  規定では、日付は選択されていません。規定の開始時間は18:00 です。

- **ウイルスアウトブレイク検知次第**

  ［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

  - ワークステーションとファイルサーバー向けアンチウイルス製品
  - 境界防御向けアンチウイルス製品
  - メールサーバー向けアンチウイルス製品

  既定では、すべてのアプリケーション種別がオンです。

  ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

  他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

  テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

  必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

  - タスク名で検索するには、検索フィールドにタスク名を入力します。
  - 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。

    既定では、タスクはアルファベットの昇順で並べ替えられます。
  - フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

  このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

  このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

  このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

  既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる(分)**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

既定では、このオプションはオフです。既定の時間は1分です。

13. ウィザードの［**タスク名の定義**］ウィンドウで、作成中のタスク名を指定します。タスク名は100文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

14. ［**タスク作成の終了**］ウィンドウで、［**終了**］をクリックしてウィザードを終了します。

    ウィザード終了後にすぐにタスクを開始するには、［**ウィザードの終了後にタスクを実行**］をオンにします。

ウィザードが完了すると、［**アップデートのインストールと脆弱性の修正**］タスクが作成され、［**タスク**］フォルダーに表示されます。

タスクの作成時に指定した設定およびタスクのその他のプロパティは、いつでも変更できます。

タスクの結果に0x80240033「Windows Update Agent error 80240033（「License terms could not be downloaded.」）」エラーが含まれている場合、Windowsレジストリを使用してこの問題を解決できます。

特定の脆弱性および類似の脆弱性を修正するには：

1. コンソールツリーの［**詳細**］フォルダーで、［**アプリケーションの管理**］フォルダーから［**ソフトウェアの脆弱性**］サブフォルダーを選択します。

2. 修正する脆弱性を選択します：

3. ［**脆弱性修正ウィザードを実行**］をクリックします。

   脆弱性修正ウィザードが起動します。

   脆弱性修正ウィザードは、脆弱性とパッチ管理が使用可能なライセンスがある場合のみ使用できます。

   ウィザードの指示に従ってください。

4. ［**脆弱性を修正するタスクがあるかどうか検索する**］ウィンドウで、次のパラメータを指定します：

   - **この脆弱性を修正するタスクのみ表示**

     このオプションをオンにすると、脆弱性修正ウィザードで、選択した脆弱性を修正する既存のタスクが検索されます。

     このオプションがオフまたは該当するタスクが見つからなかった場合、脆弱性修正ウィザードで、脆弱性修正のルールまたはタスクを作成するように要求されます。

     既定では、このオプションはオンです。

   - **この脆弱性を修正するアップデートを承認する**

選択した脆弱性を修正するアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

既定では、このオプションはオフです。

5. ［脆弱性を修正するタスクがあるかどうか検索する］をオンにして、該当するタスクが見つかった場合、これらのタスクのプロパティを表示したり手動で開始することができます。追加の操作は必要ありません。

   追加の操作を実行する場合、［**脆弱性の修正タスクを新規作成**］をクリックします。

6. 新しいタスクに追加する脆弱性修正ルールの種別を選択し、［**終了**］をクリックします。

7. アプリケーションの以前のアップデートをインストールするかを確認するダイアログで、いずれかを選択します。選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、［**はい**］をクリックします。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、［**いいえ**］をクリックします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

   アップデートのインストールと脆弱性修正タスク作成ウィザードが起動します。ウィザードの指示に従ってください。

8. ウィザードの［**オペレーティングシステムの再起動のオプションを選択**］ウィンドウで、タスク完了後にクライアントデバイスのオペレーティングシステムの再起動が必要になった場合の処理を選択します。

   - **デバイスを再起動しない**

     操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

   - **デバイスを再起動する**

     インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

   - **ユーザーに処理を確認する**

     手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

     既定では、このオプションがオンです。

     - **通知の繰り返し間隔（分）**

このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

- **再起動するまでの時間（分）**

  ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

  既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

9. ウィザードの［**タスクを割り当てるデバイスの選択**］ページで、次のいずれかのオプションをオンにします：

- **ネットワークの管理サーバーによって検出されたデバイスを選択する**

  タスクを特定のデバイスに割り当てます。特定のデバイスには、管理グループに属するデバイスと管理グループが割り当てられていないデバイスの両方を含めることができます。

  たとえば、未割り当てデバイスでネットワークエージェントのインストールタスクを実行する時に、このオプションを使用すると便利です。

- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

  タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

  特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

- **デバイスの抽出にタスクを割り当てる**

デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

- **管理グループにタスクを割り当てる**

  任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

  たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

  タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

10. ウィザードの［**タスクスケジュールの設定**］ページで、タスク開始のスケジュールを作成できます。必要に応じて、次の設定を指定します：

- **実行予定：**

  タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

  - **N 時間ごと**

    指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

    既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

  - **N 日ごと**

    日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

    既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

  - **N 週間ごと**

    指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

    既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

  - **N 分ごと**

    タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

    既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

  - **毎日（サマータイムはサポートしていません）**

日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を1時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

このスケジュールの使用は推奨されません。Kaspersky Security Center の旧バージョンとの後方互換性を維持するために用意されているオプションとなります。

既定では、毎日、現在のシステム時刻にタスクが実行されます。

- **毎週**

  毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。

  指定した日付が存在しない月には、月の最終日にタスクを実行します。

  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。

  規定では、日付は選択されていません。規定の開始時間は18:00 です。

- **ウイルスアウトブレイク検知次第**

  ［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

  - ワークステーションとファイルサーバー向けアンチウイルス製品
  - 境界防御向けアンチウイルス製品
  - メールサーバー向けアンチウイルス製品

  既定では、すべてのアプリケーション種別がオンです。

  ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

  他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

  テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

  必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

  - タスク名で検索するには、検索フィールドにタスク名を入力します。
  - 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。

    既定では、タスクはアルファベットの昇順で並べ替えられます。
  - フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

  このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

  このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

  このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

  既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる(分)**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

既定では、このオプションはオフです。既定の時間は1分です。

11. ウィザードの［**タスク名の定義**］ウィンドウで、作成中のタスク名を指定します。タスク名は100文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

12. ［**タスク作成の終了**］ウィンドウで、［**終了**］をクリックしてウィザードを終了します。

    ウィザード終了後にすぐにタスクを開始するには、［**ウィザードの終了後にタスクを実行**］をオンにします。

ウィザードが完了すると、［**アップデートのインストールと脆弱性の修正**］タスクが作成され、［**タスク**］フォルダーに表示されます。

タスクの作成時に指定した設定およびタスクのその他のプロパティは、いつでも変更できます。

脆弱性の修正の既存タスクへのルールの追加による脆弱性の修正

脆弱性の修正の既存タスクにルールを追加して脆弱性を修正するには：

1. コンソールツリーの［**詳細**］フォルダーで、［**アプリケーションの管理**］フォルダーから［**ソフトウェアの脆弱性**］サブフォルダーを選択します。

2. 修正する脆弱性を選択します：

3. ［**脆弱性修正ウィザードを実行**］をクリックします。

   脆弱性修正ウィザードが起動します。

   脆弱性修正ウィザードは、脆弱性とパッチ管理が使用可能なライセンスがある場合のみ使用できます。

   ウィザードの指示に従ってください。

4. ［**脆弱性を修正するタスクがあるかどうか検索する**］ウィンドウで、次のパラメータを指定します：

   - **この脆弱性を修正するタスクのみ表示**

     このオプションをオンにすると、脆弱性修正ウィザードで、選択した脆弱性を修正する既存のタスクが検索されます。

     このオプションがオフまたは該当するタスクが見つからなかった場合、脆弱性修正ウィザードで、脆弱性修正のルールまたはタスクを作成するように要求されます。

     既定では、このオプションはオンです。

   - **この脆弱性を修正するアップデートを承認する**

選択した脆弱性を修正するアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

既定では、このオプションはオフです。

5. ［脆弱性を修正するタスクがあるかどうか検索する］をオンにして、該当するタスクが見つかった場合、これらのタスクのプロパティを表示したり手動で開始することができます。追加の操作は必要ありません。

   追加の操作を実行する場合、［**既存のタスクに脆弱性の修正ルールを追加する**］をクリックします。

6. ルールを追加するタスクを選択し、［**ルールの追加**］をクリックします。

   既存のタスクのプロパティを表示したり、タスクを手動で作成したり、新規タスクを作成することもできます。

7. 選択したタスクに追加するルールの種別を選択し、［**終了**］をクリックします。

8. アプリケーションの以前のアップデートをインストールするかを確認するダイアログで、いずれかを選択します。選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、［**はい**］をクリックします。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、［**いいえ**］をクリックします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

既存の**アップデートのインストールと脆弱性の修正**タスクに新しい脆弱性の修正ルールが追加されます。

隔離されたネットワークでの脆弱性の修正

このセクションでは、インターネット接続のない管理サーバーに接続されている管理対象デバイスのサードパーティ製ソフトウェアの脆弱性を修正するために実行できる手順について説明します。

シナリオ：分離されたネットワークでのサードパーティ製ソフトウェアの脆弱性の修正

分離されたネットワーク内の管理対象デバイスにインストールされているサードパーティ製ソフトウェアのアップデートをインストールして脆弱性を修正できます。このネットワークには管理サーバーと、そこに接続されているインターネット接続のない管理対象デバイスが含まれます。このようなネットワークの脆弱性を修正するには、インターネットに接続された管理サーバーが必要です。次に、インターネットにアクセス可能な管理サーバーを使用してパッチ（必要なアップデート）をダウンロードし、分離された管理サーバーにパッチを送信できるようになります。

Kaspersky Security Center を使用して、分離された管理サーバー上で製造元が発行したサードパーティ製品のアップデートはダウンロードすることができますが、Microsoft 製品のアップデートはダウンロードすることはできません。

分離されたネットワーク上での脆弱性の修正プロセスがどのように動作するかについては、このプロセスの説明とスキームを参照してください。

必須条件

開始する前に、次を実行します：

1. インターネットに接続してパッチをダウンロードするためのデバイスを1つ割り当てます。このデバイスは、インターネットにアクセス可能な管理サーバーとしてカウントされます。

2. 次の端末にバージョン14以降のKaspersky Security Centerをインストールします：

   - インターネットに接続されている管理サーバーとして動作する割り当て済みデバイス

   - インターネットから分離された管理サーバーとして動作する分離されたデバイス（以降「分離された管理サーバー」と表記）

3. すべての管理サーバーに、アップデートとパッチをダウンロードして保存できる十分なディスク容量があることを確認してください。

実行するステップ

分離された管理サーバーの管理対象デバイスへのアップデートのインストールとサードパーティ製ソフトウェアの脆弱性の修正には、次の段階があります。

1 インターネットにアクセス可能な管理サーバーの設定

必要なサードパーティ製ソフトウェアアップデートのリクエストを処理し、パッチをダウンロードするためにインターネットにアクセス可能な管理サーバーを準備します。

2 分離された管理サーバーの設定

分離された管理サーバーを準備します。分離された管理サーバーは定期的に必要な更新のリストを作成して、インターネットにアクセス可能な管理サーバーによってダウンロードされたパッチを処理できます。設定後、分離された管理サーバーはインターネットからパッチをダウンロードしようとすることはありません。その代わり、パッチ経由でアップデートを取得します。

3 分離された管理サーバーへのパッチの送信とアップデートのインストール

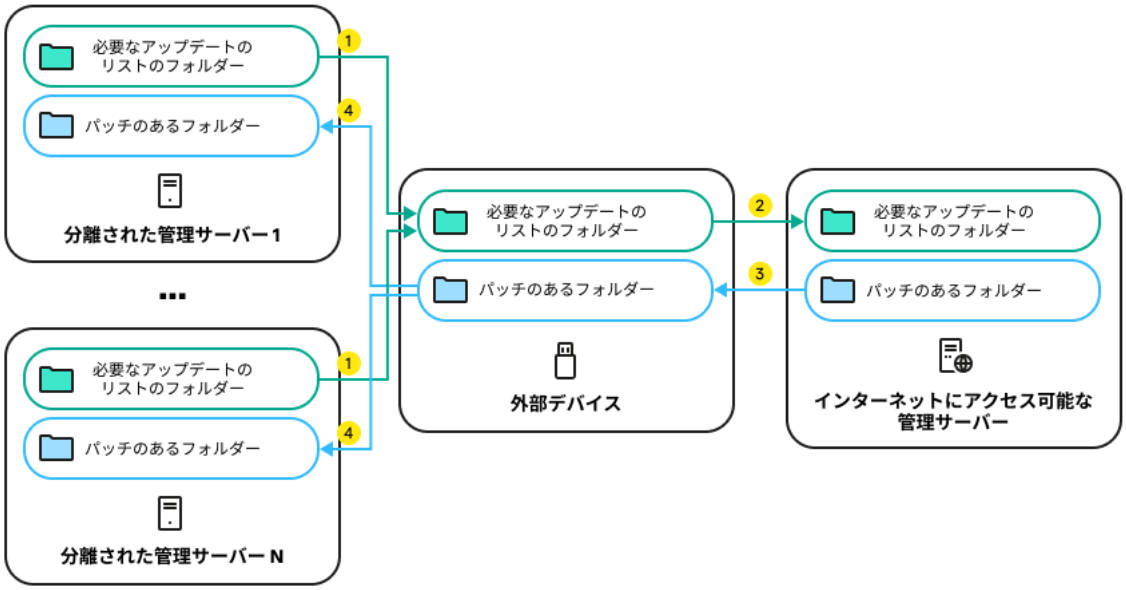
管理サーバーの設定が完了すると、インターネットにアクセス可能な管理サーバーと分離された管理サーバーの間で必要なアップデートリストとパッチを送信することができるようになります。次に、パッチからのアップデートと修正が、*アップデートのインストールと脆弱性の修正*タスクを使用して管理対象デバイスにインストールされます。

結果

サードパーティ製ソフトウェアのアップデートは、分離された管理サーバーに送信され、Kaspersky Security Centerを使用して接続された管理対象デバイスにインストールされます。管理サーバーを1回構成するだけで、その後は必要に応じて、たとえば1日に1回または数回更新アップデートを取得できます。

分離されたネットワークでのサードパーティ製ソフトウェアの脆弱性の修正について

隔離されたネットワークでのサードパーティ製品の脆弱性の修正プロセスについては図に示したとおりで、以下に説明します。このプロセスは定期的に繰り返すことができます。



インターネットにアクセス可能な管理サーバーと分離された管理サーバー間でのパッチと必要なアップデートのリストを送信するプロセス

インターネットから分離されたすべての管理サーバーは（以降、「分離された管理サーバー」と表記）、この管理サーバーに接続された管理対象デバイス上にインストールする必要のあるアップデートのリストを生成します。必要なアップデートのリストは特定のフォルダーに保管され、バイナリファイルの形式で表示されます。各ファイルには必要なアップデートを持つパッチの ID が含まれる名前が付いています。その結果、リスト内のすべてのファイルが特定のパッチを指します。

外付けドライブを使用して、分離された管理サーバーからの必要なアップデートのリストを、インターネットにアクセス可能な割り当て済みの管理サーバーに転送することができます。その後、割り当てられた管理サーバーはインターネットからパッチをダウンロードし、別のフォルダーに保存します。

すべてのパッチが特別なフォルダーに保存されたら、必要なアップデートのリストを取得した、分離された管理サーバーにパッチを移動します。隔離された管理サーバー上でパッチ用に作成されたフォルダーにパッチを保存します。結果、*アップデートのインストールと脆弱性の修正*タスクが分離された管理サーバーの管理対象デバイスにパッチを実行し、アップデートをインストールします。

分離されたネットワークで脆弱性を修正するためのインターネットにアクセス可能な管理サーバーの構成

分離されたネットワークで脆弱性の修正およびパッチの送信を準備するには、最初にインターネットにアクセス可能な管理サーバーを設定し、次に分離された管理サーバーを設定します。

インターネットにアクセス可能な管理サーバーを設定するには：

1. 管理サーバーがインストールされているディスクに 2 つのフォルダーを作成します：
   - 必要なアップデートのリストのフォルダー
   - パッチのフォルダー

   これらのフォルダーには好きな名前を付けることができます。
2. オペレーティングシステムの標準の管理ツールを使用して、作成したフォルダーで KLAdmins グループに変更権限を付与します。
3. klscflag ユーティリティを使用して、管理サーバーのプロパティにフォルダーのパスを書き込みます。

Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

4. Windows コマンドプロンプトで次のコマンドを入力します：

   - パッチのフォルダーのパスを設定するには：
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<フォルダーのパス>"`
   - 必要なアップデートのリストのフォルダーのパスを設定するには：
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<フォルダーのパス>"`

   例：`klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\FolderForPatches"`

5. 必要であれば、klscflag ユーティリティを使用して、管理サーバーが新しいパッチリクエストをチェックする頻度を指定します：
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <頻度の値（秒）>`
   既定値は 120 秒です。
   例：`klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

6. 管理対象デバイスにインストールされているサードパーティ製ソフトウェアのパッチに関する情報を取得するには、*脆弱性とアプリケーションのアップデートの検索*タスクを作成し、タスクスケジュールを設定します。

7. *脆弱性の修正*タスクを作成し、脆弱性を修正するために使用されるサードパーティ製ソフトウェアのパッチを指定して、タスクスケジュールを設定します。
   スケジュールで指定されているよりも早く実行したい場合は、手動でタスクを実行します。タスクを開始する順序は重要です。*脆弱性の修正*タスクは、*脆弱性とアプリケーションのアップデートの検索*タスクを完了した後に実行する必要があります。

8. 管理サーバーサービスを再起動します。

これで、インターネットにアクセス可能な管理サーバーで、アップデートをダウンロードして分離された管理サーバーに送信する準備が整いました。脆弱性の修正を開始する前に、分離された管理サーバーを設定してください。

分離されたネットワークの脆弱性を修正するための分離された管理サーバーの設定

インターネットにアクセス可能な管理サーバーの設定が完了してから、ネットワーク内の分離されたすべての管理サーバーを準備してください。分離された管理サーバーに接続された管理対象デバイスの脆弱性を修正し、アップデートをインストールすることができます。

分離された管理サーバーを設定するには、すべての管理サーバーで次の操作を実行してください：

1. 脆弱性とパッチ管理（VAPM）機能のライセンスをアクティベートします。

2. 管理サーバーがインストールされているディスクに 2 つのフォルダーを作成します：

   - 必要なアップデートのリストが存在するフォルダー
   - パッチのフォルダー

   これらのフォルダーには好きな名前を付けることができます。

3. オペレーティングシステムの標準の管理ツールを使用して、作成したフォルダーで KLAdmins グループに*変更*権限を付与します。

4. klscflag ユーティリティを使用して、管理サーバーのプロパティにフォルダーのパスを書き込みます。

   Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

5. Windows コマンドプロンプトで次のコマンドを入力します：

   - パッチのフォルダーのパスを設定するには：
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<フォルダーのパス>"`
   - 必要なアップデートのリストのフォルダーのパスを設定するには：
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<フォルダーのパス>"`

   例：`klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\FolderForPatches"`

6. 必要であれば、klscflag ユーティリティを使用して、分離された管理サーバーが新しいパッチをチェックする頻度を指定します：
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <頻度の値（秒）>`

   既定値は 120 秒です。

   Example: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`

7. 必要であれば、klscflag ユーティリティを使用して、パッチの SHA256 ハッシュを計算します：
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   このコマンドを入力すると、分離された管理サーバーに転送されてからパッチが変更されていないことと、必要なアップデートを含む正しいパッチを受け取ったことを確認できます。

   既定では、Kaspersky Security Center はパッチの SHA256 ハッシュを計算しません。このオプションを有効にすると、分離された管理サーバーがパッチを受信した後、Kaspersky Security Center はそれらのハッシュを計算し、取得した値を管理サーバーデータベースに保存されているハッシュと比較します。計算されたハッシュがデータベース内のハッシュと一致しない場合はエラーが発生し、間違ったパッチを置き換える必要があります。

8. 管理対象デバイスにインストールされているサードパーティ製ソフトウェアのパッチに関する情報を取得するには、「*脆弱性とアプリケーションのアップデートの検索*」タスクを作成し、タスクスケジュールを設定します。

9. *脆弱性の修正*タスクを作成し、脆弱性を修正するために使用されるサードパーティ製ソフトウェアのパッチを指定して、タスクスケジュールを設定します。

   スケジュールで指定されているよりも早く実行したい場合は、手動でタスクを実行します。タスクを開始する順序は重要です。*脆弱性の修正*タスクは、*脆弱性とアプリケーションのアップデートの検索*タスクを完了した後に実行する必要があります。

10. 管理サーバーサービスを再起動します。

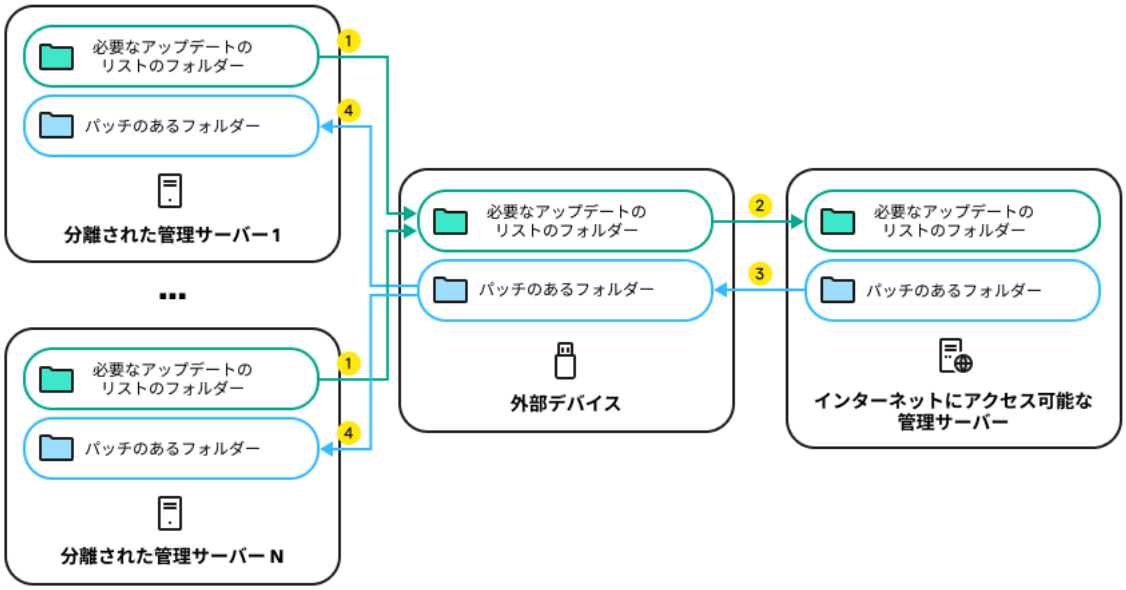
すべての管理サーバーを設定すると、パッチと必要な更新のリストを移動し、分離されたネットワーク内の管理対象デバイスのサードパーティ製ソフトウェアの脆弱性を修正できるようになります。

分離されたネットワークでのパッチの送信とアップデートのインストール

管理サーバーの設定を完了してから、インターネットにアクセス可能な管理サーバーから分離された管理サーバーにアップデートを含むパッチを転送できます。アップデートは、たとえば、1日に1回または数回など、必要に応じて何度でも送信およびインストールできます。

管理サーバー間でパッチと必要なアップデートのリストを転送するには、リムーバブルドライブなどの外付けドライブが必要です。したがって、外付けドライブにパッチをダウンロードして保存する十分なディスク容量があることを確認してください。

パッチを送信するプロセスと必要なアップデートのリストは図のとおりで、以下に説明します。



インターネットにアクセス可能な管理サーバーと分離された管理サーバー間でのパッチと必要なアップデートのリストを送信するプロセス

分離された管理サーバーに接続されている管理対象デバイスにアップデートをインストールして脆弱性を修正するには：

1. 実行されていない場合は、*アップデートのインストールと脆弱性の修正*タスクを実行します。
2. 外付けドライブを分離された任意の管理サーバーに接続します。
3. 外付けドライブに2つのフォルダーを作成します。1つは必要なアップデートのリスト用で、もう1つはパッチ用です。これらのフォルダーには好きな名前を付けることができます。

   以前にフォルダーを作成していた場合は、それらを消去します。
4. すべての分離された管理サーバーから必要なアップデートのリストをコピーして、外付けドライブ上にある必要なアップデートのリスト用のフォルダーに貼り付けます。

   結果、すべての分離された管理サーバーから取得したすべてのリストを1津のフォルダーに集約したことになります。このフォルダーには、分離されたすべての管理サーバーに必要なパッチのIDが付いたバイナリファイルが含まれます。
5. 外付けドライブをインターネットにアクセス可能な管理サーバーに接続します。
6. 外付けドライブから必要なアップデートのリストをコピーして、インターネットにアクセス可能な管理サーバー上にある必要なアップデート用のフォルダーに貼り付けます。

   すべての必要なパッチは、管理サーバー上にあるパッチ用のフォルダーにインターネットから自動的にダウンロードされます。これには数時間かかる場合があります。

7. 必要なパッチがすべてダウンロードされていることを確認してください。この目的のために、次の操作のうち1つを実行できます：

   - インターネットにアクセス可能な管理サーバー上のパッチがないかフォルダーを確認してください。必要なアップデートのリストで指定されたすべてのパッチは、必要なフォルダーにダウンロードされます。これは、必要なパッチの数が少ない場合に便利です。

   - シェルスクリプトなどの特別なスクリプトを準備します。多数のパッチを入手した場合、すべてのパッチがダウンロードされたことを自分で確認するのは難しくなります。このような場合は、チェックを自動化することをお勧めします。

8. インターネットにアクセス可能な管理サーバーからパッチをコピーして、外付けドライブの対応するフォルダーに貼り付けます。

9. 分離されたすべての管理サーバーにパッチを転送します。パッチを特定のフォルダーに入れます。

その結果、分離されたすべての管理サーバーは、現在の管理サーバーに接続されている管理対象デバイスに必要なアップデートの実際のリストを作成します。インターネットにアクセス可能な管理サーバーが必要なアップデートのリストを受信した後、管理サーバーはインターネットからパッチをダウンロードします。パッチが分離された管理サーバー上に現れると、*アップデートのインストールと脆弱性の修正*タスクがパッチを処理します。このように、アップデートが管理対象デバイスにインストールされ、ソフトウェアの脆弱性が修正されます。

*アップデートのインストールと脆弱性の修正*タスクの実行中には、管理サーバーデバイスを再起動しないでください。また、再起動を必要とする*管理サーバーデータのバックアップ*タスクも実行しないでください。*アップデートのインストールと脆弱性の修正*タスクが中断され、アップデートがインストールされません。この場合、このタスクを手動で再開するか、設定されたスケジュールに従って実行されるまで待つ必要があります。

分離されたネットワークでのパッチの送信とアップデートのインストールを無効にする

分離されたネットワークから1つまたはそれ以上のサーバーを取り出すことにした場合など、分離された管理サーバーでパッチの送信を無効にすることができます。このように、パッチの数とそれらをダウンロードする時間を削減することができます。

分離された管理サーバーでパッチの転送を無効にするには：

1. 管理サーバーを分離状態から取り出すには、インターネットに接続できる管理サーバーのプロパティで、パッチのフォルダーと必要なアップデートのリストからパスを削除してください。分離されたネットワークに管理サーバーをそのまま置いておくには、この手順を省略してください。

   Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

   コマンドプロンプトで次のコマンドを入力します：

   - パッチのフォルダーのパスを削除するには：
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```

   - 必要なアップデートのリストのフォルダーのパスを削除するには：
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. 管理サーバーのフォルダーのパスを削除した場合はこの管理サーバーサービスを再起動してください。

3. 分離状態から取り出すすべての管理サーバーのプロパティで、パッチのフォルダーのパスと必要なアップデートのリストのフォルダーのパスを削除してください。

   管理者権限を使用し、Windows コマンドプロンプトで次のコマンドを入力します：

   - パッチのフォルダーのパスを削除するには：
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""`
   - 必要なアップデートのリストのフォルダーのパスを削除するには：
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""`

4. フォルダーのパスを削除したすべての管理サーバーのサービスを再起動します。

インターネットにアクセス可能な管理サーバーを再設定すると、Kaspersky Security Center を介してパッチを受信することはなくなります。たとえば、一部の分離された管理サーバーのみを再設定し、それらの一部を分離されたネットワークから削除すると、残りの分離された管理サーバーのパッチのみを受け取ることになります。

将来、無効になっている分離された管理サーバーの脆弱性の修正を開始する場合は、もう一度これらの管理サーバーとインターネットにアクセスできる管理サーバーを構成する必要があります。

検知されたソフトウェアの脆弱性への非対応の判断

必要に応じて、検知されたソフトウェア脆弱性を無視することもできます。ソフトウェア脆弱性に対応しない理由として、次が考えられます：

- 管理者として、該当するソフトウェアの脆弱性が組織内で緊急なものではないと判断した場合。
- 脆弱性の修正を適用すると、該当するソフトウェアでデータの破損などが生じる可能性があることが判明した場合。
- 管理者として、管理対象デバイスを保護する別の対策を使用しているため、ソフトウェア脆弱性が組織ネットワークにとって危険ではないと判断した場合。

すべてのデバイス上または選択した特定のデバイス上で、ソフトウェア脆弱性を無視できます。

すべての管理対象デバイスで、特定のソフトウェア脆弱性に対応せずに無視するには：

1. コンソールツリーの［**詳細**］フォルダーで、［**アプリケーションの管理**］フォルダーから［**ソフトウェアの脆弱性**］サブフォルダーを選択します。

   フォルダーの作業領域に、デバイスにインストールされているアプリケーションからネットワークエージェントが検知した脆弱性のリストが表示されます。

2. 対応せずに無視する脆弱性を選択します。

3. 脆弱性のコンテキストメニューから［**プロパティ**］を選択します。

   脆弱性のプロパティウィンドウが表示されます。

4. ［**全般**］セクションで、［**脆弱性を無視**］をオンにします。

5. ［**OK**］をクリックします。

   ソフトウェア脆弱性のプロパティウィンドウが閉じます。

すべての管理対象デバイスで、対象のソフトウェア脆弱性が無視されます。

選択した管理対象デバイスで、特定のソフトウェア脆弱性に対応せずに無視するには：

1. 選択した管理対象デバイスのプロパティウィンドウを開き、［**ソフトウェアの脆弱性**］セクションを選択します。
2. ソフトウェアの脆弱性を選択します。
3. 選択した脆弱性を無視することを選択します。

選択したデバイスで、対象のソフトウェア脆弱性が無視されます。

無視することを選択したソフトウェアの脆弱性は、［*脆弱性の修正*］タスクまたは［*アップデートのインストールと脆弱性の修正*］タスクが完了しても修正されません。脆弱性のリストで、無視することを選択した脆弱性をフィルターを使用して表示から除外することができます。

サードパーティ製ソフトウェアの脆弱性へのユーザー修正の選択

［*脆弱性の修正*］タスクを使用するには、タスクの設定で、サードパーティ製ソフトウェアの脆弱性を修正するソフトウェアアップデートを手動で指定する必要があります。［*脆弱性の修正*］タスクでは、Microsoft 製品に対しては推奨される修正を、その他のサードパーティ製ソフトウェアに対してはユーザー修正をインストールして脆弱性を修正します。*ユーザー修正*は、脆弱性を修正するためにインストールするように管理者が手動で指定するソフトウェアアップデートです。

サードパーティ製ソフトウェアの脆弱性へのユーザー修正を選択するには：

1. コンソールツリーの［**詳細**］→［**アプリケーションの管理**］フォルダーで、［**ソフトウェアの脆弱性**］サブフォルダーを選択します。

   フォルダーの作業領域に、デバイスにインストールされているアプリケーションからネットワークエージェントが検知した脆弱性のリストが表示されます。
2. ユーザー修正を指定する脆弱性を選択します。
3. 脆弱性のコンテキストメニューから［**プロパティ**］を選択します。

   脆弱性のプロパティウィンドウが表示されます。
4. ［**ユーザーによる修正とその他の修正**］セクションで、［**追加**］をクリックします。

   使用可能なインストールパッケージのリストが表示されます。ここで表示されるインストールパッケージのリストは、［**リモートインストール**］→［**インストールパッケージ**］リストの順に移動して表示されるリストと同じものです。選択している脆弱性に対するユーザー修正を含んだインストールパッケージを作成していない場合、新規パッケージウィザードを起動してパッケージを作成できます。
5. サードパーティ製ソフトウェアの脆弱性に対するユーザー修正を含んだインストールパッケージを1つ以上選択します。
6. ［**OK**］をクリックします。

ソフトウェア脆弱性に対するユーザー修正を含んだインストールパッケージが指定されます。*脆弱性の修正*タスクが実行されると、インストールパッケージがインストールされてソフトウェア脆弱性が修正されます。

アップデートインストールのルール

アプリケーションの脆弱性を修正する時には、アップデートのインストールに関するルールを指定する必要があります。これらのルールにより、どのアップデートをインストールし、どの脆弱性を修正するかが決まります。

ルールの設定内容は、Microsoft 製品の更新プログラムのみを対象としたルールを作成するのか、サードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のみを対象としたルールを作成するのか、それともそれらすべての製品を対象としたルールを作成するのかによって異なります。Microsoft 製品またはサードパーティ製品のいずれかのみを対象にルールを作成する場合、特定のアプリケーションとバージョンを選択してアップデートをインストールできます。すべての製品を対象にルールを作成する場合、インストールする特定のアップデートおよびアップデートをインストールすることで修正する脆弱性を選択できます。

すべての製品のアップデートを対象とするルールを作成するには：

1. 新規タスクウィザードの［**設定**］ページで、［**追加**］をクリックします。
   ルール作成ウィザードが起動します。ウィザードの指示に従ってください。
2. ［**ルールの種別**］ウィンドウで、［**すべてのアップデートのルール**］を選択します。
3. ［**全般基準**］ウィンドウで、ドロップダウンリストを使用して次の設定を指定します：
   - **インストールするアップデートの設定**

     クライアントデバイスにインストールする必要がある更新を選択します。
     - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
     - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
     - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。
   - **次のレベル以上の深刻度の脆弱性を修正する**

     ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

     このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

     このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

     既定では、このオプションはオフです。
4. ［**アップデート**］ページで、インストールするアップデートを選択します：
   - **すべての適用可能なアップデートをインストールする**

ウィザードの［**全般基準**］ウィンドウで指定した基準に合致するソフトウェアアップデートをすべてインストールします。既定では、この項目が選択されます。

- **リストのアップデートのみをインストールする**

  手動で選択したリストのソフトウェアアップデートのみをインストールします。追加できるアップデートには、使用可能なすべてのソフトウェアアップデートが含まれます。

  特定のアップデートを選択する状況としてはたとえば、テスト環境でのインストールの確認、重要なアプリケーションのみのアップデート、特定のアプリケーションのみのアップデートなどが考えられます。

  - **選択したアップデートのインストールに必要な以前のアップデートをすべて自動的にインストールする**

    選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、このオプションをオンのままにします。

    このオプションをオフにすると、選択したバージョンのアプリケーションのみがインストールされます。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、このオプションをオフにします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

    たとえば、デバイスにアプリケーションのバージョン 3 がインストールされていて、バージョン 5 にアップデートしたいが、バージョン 5 はバージョン 4 経由のみでしかインストールできない状況を想定します。このオプションをオンにすると、先にバージョン 4 をインストールし、続いてバージョン 5 をインストールします。このオプションをオフにすると、アプリケーションのアップデートは失敗します。

    既定では、このオプションはオンです。

5. ［**脆弱性**］ページで、選択したアップデートのインストールで修正する脆弱性を選択します：

   - **他の基準に一致するすべての脆弱性を修正する**

     ウィザードの［**全般基準**］ウィンドウで指定した基準に合致する脆弱性をすべて修正します。既定では、この項目が選択されます。

   - **リストの脆弱性のみを修正する**

     手動で選択したリストの脆弱性のみをインストールします。追加できるアップデートには、検知されたすべての脆弱性が含まれます。

     特定の脆弱性を選択する状況としてはたとえば、テスト環境での脆弱性の修正の確認、重要なアプリケーションのみでの脆弱性の修正、特定のアプリケーションのみでの脆弱性の修正などが考えられます。

6. ［**名前**］ウィンドウで、作成中のルール名を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**設定**］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが作成され、新規タスクウィザードの［**アップデートのインストールのルールを指定します**］に表示されます。

Microsoft 製品のアップデートを対象とするルールを作成するには：

1. 新規タスクウィザードの［**設定**］ページで、［**追加**］をクリックします。
   ルール作成ウィザードが起動します。ウィザードの指示に従ってください。

2. ［**ルールの種別**］ページで、［**Windows Update のルール**］を選択します。

3. ［**全般基準**］ウィンドウで、次の設定を指定します：

   - **インストールするアップデートの設定**

     クライアントデバイスにインストールする必要がある更新を選択します。
     - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
     - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
     - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。

   - **次のレベル以上の深刻度の脆弱性を修正する**

     ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

     このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

     このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

     既定では、このオプションはオフです。

   - **次のレベル以上の MSRC 深刻度の脆弱性を修正する**

     ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

     このオプションをオンにすると、MSRC（Microsoft Security Response Center）が設定する重要度レベルが、リストで選択した値（**低**、**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

     このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

     既定では、このオプションはオフです。

4. ［**アプリケーション**］ウィンドウで、アップデートをインストールするアプリケーションとアプリケーションのバージョンを選択します。既定では、すべてのアプリケーションがオンです。

5. ［**アップデートのカテゴリ**］ページで、インストールするアップデートのカテゴリを選択します。これらのカテゴリは Microsoft Update カタログで使用されているのと同じカテゴリです。既定では、すべてのカテゴリがオンです。

6. ［**名前**］ウィンドウで、作成中のルール名を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**設定**］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが作成され、新規タスクウィザードの［**アップデートのインストールのルールを指定します**］に表示されます。

サードパーティ製品のアップデートを対象とするルールを作成するには：

1. 新規タスクウィザードの［**設定**］ページで、［**追加**］をクリックします。
   ルール作成ウィザードが起動します。ウィザードの指示に従ってください。
2. ［**ルールの種別**］ページで、［**サードパーティ製品のアップデートのルール**］を選択します。
3. ［**全般基準**］ウィンドウで、次の設定を指定します：
   - **インストールするアップデートの設定**
     クライアントデバイスにインストールする必要がある更新を選択します。
     - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
     - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
     - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。
   - **次のレベル以上の深刻度の脆弱性を修正する**
     ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。
     このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。
     このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。
     既定では、このオプションはオフです。
4. ［**アプリケーション**］ページで、アップデートをインストールするアプリケーションとアプリケーションのバージョンを選択します。既定では、すべてのアプリケーションがオンです。
5. ［**名前**］ウィンドウで、作成中のルール名を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**設定**］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが作成され、新規タスクウィザードの［**アップデートのインストールのルールを指定します**］に表示されます。

アプリケーションのグループ

このセクションでは、デバイスにインストールされているアプリケーショングループの管理方法について説明します。

アプリケーションカテゴリの作成

Kaspersky Security Center では、デバイスにインストールされているアプリケーションのカテゴリを作成できます。

アプリケーションのカテゴリは、次のいずれかの方法で作成できます：

- 選択したカテゴリの実行ファイルが含まれているフォルダーを指定する
- 選択したカテゴリに追加する実行ファイルがあるデバイスを指定する
- 選択したカテゴリにアプリケーションを追加するために使用する基準を設定する

アプリケーションカテゴリが作成されると、管理者はそのアプリケーションカテゴリのルールを設定できます。ルールにより、指定したカテゴリに含まれるアプリケーションの動作を定義します。たとえば、そのカテゴリに含まれるアプリケーションの起動をブロックしたり、許可したりできます。

デバイス上のアプリケーション実行の管理

Kaspersky Security Center を使用して、許可リストモードでのデバイスのアプリケーションの起動を管理することができます。詳細は、Kaspersky Endpoint Security for Windows のオンラインヘルプを参照してください。許可リストモードでは、選択したデバイスで指定カテゴリに含まれるアプリケーションのみ起動できます。管理者は、各ユーザーのデバイスに適用されたアプリケーション起動ルールの静的分析結果を表示できます。

デバイスにインストールされたソフトウェアのインベントリ

Kaspersky Security Center では、Windows および Linux を実行しているデバイス上のソフトウェアのインベントリを実行できます。デバイスにインストールされたすべてのアプリケーションの情報をネットワークエージェントが取得します。インベントリの実行中に収集された情報は、［**アプリケーションレジストリ**］フォルダーの作業領域に表示されます。管理者は、あらゆるアプリケーションの詳細情報を、そのバージョンや製造元を含めて表示できます。

1 台のデバイスから受信できる実行ファイルは、最大で 150,000 個です。この上限に達した場合、Kaspersky Security Center は新規ファイルを取得できません。

ライセンス認証済みアプリケーショングループの管理

Kaspersky Security Center では、ライセンス認証済みアプリケーショングループを作成できます。ライセンス認証済みアプリケーショングループには、管理者が設定した基準を満たすアプリケーションが含まれます。管理者は、ライセンス認証済みアプリケーショングループについて次の基準を指定できます：

- アプリケーション名

- アプリケーションのバージョン
- 製造元
- アプリケーションタグ

1つ以上の基準を満たすアプリケーションが、自動的にグループに含まれます。ライセンス認証済みアプリケーショングループを作成するには、グループにアプリケーションを含めるための1つ以上の基準を設定する必要があります。

ライセンス認証済みアプリケーションの各グループにはそれぞれのライセンスがあります。ライセンス認証されたグループのライセンスにより、そのグループに含まれるアプリケーションをインストールできる最大数が決定されます。アプリケーションのインストール数がライセンスで設定された上限を超えると、アプリケーションサーバーに情報イベントが記録されます。管理者は、ライセンスの有効期限を指定できます。有効期限になると、管理サーバーに情報イベントが記録されます。

実行ファイルに関する情報の表示

Kaspersky Security Center は、オペレーティングシステムがインストールされて以後に各デバイスで実行された実行ファイルに関する全情報を取得します。実行ファイルの情報は、メインウィンドウの［**実行ファイル**］フォルダーの作業領域に表示されます。

アプリケーションコントロールを使用して実行ファイルを管理する

アプリケーションコントロールコンポーネントを使用すると、ユーザーデバイス上の実行ファイルの起動を許可またはブロックできます。アプリケーションコントロールコンポーネントは、Windows ベースおよび Linux ベースのオペレーティングシステムをサポートします。

Linux ベースのオペレーティングシステムの場合、Application Control コンポーネントは Kaspersky Endpoint Security 11.2 for Linux 以降から使用できます。

必須条件

- 組織内に Kaspersky Security Center が導入されている。
- Kaspersky Endpoint Security for Windows または Kaspersky Endpoint Security for Linux のポリシーが作成され、有効になっている。

実行するステップ

アプリケーションコントロールのユーザーシナリオは次のステップに分かれています：

1. **クライアントデバイス上の実行ファイルのリストの作成と表示**

   このステップでは、管理対象デバイスでどのような実行ファイルが検知されたかを把握できます。実行ファイルのリストを表示して、許可対象の実行ファイルと禁止対象の実行ファイルのリストと照合してください。組織の情報セキュリティポリシーに関連した制限が実行ファイルに対して必要になる場合もあります。

   実行手順の説明：

- 管理コンソール：実行ファイルのインベントリ
- Kaspersky Security Center Web コンソール：クライアントデバイスにある実行ファイルのリストの取得と表示

2 組織内で使用される実行ファイルのカテゴリを作成する

管理対象デバイスに保管されている実行ファイルのリストを分析します。分析に基づいて、実行ファイルのカテゴリを作成します。組織で使用される標準的な実行ファイル群をカバーする「作業用アプリケーション」カテゴリを作成することを推奨します。異なるセキュリティグループがそれぞれの業務で実行ファイルセットを使用する場合、セキュリティグループごとに別のカテゴリを作成することができます。

実行手順の説明：

- 管理コンソール：コンテンツが手動で追加されるアプリケーションカテゴリの作成、選択したデバイス上の実行ファイルが含まれるアプリケーションカテゴリの作成、特定のフォルダーの実行ファイルが含まれるアプリケーションカテゴリの作成。
- Kaspersky Security Center Web コンソール：コンテンツが手動で追加されるアプリケーションカテゴリの作成、選択したデバイス上の実行ファイルが含まれるアプリケーションカテゴリの作成、特定のフォルダーの実行ファイルが含まれるアプリケーションカテゴリの作成。

3 Kaspersky Endpoint Security ポリシーでのアプリケーションコントロール機能の設定

上述したステップで作成したカテゴリを使用して、Kaspersky Endpoint Security ポリシー内でアプリケーションコントロール機能を設定します。

実行手順の説明：

- 管理コンソール：クライアントデバイスでのアプリケーション起動コントロールの設定
- Kaspersky Security Center Web コンソール：Kaspersky Endpoint Security ポリシーでのアプリケーションコントロールの設定

4 アプリケーションコントロール機能のテストモードでの有効化

アプリケーションコントロールルールが業務で必要な実行ファイルをブロックしないことを確認するため、新規ルールの作成後にテストを有効にして動作を検証することを推奨します。テストモードで実行している場合、Kaspersky Endpoint Security for Windows は、アプリケーションコントロールルールで起動が禁止されている実行ファイルをブロックせず、その起動について管理サーバーに通知します。

アプリケーションコントロールルールのテストでは、次の手順の実施を推奨します：

- 必要に応じたテスト期間を指定する。必要なテスト期間は数日から 2 カ月ほどまで、ルールに応じて異なります。
- アプリケーションコントロールの動作テストによって記録されたイベントを分析する。

Kaspersky Security Center Web コンソールの使用方法：Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定これらの手順に従って、設定プロセスで**テストモード**を有効にします。

5 アプリケーションコントロール機能におけるカテゴリ設定の変更

必要に応じて、アプリケーションコントロール設定に変更を行います。テスト結果に応じて、アプリケーションコントロールコンポーネントのイベントに関連していた実行ファイルを「手動でコンテンツを追加するカテゴリ」に追加できます。

実行手順の説明：

- 管理コンソール：イベントに関連する実行ファイルのアプリケーションカテゴリへの追加

- Kaspersky Security Center Web コンソール：イベントに関連する実行ファイルのアプリケーションカテゴリへの追加

6. **アプリケーションコントロールルールの実運用での適用**

   アプリケーションコントロールルールのテストとカテゴリの設定が完了したら、運用モードで実際にアプリケーションコントロールルールを適用できます。

   Kaspersky Security Center Web コンソールの使用方法：Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定これらの手順に従って、設定プロセスで**テストモード**を無効にします。

7. **アプリケーションコントロールの設定の検証**

   次の手順がすべて完了していることを確認してください：

   - 実行ファイルのカテゴリを作成しました。
   - カテゴリを使用してアプリケーションコントロールルールの設定します。
   - アプリケーションコントロールルールの実運用での適用。

結果

シナリオが完了すると、管理対象デバイス上の実行ファイルの起動がコントロールされます。ユーザーは、組織で許可されている実行ファイルのみを実行することができ、組織で禁止されている実行ファイルを実行することはできません。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ
- Kaspersky Security for Virtualization Light Agent

Kaspersky Endpoint Security for Windows ポリシー用のアプリケーションカテゴリの作成

［**アプリケーションカテゴリ**］フォルダーまたは Kaspersky Endpoint Security for Windows ポリシーの［**プロパティ**］ウィンドウから Kaspersky Endpoint Security for Windows ポリシー用のアプリケーションカテゴリを作成できます。

*［**アプリケーションカテゴリ**］フォルダーから Kaspersky Endpoint Security ポリシー用のアプリケーションカテゴリを作成するには：*

1. コンソールツリーで、［**詳細**］→［**アプリケーションの管理**］→［**アプリケーションカテゴリ**］の順に選択します。
2. ［**アプリケーションカテゴリ**］フォルダーの作業領域で［**新しいカテゴリ**］をクリックします。

   新規カテゴリウィザードが起動します。
3. ［**カテゴリ種別**］ウィンドウで、アプリケーションカテゴリの種別を選択します：

- **手動でコンテンツを追加するカテゴリ**：実行ファイルを作成中のカテゴリに割り当てるために使用される基準を指定します。
- **自動でコンテンツが追加されるカテゴリ**：作成されたカテゴリに実行ファイルを自動的に割り当てる時の割り当て元のフォルダーを指定します。

  コンテンツを自動で追加するカテゴリを作成する場合、以下のファイル種別に対してインベントリが実行されます：EXE、COM、DLL、SYS、BAT、PS1、CMD、JS、VBS、REG、MSI、MSC、CPL、HTML、HTM、DRV、OCX、SCR。

- **選択したデバイスの実行ファイルを含むカテゴリ**：実行ファイルをカテゴリに自動的に割り当てる必要があるデバイスを指定します。

4. ウィザードの指示に従ってください。

ウィザードが完了すると、カスタマイズされたアプリケーションカテゴリが作成されます。［**アプリケーションカテゴリ**］フォルダーの作業領域のカテゴリリストを使用して、新しく作成したカテゴリを確認できます。

アプリケーションカテゴリは、［**ポリシー**］フォルダーからも作成できます。

*Kaspersky Endpoint Security for Windows ポリシーの［**プロパティ**］ウィンドウから、アプリケーションカテゴリを作成するには：*

1. コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. ［**ポリシー**］フォルダーの作業領域で、カテゴリを作成先の Kaspersky Endpoint Security ポリシーを選択します。
3. 右クリックして、［**プロパティ**］を選択します。
4. ［**プロパティ**］ウィンドウが開いたら、左側の［**セクション**］ペインで、［**セキュリティコントロール**］→［**アプリケーションコントロール**］の順に選択します。
5. ［**アプリケーションコントロール**］セクションで、［**コントロールモード**］と［**処理**］ドロップダウンリストで拒否リストまたは許可リストを選択し、［**追加**］をクリックします。

   ［**アプリケーションコントロールルール**］ウィンドウが開き、カテゴリのリストが表示されます。
6. ［**新規作成**］をクリックします。
7. 新規カテゴリの名前を入力し［**OK**］をクリックします。

   新規カテゴリウィザードが起動します。
8. ［**カテゴリ種別**］ウィンドウで、アプリケーションカテゴリの種別を選択します：
   - **手動でコンテンツを追加するカテゴリ**：実行ファイルを作成中のカテゴリに割り当てるために使用される基準を指定します。
   - **自動でコンテンツが追加されるカテゴリ**：作成されたカテゴリに実行ファイルを自動的に割り当てる時の割り当て元のフォルダーを指定します。

コンテンツを自動で追加するカテゴリを作成する場合、以下のファイル種別に対してインベントリが実行されます：EXE、COM、DLL、SYS、BAT、PS1、CMD、JS、VBS、REG、MSI、MSC、CPL、HTML、HTM、DRV、OCX、SCR。

- **選択したデバイスの実行ファイルを含むカテゴリ**：実行ファイルをカテゴリに自動的に割り当てる必要があるデバイスを指定します。

9. ウィザードの指示に従ってください。

ウィザードが完了すると、カスタマイズされたアプリケーションカテゴリが作成されます。新しく作成したカテゴリは、カテゴリのリストで確認できます。

アプリケーションカテゴリは、Kaspersky Endpoint Security for Windows に内蔵されたアプリケーションコントロールコンポーネントによって使用されます。アプリケーションコントロールを使用して、クライアントデバイスでアプリケーションの起動を制限することができます。たとえば、指定したカテゴリ内のアプリケーションのみが起動されるよう制限できます。

コンテンツが手動で追加されるアプリケーションカテゴリの作成

組織内で起動を許可またはブロックする実行ファイルのテンプレートとしての条件を、単独でまたは組み合わせて指定できます。一定の条件に一致する実行ファイルをまとめて管理するために、アプリケーションカテゴリを作成してアプリケーションコントロールの設定で使用できます。

コンテンツが手動で追加されるアプリケーションカテゴリを作成するには：

1. コンソールツリーで、［**詳細**］フォルダーから［**アプリケーションの管理**］フォルダーに進み、［**アプリケーションカテゴリ**］サブフォルダーを選択します。

2. ［**新しいカテゴリ**］をクリックします。

［**新規カテゴリウィザード**］が起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ［**カテゴリ種別**］ウィザードページで、ユーザーカテゴリタイプとして［**手動で追加したコンテンツによるカテゴリ**］をオンにします。

4. ［**アプリケーションカテゴリ名の入力**］ウィザードページで、新しいアプリケーションカテゴリ名を入力します。

5. ［**カテゴリにアプリケーションを含める条件の設定**］ページで、［**追加**］をクリックします。

6. ドロップダウンリストで、関連する設定を指定します：

- **実行ファイルのリストから**

このオプションをオンにすると、クライアントデバイス上の実行ファイルのリストを使用して、アプリケーションを選択してカテゴリに追加できます。

- **ファイルのプロパティ**

このオプションをオンにすると、アプリケーションカテゴリに追加する実行ファイルの詳細なデータを指定できます。

- **フォルダーのファイルのメタデータ**

  実行ファイルを含んだクライアントデバイスのフォルダーを指定します。指定フォルダーにある実行ファイルのメタデータが管理サーバーに送信されます。同じメタデータを含む実行ファイルがアプリケーションカテゴリに追加されます。

- **フォルダーに含まれるファイルのチェックサム**

  このオプションをオンにすると、クライアントデバイス上のフォルダーを選択または作成できます。指定フォルダーにあるファイルの MD5 ハッシュが管理サーバーに送信されます。指定フォルダーにあるファイルとハッシュが同じであるアプリケーションが、アプリケーションカテゴリに追加されます。

- **フォルダー内のファイルの証明書**

  このオプションをオンにすると、証明書で署名された実行ファイルを含むフォルダーをクライアントデバイス上で指定できます。読み込まれた実行ファイルの証明書は、カテゴリの条件に追加されます。指定された証明書に従って署名された実行ファイルが、アプリケーションカテゴリに追加されます。

- **MSI インストーラーファイルのメタデータ**

  このオプションをオンにすると、MSI インストーラーファイルを、アプリケーションカテゴリにアプリケーションを追加する条件として指定できます。アプリケーションのインストーラーのメタデータが管理サーバーに送信されます。インストーラーのメタデータが指定の MSI インストーラーと同じアプリケーションが、アプリケーションカテゴリに追加されます。

- **MSI インストーラーに含まれるファイルのチェックサム**

  このオプションをオンにすると、MSI インストーラーファイルを、アプリケーションカテゴリにアプリケーションを追加する条件として指定できます。アプリケーションのインストーラーファイルのハッシュが管理サーバーに送信されます。MSI インストーラーファイルのハッシュが指定のハッシュと同一のアプリケーションが、アプリケーションカテゴリに追加されます。

- **KL カテゴリから選択**

  このオプションをオンにすると、カスペルスキー製品のカテゴリを、アプリケーションカテゴリにアプリケーションを追加する条件として指定できます。指定したカスペルスキー製品カテゴリのアプリケーションが、アプリケーションカテゴリに追加されます。

- **アプリケーションのパスを指定（マスクをサポート）**

このオプションをオンにすると、クライアントデバイス上のファイルやフォルダーのパスを指定できます。指定したファイルやフォルダーに含まれる実行ファイルが、アプリケーションカテゴリに追加されます。「*C:\path_to_exe**」などの正規表現を使用できます。例： *C:\Program Files\Internet Explorer**。

- **リポジトリから証明書を選択**

  このオプションをオンにすると、保管領域の証明書を指定できます。指定された証明書に従って署名された実行ファイルが、アプリケーションカテゴリに追加されます。

- **ドライブ種別**

  このオプションをオンにすると、アプリケーションを実行するメディアの種別（任意のドライブまたはリムーバブルドライブ）を指定できます。指定した種別のドライブ上で実行されたアプリケーションが、アプリケーションカテゴリに追加されます。

7. ［**アプリケーションカテゴリの作成**］ウィザードページで、［**終了**］をクリックします。

Kaspersky Security Center は、デジタルで署名されたファイルからのメタデータのみを取り扱います。デジタル署名を含まないファイルからのメタデータに基づいたカテゴリは作成されません。

ウィザードが完了するとアプリケーションカテゴリが作成され、コンテンツが手動で追加されます。［**アプリケーションカテゴリ**］フォルダーの作業領域のカテゴリリストを使用して、新しく作成したカテゴリを確認できます。

選択したデバイスの実行ファイルを含むアプリケーションカテゴリの作成

選択したデバイス上に存在する実行ファイルを、許可またはブロックする実行ファイルのテンプレートとして使用できます。選択したデバイス上に存在する実行ファイルを基準に、アプリケーションカテゴリを作成してアプリケーションコントロールの設定で使用できます。

デバイスから実行ファイルのリストを取得するには：

1. Kaspersky Endpoint Security for Windows または Kaspersky Endpoint Security for Linux のポリシーが作成され、有効になっていることを確認します。ポリシーでアプリケーションコントロールコンポーネントを有効にします。
2. クライアントデバイスに保存されている実行ファイルのリストを取得します。

選択したデバイスの実行ファイルを含むアプリケーションカテゴリを作成するには：

1. コンソールツリーで、［**詳細**］フォルダーから［**アプリケーションの管理**］フォルダーに進み、［**アプリケーションカテゴリ**］サブフォルダーを選択します。
2. ［**新しいカテゴリ**］をクリックします。

   ［**新規カテゴリウィザード**］が起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ［**カテゴリ種別**］ウィザードページで、ユーザーカテゴリの種類として、［**選択したデバイスからの実行ファイルを含むカテゴリ**］をオンにします。

4. ［**アプリケーションカテゴリ名の入力**］ウィザードページで、新しいアプリケーションカテゴリ名を入力します。

5. ［**設定**］ウィザードページで、［**追加**］をクリックします。

6. アプリケーションカテゴリーを作成するために、実行ファイルを使用するデバイスを選択します。

7. 次の設定を指定します：

- **ハッシュ値計算アルゴリズム**

  ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、このカテゴリ内のファイルに、Kaspersky Security Center によるハッシュ値計算のアルゴリズムを選択する必要があります。計算されたハッシュ値に関する情報は、管理サーバーのデータベースに保存されます。ハッシュ値の保存でデータベースのサイズが大幅に増えることはありません。

  暗号学的ハッシュ関数 SHA256 はアルゴリズムに脆弱性が発見されておらず、現在最も信頼できる暗号化機能と判断されています。SHA256 計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降でサポートされています。ハッシュ関数 MD5 の計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のすべてのバージョンでサポートされます。

  カテゴリ内のファイルに、Kaspersky Security Center によるハッシュ値計算のオプションを選択します：

  - ネットワークにインストールされているセキュリティ製品のすべてのインスタンスが Kaspersky Endpoint Security 10 Service Pack 2 for Windows またはそれ以降のバージョンである場合は、［**SHA256**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンで、実行ファイルの SHA256 ハッシュ値の基準に従って作成したカテゴリは追加しないでください。セキュリティ製品の動作に不具合が生じることがあります。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 MD5 を使用することができます。

  - ネットワークに Kaspersky Endpoint Security 10 Service Pack 2 for Windows より以前のバージョンの製品がインストールされている場合は、［**MD5 ハッシュ**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョン向けの実行ファイルの MD5 チェックサムの基準に従って作成したカテゴリは追加できません。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 SHA256 を使用できます。

  ネットワークにある別々の端末で Kaspersky Endpoint Security 10 の以前のバージョンと以降のバージョンと両方が使用されている場合は、［**SHA256**］と［**MD5 ハッシュ**］の両方をオンにしてください。

  既定では、［**このカテゴリのファイルの SHA256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）**］が選択されています。

  ［**このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）**］は既定ではオフです。

- **データを管理サーバーのリポジトリと同期**

  指定したフォルダーでの変更内容を管理サーバーに定期的にチェックさせる場合は、このオプションを使用します。

  既定では、このオプションはオフです。

  このオプションをオンにする場合、指定したフォルダーでの変更内容をチェックする間隔（時間単位）を指定します。既定の間隔は 24 時間です。

8. ［**フィルター**］ウィザードページで、以下の設定を行います：

- **ファイル種別**

  このセクションでは、アプリケーションカテゴリを作成するのに使用するファイルの種別を指定できます。

  すべてのファイル：カテゴリの作成時にすべてのファイルが使用されます。既定では、このオプションがオンです。

  アプリケーションカテゴリ以外のファイルのみ：カテゴリの作成時に、アプリケーションカテゴリ以外のファイルのみが使用されます。

- **フォルダー**

  このセクションでは、選択したデバイス上で、アプリケーションカテゴリを作成するのに使用するファイルが含まれているフォルダーを指定できます。

  すべてのフォルダー：カテゴリの作成時にすべてのフォルダーのファイルが使用されます。既定では、このオプションがオンです。

  指定フォルダー：カテゴリの作成時に指定したフォルダーのファイルのみが使用されます。このオプションをオンにする場合、フォルダーのパスを指定する必要があります。

9. ［**アプリケーションカテゴリの作成**］ウィザードページで、［**終了**］をクリックします。

ウィザードが完了すると、ユーザーアプリケーションカテゴリが作成されます。［**アプリケーションカテゴリ**］フォルダーの作業領域のカテゴリリストを使用して、新しく作成したカテゴリを確認できます。

特定のフォルダーにある実行ファイルを含むアプリケーションカテゴリの作成

選択したフォルダー上に存在する実行ファイルを、組織内で許可またはブロックする実行ファイルの条件として使用できます。選択したフォルダー上に存在する実行ファイルを基準に、アプリケーションカテゴリを作成してアプリケーションコントロールの設定で使用できます。

特定のフォルダーの実行ファイルを含むアプリケーションカテゴリを作成するには：

1. コンソールツリーで、［**詳細**］フォルダーから［**アプリケーションの管理**］フォルダーに進み、［**アプリケーションカテゴリ**］サブフォルダーを選択します。

2. ［**新しいカテゴリ**］をクリックします。

   ［**新規カテゴリウィザード**］が起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ［**カテゴリ種別**］ウィザードページで、ユーザーカテゴリの種類として［**特定のフォルダーの実行ファイルを含むカテゴリ**］を選択します。

4. ［**アプリケーションカテゴリ名の入力**］ウィザードページで、新しいアプリケーションカテゴリ名を入力します。

5. ［**リポジトリフォルダー**］ウィザードページで、［**参照**］をクリックします。

6. アプリケーションカテゴリの作成に使用される実行ファイルのフォルダーを指定します。

7. 次の設定を定義します：

- **ダイナミックリンクライブラリ（DLL）をこのカテゴリに含める**

  アプリケーションカテゴリにはダイナミックリンクライブラリ（DLL 形式のファイル）が含まれ、アプリケーションコントロールコンポーネントでは、システムで実行されているそのようなライブラリの処理を記録します。このカテゴリに DLL ファイルを含めると、Kaspersky Security Center のパフォーマンスが低下することがあります。

  既定では、このチェックボックスはオフです。

- **このカテゴリ内のスクリプトデータを含める**

  アプリケーションカテゴリにはスクリプトのデータが含まれ、ウェブ脅威対策によってスクリプトはブロックされません。このカテゴリにスクリプトデータを含めると、Kaspersky Security Center のパフォーマンスが低下することがあります。

  既定では、このチェックボックスはオフです。

- **ハッシュ値計算アルゴリズム**：**このカテゴリのファイルの SHA256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）/ このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）**

  ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、このカテゴリ内のファイルに、Kaspersky Security Center によるハッシュ値計算のアルゴリズムを選択する必要があります。計算されたハッシュ値に関する情報は、管理サーバーのデータベースに保存されます。ハッシュ値の保存でデータベースのサイズが大幅に増えることはありません。

  暗号学的ハッシュ関数 SHA256 はアルゴリズムに脆弱性が発見されておらず、現在最も信頼できる暗号化機能と判断されています。SHA256 計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降でサポートされています。ハッシュ関数 MD5 の計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のすべてのバージョンでサポートされます。

  カテゴリ内のファイルに、Kaspersky Security Center によるハッシュ値計算のオプションを選択します：

  - ネットワークにインストールされているセキュリティ製品のすべてのインスタンスが Kaspersky Endpoint Security 10 Service Pack 2 for Windows またはそれ以降のバージョンである場合は、［**SHA256**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンで、実行ファイルの SHA256 ハッシュ値の基準に従って作成したカテゴリは追加しないでください。セキュリティ製品の動作に不具合が生じることがあります。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 MD5 を使用することができます。

  - ネットワークに Kaspersky Endpoint Security 10 Service Pack 2 for Windows より以前のバージョンの製品がインストールされている場合は、［**MD5 ハッシュ**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョン向けの実行ファイルの MD5 チェックサムの基準に従って作成したカテゴリは追加できません。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 SHA256 を使用できます。

  ネットワークにある別々の端末で Kaspersky Endpoint Security 10 の以前のバージョンと以降のバージョンと両方が使用されている場合は、［**SHA256**］と［**MD5 ハッシュ**］の両方をオンにしてください。

  既定では、［**このカテゴリのファイルの SHA256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）**］が選択されています。

  ［**このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）**］は既定ではオフです。

- **変更のあったフォルダーを強制スキャンする**

  このオプションを有効にすると、カテゴリコンテンツ追加のフォルダーでの変更が定期的にチェックされます。チェックボックスに隣接する入力フィールドで、チェックの頻度を時間単位で指定できます。既定では、24 時間ごとに強制的にチェックされます。

  このオプションを無効にすると、フォルダーが強制的にチェックされることはありません。ファイルの修正、追加または削除があった場合、サーバーはそのファイルにアクセスを試みます。

  既定では、このオプションはオフです。

8. ［**アプリケーションカテゴリの作成**］ウィザードページで、［**終了**］をクリックします。

ウィザードが完了すると、ユーザーアプリケーションカテゴリが作成されます。［**アプリケーションカテゴリ**］フォルダーの作業領域のカテゴリリストを使用して、新しく作成したカテゴリを確認できます。

イベントに関連する実行ファイルのアプリケーションカテゴリへの追加

手動で追加された内容を含む既存のアプリケーションカテゴリや新しいアプリケーションカテゴリに、［**アプリケーションの起動が禁止されました**］イベントと［**アプリケーションの起動がテストモードでブロックされています**］イベントを発生させた実行ファイルを追加できます。

アプリケーションコントロールイベントの対象となった実行ファイルをアプリケーションカテゴリに追加するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**イベント**］タブを選択します。
3. ［**イベント**］タブで、必要なイベントを選択します。
4. 選択したイベントのコンテキストメニューから［**カテゴリに追加**］を選択します。
5. 表示された［**イベントに関係する実行ファイルへの処理**］ウィンドウで、関連する設定を指定します：

   次のいずれかのオプションを選択します：

   - **新規アプリケーションカテゴリへ追加**

     新しいアプリケーションカテゴリを作成する場合は、このオプションをオンにします。

     ［OK］をクリックして新規カテゴリウィザードを実行します。ウィザードが完了すると、指定した設定でカテゴリが作成されます。

     既定では、このオプションはオフです。

   - **アプリケーションカテゴリへ追加**

     既存のアプリケーションカテゴリにルールを追加する場合は、このオプションをオンにします。アプリケーションカテゴリのリストから関連するカテゴリを選択します。

     既定ではこのオプションが選択されます。

   ［**ルール種別**］セクションで、次のいずれかを選択します：

   - **カテゴリに追加**

アプリケーションカテゴリの条件にルールを追加する場合は、このオプションをオンにします。

既定ではこのオプションが選択されます。

- **除外に追加する場合のルール**

  アプリケーションカテゴリの除外にルールを追加する場合は、このオプションを選択します。

［**ファイル情報種別**］セクションで、次のいずれかを選択します：

- **証明書の詳細情報（証明書がないファイルの場合 SHA256 ハッシュ）**

  ファイルが証明書によって署名されていることがあります。複数のファイルが同じ証明書で署名されていることがあります。たとえば、同じアプリケーションの異なるバージョンが同じ証明書で署名されていたり、同じ開発元の様々なアプリケーションが同じ証明書で署名されていたりすることがあります。証明書を選択した場合、アプリケーションの複数のバージョンまたは同じ開発元の複数のアプリケーションが同じカテゴリに属す場合があります。

  それぞれのファイルには固有の SHA256 ハッシュ関数があります。SHA256 ハッシュ関数を選択した場合、1つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

  実行ファイルの証明書の詳細（または証明書がないファイルの SHA256 ハッシュ機能）をカテゴリルールに追加する場合は、このオプションを選択します。

  既定では、このオプションがオンです。

- **証明書の詳細情報（証明書のないファイルはスキップ）**

  ファイルが証明書によって署名されていることがあります。複数のファイルが同じ証明書で署名されていることがあります。たとえば、同じアプリケーションの異なるバージョンが同じ証明書で署名されていたり、同じ開発元の様々なアプリケーションが同じ証明書で署名されていたりすることがあります。証明書を選択した場合、アプリケーションの複数のバージョンまたは同じ開発元の複数のアプリケーションが同じカテゴリに属す場合があります。

  実行ファイルの証明書の詳細をカテゴリルールに追加する場合は、このオプションを選択します。実行ファイルに証明書がない場合、そのファイルはスキップされます。このファイルに関する情報は、カテゴリに追加されません。

- **SHA256 のみ（ハッシュのないファイルはスキップ）**

  それぞれのファイルには固有の SHA256 ハッシュ関数があります。SHA256 ハッシュ関数を選択した場合、1つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

  実行ファイルの SHA256 ハッシュ機能の詳細だけを追加する場合、このオプションをオンにします。

- **MD5 のみ（非推奨、Kaspersky Endpoint Security 10 Service Pack 1 の場合のみ）**

それぞれのファイルには固有の MD5 ハッシュ関数があります。MD5 ハッシュ関数を選択した場合、1 つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

実行ファイルの MD5 ハッシュ機能の詳細だけを追加する場合、このオプションを選択します。Kaspersky Endpoint Security 10 Service Pack 1 for Windows およびそれ以前のすべてのバージョンで、MD5 ハッシュ機能の計算がサポートされています。

6. ［**OK**］をクリックします。

クライアントデバイスでのアプリケーション起動コントロールの設定

アプリケーションのカテゴリ化によって、デバイスで実行されるアプリケーションの管理を最適化できます。アプリケーションカテゴリを作成し、アプリケーションコントロールのポリシーを設定することで、指定のカテゴリのアプリケーションだけが、そのポリシーを適用したデバイスで起動されるようにすることができます。たとえば、*Application_1* と *Application_2* というアプリケーションを含むカテゴリを作成するとします。このカテゴリをポリシーに追加すると、*Application_1* と *Application_2* の 2 つのアプリケーションだけがポリシーの適用先デバイスで起動できます。そのカテゴリにない *Application_3* などのアプリケーションをユーザーが起動しようとすると、このアプリケーションの起動はブロックされます。アプリケーションコントロールルールに従って *Application_3* の開始がブロックされている旨の通知が表示されます。特定のフォルダーの様々な基準に基づいて自動でコンテンツが追加されるカテゴリを作成できます。その場合、指定のフォルダーのカテゴリにファイルが自動的に追加されます。アプリケーションの実行ファイルが指定のフォルダーにコピーされて自動的に処理され、そのメトリックがカテゴリに追加されます。

クライアントデバイスでのアプリケーション起動コントロールを設定するには：

1. コンソールツリーの［**詳細**］→［**アプリケーションの管理**］フォルダーで、［**アプリケーションカテゴリ**］サブフォルダーを選択します。

2. ［**アプリケーションカテゴリ**］フォルダーの作業領域で、起動を管理するアプリケーションのカテゴリを作成します。

3. Kaspersky Endpoint Security for Windows の新規ポリシーを作成するには、［**管理対象デバイス**］フォルダーの［**ポリシー**］タブで、［**新規ポリシー**］をクリックして、ウィザードの指示に従います。

   該当するポリシーが既に存在する場合は、この手順をスキップできます。このポリシーの設定により、指定されたカテゴリのアプリケーションの起動コントロールを設定できます。新しく作成したポリシーは、［**管理対象デバイス**］フォルダーの［**ポリシー**］タブに表示されます。

4. Kaspersky Endpoint Security for Windows ポリシーのコンテキストメニューから［**プロパティ**］を選択します。

   Kaspersky Endpoint Security for Windows ポリシーのプロパティウィンドウが表示されます。

5. Kaspersky Endpoint Security for Windows ポリシーのプロパティウィンドウで、［**セキュリティコントロール**］の［**アプリケーションコントロール**］セクションの［**アプリケーションコントロール**］をオンにします。

6. ［**追加**］をクリックします。

   ［**アプリケーションコントロールルール**］ウィンドウが表示されます。

7. ［**アプリケーションコントロールルール**］ウィンドウの［**カテゴリ**］から、起動ルールを適用するアプリケーションカテゴリを選択します。選択したアプリケーションカテゴリの起動ルールを設定します。

   実行ファイルの MD5 ハッシュ値の基準に基づいてアプリケーションカテゴリを作成した場合、Kaspersky Endpoint Security 10 Service Pack 2 以降ではカテゴリは表示されません。

Kaspersky Endpoint Security 10 Service Pack 2 より前のバージョンで、実行ファイルの SHA256 ハッシュ値の基準に従って作成したカテゴリは追加しないでください。追加すると、アプリケーションに障害が発生することがあります。

コントロールルールの設定方法の詳細は、Kaspersky Endpoint Security for Windows のオンラインヘルプを参照してください。

8. ［**OK**］をクリックします。

作成したルールに従って、指定されたカテゴリに属するアプリケーションがデバイスで実行されます。新しく作成したルールは Kaspersky Endpoint Security for Windows ポリシーのプロパティウィンドウにある［**アプリケーションコントロール**］セクションに表示されます。

実行ファイルに適用された起動ルールの静的分析結果の表示

ユーザーによる起動がブロックされている実行ファイルの情報を表示するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、［**ポリシー**］タブを選択します。
2. Kaspersky Endpoint Security for Windows ポリシーのコンテキストメニューから［**プロパティ**］を選択します。

   アプリケーションポリシーのプロパティウィンドウが表示されます。
3. ［**セクション**］ペインで［**セキュリティコントロール**］ - ［**アプリケーションコントロール**］の順に選択します。
4. ［**静的分析**］をクリックします。

   ［**アクセス権リストの分析**］ウィンドウが開きます。ウィンドウの左側に、Active Directory のデータに基づくユーザーリストが表示されます。
5. リストからユーザーを選択します。

   ウィンドウの右側に、選択したユーザーに割り当てられたアプリケーションのカテゴリが表示されます。
6. ユーザーが実行することを許可されていない実行ファイルを表示するには、［**アクセス権リストの分析**］ウィンドウで［**ファイルの表示**］をクリックします。

   ウィンドウが開き、ブロックされている実行ファイルのリストが表示されます。
7. カテゴリに含まれる実行ファイルのリストを表示するには、アプリケーションカテゴリを選択して［**カテゴリのファイルを表示**］をクリックします。

   ウィンドウが開き、アプリケーションカテゴリに含まれる実行ファイルのリストが表示されます。

アプリケーションレジストリの表示

Kaspersky Security Center は、管理対象デバイスにインストールされているすべてのソフトウェアのインベントリを作成します。

ネットワークエージェントが、Windows または Linux デバイスにインストールされているアプリケーションのリストを作成し、管理サーバーに送信します。Windows ベースのクライアントデバイスの場合、ネットワークエージェントは、インストールされているアプリケーションに関する大部分の情報を Windows レジストリから受け取ります。Linux ベースのクライアントデバイスの場合、パッケージマネージャーはインストールされているアプリケーションに関する情報をネットワークエージェントに提供します。

クライアントデバイスにインストールされているアプリケーションのレジストリを表示するには：

コンソールツリーの［**詳細**］フォルダーで、［**アプリケーションの管理**］フォルダーから［**アプリケーションレジストリ**］サブフォルダーを選択します。

クライアントデバイスと管理サーバーにインストールされているアプリケーションのリストが、［**アプリケーションレジストリ**］フォルダーの作業領域に表示されます。

任意のアプリケーションについて、コンテキストメニューを開いて［**プロパティ**］を選択することで、詳細情報を表示できます。アプリケーションのプロパティウィンドウに、アプリケーションに関する詳細情報、アプリケーションの実行ファイルに関する情報、アプリケーションがインストールされているデバイスのリストが表示されます。

すべてのアプリケーションのコンテキストメニューで次の操作を実行できます：

- 選択中のアプリケーションをアプリケーションカテゴリに追加する。
- アプリケーションにタグを割り当てる。
- アプリケーションのリストを CSV ファイルまたは TXT ファイルにエクスポートする。
- 製造元名、バージョン番号、実行ファイルのリスト、該当するアプリケーションがインストールされているデバイスのリスト、適用可能なソフトウェアアップデートのリスト、検出されたソフトウェア脆弱性のリストなど、アプリケーションの様々なプロパティを表示する。

指定された基準を満たすアプリケーションを表示するには、［**アプリケーションレジストリ**］フォルダーの作業領域にあるフィルターフィールドを使用できます。

選択したデバイスのプロパティウィンドウの［**アプリケーションレジストリ**］セクションで、デバイスにインストールされているアプリケーションのリストを表示できます。

インストール済みアプリケーションのレポートの生成

［**アプリケーションレジストリ**］作業領域で［**インストール済みアプリケーションのレポートの表示**］をクリックして、それぞれのアプリケーションがインストールされているデバイスの台数などのインストール済みアプリケーションに関する統計情報を含んだレポートを生成することもできます。**インストール済みアプリケーションのレポート**には、カスペルスキー製品とサードパーティ製品の両方の情報が含まれています。クライアントデバイスにインストールされているカスペルスキー製品のみの情報が必要な場合は、［**サマリー**］リストで「AO Kaspersky Lab」を選択します。

セカンダリ管理サーバーや仮想管理サーバーに接続しているデバイスにインストールされているカスペルスキー製品およびサードパーティソフトウェアの情報も、プライマリ管理サーバーのアプリケーションレジストリに保存されます。セカンダリ管理サーバーと仮想管理サーバーからのデータの追加が完了したら、［**インストール済みアプリケーションのレポートの表示**］をクリックして表示される**インストール済みアプリケーションのレポート**ページでこれらの情報を確認できます。

セカンダリ管理サーバーと仮想管理サーバーからの情報をインストール済みアプリケーションのレポートに加えるには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**レポート**］タブを選択します。
3. ［**レポート**］タブで、［**インストール済みアプリケーションのレポート**］を選択します。
4. レポートのコンテキストメニューから［**プロパティ**］を選択します。
   インストール済みアプリケーションのレポートのプロパティウィンドウが表示されます。
5. ［**管理サーバーの階層**］セクションで、［**セカンダリまたは仮想管理サーバーのデータを含める**］をオンにします。
6. ［OK］をクリックします。

セカンダリ管理サーバーおよび仮想管理サーバーからの情報が［**インストール済みアプリケーションのレポート**］に含められます。

ソフトウェアインベントリを開始するまでの時間の変更

Kaspersky Security Center は、Windows を実行している管理対象クライアントデバイスにインストールされているすべてのソフトウェアのインベントリを作成します。

ネットワークエージェントが、デバイスにインストールされているアプリケーションのリストを作成し、管理サーバーに送信します。ネットワークエージェントは、インストールされたアプリケーションに関する情報を Windows のレジストリから自動的に取得します。

デバイスのリソースを節約するため、既定ではネットワークエージェントサービスが起動してから 10 分後に、インストールされているアプリケーションの情報を取得し始めます。

デバイスでネットワークエージェントサービスが起動してからソフトウェアインベントリを開始するまでの時間を変更するには：

1. ネットワークエージェントがインストールされたデバイスのシステムレジストリを開きます（たとえば、ローカルで［**スタート**］→［**ファイル名を指定して実行**］で regedit コマンドを使用します）。
2. 次のレジストリエントリに移動します：
   - 32 ビットシステム：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - 64 ビットシステム：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF
3. KLINV_INV_COLLECTOR_START_DELAY_SEC キーで、値を秒単位で指定します。
   既定値は 600 秒です。
4. ネットワークエージェントサービスを再起動します。

ネットワークエージェントサービスが起動してからソフトウェアインベントリを開始するまでの時間が変更されます。

サードパーティ製品のライセンス管理について

Kaspersky Security Center では、管理対象デバイスにインストールされているサードパーティ製品のライセンス使用状況を追跡できます。ライセンス使用状況を追跡できるアプリケーションのリストは、アプリケーションレジストリから取得できます。ライセンスごとに、次の制限の中から対象を指定して違反を追跡できます：

- このライセンスを使用してアプリケーションをインストールできるデバイスの最大数
- ライセンスの有効期限

Kaspersky Security Center は、実際のライセンスを指定したかどうかを確認しません。指定した制限のみを追跡できます。ライセンスに設定した制限事項の1つに違反した場合、管理サーバーは、情報、警告、または機能エラーの各イベントを登録します。

ライセンスはアプリケーショングループにバインドされています。アプリケーショングループは、1つまたは複数の基準に基づいて組み合わせるサードパーティ製品のグループです。アプリケーションは、アプリケーションの名前、バージョン、ベンダー、タグで定義できます。少なくとも基準の1つが満たされた場合にアプリケーションがグループに追加されます。各アプリケーショングループに複数のライセンスをバインドできますが、各ライセンスは単一のアプリケーショングループにのみバインドできます。

ライセンス使用状況を追跡するために使用できるもう1つのツールは、ライセンス認証済みアプリケーショングループのステータスレポートです。このレポートでは、ライセンス認証済みアプリケーショングループの現在のステータスについての、次のような情報を確認できます：

- 各アプリケーショングループのライセンスのインストール数
- 使用中のライセンスと空き状態のライセンスの数
- 管理対象デバイスにインストールされているライセンス認証済みアプリケーションの詳細情報

サードパーティ製品のライセンス管理用ツールは、［**サードパーティのライセンスの使用**］サブフォルダー（［**詳細**］→［**アプリケーションの管理**］→［**サードパーティのライセンスの使用**］）にあります。このサブフォルダーでは、アプリケーショングループの作成、ライセンスの追加、およびライセンス認証済みアプリケーショングループのステータスに関するレポートの生成を行うことができます。

［Configure interface］ウィンドウで脆弱性とパッチ管理のオプションをオンにしている場合のみ、サードパーティ製品のアップデート用のライセンス管理ツールが使用できます。

ライセンス認証済みアプリケーショングループの作成

ライセンス認証済みアプリケーショングループを作成するには：

1. コンソールツリーの［**詳細**］→［**アプリケーションの管理**］フォルダーから［**サードパーティのライセンスの使用**］サブフォルダーを選択します。
2. ［**ライセンス認証済みアプリケーショングループの追加**］をクリックして、ライセンス認証済みアプリケーショングループの追加ウィザードを実行します。

   ライセンス認証済みアプリケーショングループの追加ウィザードが開始します。
3. **ライセンス認証済みアプリケーショングループに関する詳細情報**ステップでは、アプリケーショングループに含めるアプリケーションを指定します：

- **ライセンス認証済みアプリケーショングループの名前**
- **制限違反を追跡する**

  アプリケーショングループのライセンスに設定する制限の1つに違反すると、管理サーバーは情報、警告、または機能エラーのイベントを登録します。

  - 情報イベント：**インストール数が上限に近づいている（95% を超える数を使用済み）ライセンス認証済みアプリケーショングループがあります**
  - 警告イベント：**インストール数が上限に近づいているライセンス認証済みアプリケーショングループがあります**
  - 機能エラーイベント：**インストール数の上限を超えたライセンス認証済みアプリケーショングループがあります**

    イベントは、指定された条件が満たされた時に1回だけ登録されます。次回は、インストール数が正常レベルに戻って、再度イベントが発生した場合にのみ、同じイベントを登録できます。イベントは1時間に複数回登録できません。

- **検出されたアプリケーションをこのライセンス認証済みアプリケーショングループに追加する基準**

  アプリケーショングループに含めるアプリケーションを定義する基準を指定します。アプリケーションは、アプリケーションの名前、バージョン、ベンダー、タグで定義できます。少なくとも1つの基準を指定する必要があります。少なくとも基準の1つが満たされた場合にアプリケーションがグループに追加されます。

4. **既存のライセンスに関するデータを入力します**ステップで、追跡するライセンスを指定します。［**ライセンス数の上限を管理する**］をオンにして、ライセンスを追加します：

   a. ［**追加**］をクリックします。

   b. 追加するライセンスを選択し、［**OK**］をクリックします。必要なライセンスがリストにない場合は、［**追加**］をクリックして、ライセンスのプロパティを指定します。

5. ［**ライセンス認証済みアプリケーショングループの追加**］ステップで、［**終了**］をクリックします。

ライセンス認証済みアプリケーショングループが作成され、［**サードパーティのライセンスの使用**］フォルダーに表示されます。

ライセンス認証済みアプリケーショングループのライセンスの管理

ライセンス認証済みアプリケーショングループのライセンス情報を作成するには：

1. コンソールツリーの［**詳細**］→［**アプリケーションの管理**］フォルダーから［**サードパーティのライセンスの使用**］サブフォルダーを選択します。
2. ワークスペースの［**サードパーティのライセンスの使用**］フォルダーで、［**認証済みアプリケーションのライセンス管理**］をクリックします。

   ［**ライセンス認証済みアプリケーションのライセンス管理**］ウィンドウが表示されます。
3. ［**ライセンス認証済みアプリケーションのライセンス管理**］ウィンドウで、［**追加**］をクリックします。

［**ライセンス**］ウィンドウが開きます。

4. ［**ライセンス**］ウィンドウで、ライセンスのプロパティと、そのライセンスによってライセンス認証済みアプリケーショングループに適用される制限を設定します。

   - **名前**：ライセンスの名前。
   - **コメント**：選択されたライセンスに関する注記。
   - **制限**：このライセンスを使用してアプリケーションをインストールできるデバイスの台数。
   - **有効期限**：ライセンスの有効期限。

   作成されたライセンスが［**ライセンス認証済みアプリケーションのライセンス管理**］ウィンドウに表示されます。

ライセンス認証済みアプリケーショングループにライセンスを適用するには：

1. コンソールツリーの［**詳細**］→［**アプリケーションの管理**］フォルダーから［**サードパーティのライセンスの使用**］サブフォルダーを選択します。
2. ［**サードパーティのライセンスの使用**］フォルダーで、ライセンスを適用するライセンス認証済みアプリケーショングループを選択します。
3. ライセンス認証済みアプリケーショングループのコンテキストメニューから［**プロパティ**］を選択します。

   ライセンス認証済みアプリケーショングループのプロパティウィンドウが表示されます。
4. ライセンス認証済みアプリケーショングループのプロパティウィンドウにある［**ライセンス**］セクションで［**ライセンス数の上限を管理する**］を選択します。
5. ［**追加**］をクリックします。

   ［**ライセンスの選択**］ウィンドウが表示されます。
6. ［**ライセンスの選択**］ウィンドウで、ライセンス認証済みアプリケーショングループに適用するライセンスを選択します。
7. ［**OK**］をクリックします。

   ライセンス認証済みアプリケーショングループに対してライセンスで指定された制限が、選択したライセンス認証済みアプリケーショングループにも適用されます。

実行ファイルのインベントリ

管理対象デバイス上に保管された実行ファイルのリストを取得できます。実行ファイルのインベントリを実行するには、インベントリタスクを作成する必要があります。

実行ファイルのインベントリ機能は、次のアプリケーションで使用できます：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

- Kaspersky Security for Virtualization 4.0 Light Agent 以降のバージョン

1 台のデバイスから受信できる実行ファイルは、最大で 150,000 個です。この上限に達した場合、Kaspersky Security Center は新規ファイルを取得できません。

開始する前に、管理サーバーにデータを転送するため、Kaspersky Endpoint Security のポリシーとネットワークエージェントのポリシーでアプリケーションの開始に関する通知を有効にしてください。

アプリケーションの開始に関する通知を有効にするには：

- Kaspersky Endpoint Security のポリシー設定を開き、次の操作を実行してください：
  1. ［**全般設定**］→［**レポートと保管領域**］の順に選択します。
  2. ［**管理サーバーへのデータ転送**］で、［**起動されたアプリケーションの情報**］をオンにします。
  3. 変更を保存します。
- ネットワークエージェントのポリシー設定を開き、次の操作を実行します：
  1. ［**リポジトリ**］セクションに移動します。
  2. ［**インストール済みアプリケーションの詳細**］をオンにします。
  3. 変更を保存します。

クライアントデバイス上の実行ファイルのインベントリタスクを作成するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. ［**タスク**］フォルダーの作業領域の［**新規タスク**］をクリックします。
   新規タスクウィザードが起動します。
3. ウィザードの［**タスク種別の選択**］ウィンドウで、タスク種別として［**Kaspersky Endpoint Security**］を選択し、タスクサブタイプとして［**インベントリ**］を選択して［**次へ**］をクリックします。
4. 引き続きウィザードの指示に従って操作します。

   ウィザードが終了したら、Kaspersky Endpoint Security のインベントリタスクが作成されます。新規作成されたタスクが、［**タスク**］フォルダーの作業領域のタスクのリストに表示されます。

デバイスのインベントリで検出された実行ファイルのリストは、［**実行ファイル**］フォルダーの作業領域に表示されます。

インベントリでは、以下の形式の実行ファイルが検出されます：MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR、HTML ファイル。

実行ファイルに関する情報の表示

クライアントデバイスで検出されたすべての実行ファイルのリストを表示するには：

コンソールツリーの［**アプリケーションの管理**］フォルダーで、［**実行ファイル**Application management］フォルダーから［Application categories］サブフォルダーを選択します。

［**実行ファイル**］フォルダーの作業領域には、デバイスで実行された実行ファイルと、Kaspersky Endpoint Security for Windows のインベントリタスクの実行中に検出された実行ファイルのリストが表示されます。

指定した基準を満たす実行ファイルのデータを表示するには、フィルタリングを使用できます。

実行ファイルのプロパティを表示するには：

ファイルのコンテキストメニューから［**プロパティ**］を選択します。

実行ファイルに関する情報とともに、その実行ファイルが検出されたデバイスのリストが別ウィンドウに表示されます。

監視とレポート

このセクションでは Kaspersky Security Center の監視機能とレポート機能について説明しています。これらの機能を使用して、インフラストラクチャの状況、保護ステータス、統計情報を確認できます。

Kaspersky Security Center の導入後または運用中に、必要に応じて監視とレポート機能の設定を最適な状態に編集できます。

- **ステータス信号**

  管理コンソールでは、ステータス信号を確認することで、Kaspersky Security Center と管理対象デバイスの現在のステータスをすぐに参照できます。

- **統計**

  保護システムと管理対象デバイスのステータスの統計は、カスタマイズ可能な情報パネルに表示されます。

- **レポート**

  レポート機能を使用することで、組織ネットワークのセキュリティに関する詳細な数値データを取得し、これらの情報をファイルに保存したり、メールで送信したり、印刷することができます。

- **イベント**

  イベントの抽出は、管理サーバーのデータベース内に保存されているイベントを一定の条件を指定して抽出し、画面上に表示できる機能です。これらのイベントは、次のカテゴリに従ってグループ化されます：

  - 重要度：**緊急イベント**、**機能エラー**、**警告**、**情報イベント**
  - 発生時期：**最近のイベント**
  - 種別：**ユーザー要求**、**監査イベント**

また、Kaspersky Security Center Web コンソールで編集可能な設定を使用して、ユーザー定義のイベントの抽出を作成し表示できます。

シナリオ：監視とレポート

このセクションでは、Kaspersky Security Center の監視機能とレポート機能を設定する手順を説明しています。

必須条件

組織のネットワークへの Kaspersky Security Center の導入後、監視を開始し、動作状況のレポートを生成できます。

実行するステップ

組織のネットワークにおける監視の実施とレポートの利用は、以下の手順で進みます：

1. **デバイスのステータスの切り替えの設定**

   特定の条件に応じて、デバイスのステータスの割り当てを定義した設定を確認します。各種設定を変更することで、重要度レベルが「*緊急*」または「*警告*」のイベントの数を変えることができます。

   デバイスのステータスの切り替えの設定中、新しい設定が組織の情報セキュリティポリシーと矛盾していないこと、組織のネットワークにおける重要なセキュリティイベントに迅速に対応できることを確認してください。

2. **クライアントデバイスで発生したイベントに関する通知の設定**

   組織の要件に応じて、クライアントのデバイス上でイベントの通知（メール、SMS、ファイルの実行）を設定します。

3. **ウイルスアウトブレイクイベントについてのセキュリティネットワーク対応の変更**

   新しいイベントに対するネットワーク対応を調整するには、管理サーバーで個別のしきい値を変更します。イベント発生時に有効になる基準のより厳しいポリシーを作成したり、イベント発生時に実行されるタスクを作成できます。

4. **統計情報の管理**

   組織の要件に応じて、統計の表示を設定します。

5. **組織のネットワークのセキュリティステータスの確認**

   組織のネットワークのセキュリティステータスを確認するには、次の操作を実行します：

   - ［**管理サーバー**］フォルダーのワークスペースの［**統計**］タブで、下位の［**保護ステータス**］タブ（ページ）を開き、［**リアルタイム保護のステータス**］情報パネルを確認する
   - **［保護ステータスレポート］**を生成し確認する
   - **［エラーに関するレポート］**を生成し確認する

6. **保護されていないクライアントデバイスの検出**

   保護されていないクライアントデバイスを検出するには、［**管理サーバー**］フォルダーのワークスペースの［**統計**］タブで、下位の［**保護ステータス**］タブ（ページ）を開き、［**ネットワーク上の新しいデバイスの検出履歴**］情報パネルを確認します。または**［製品導入レポート］**を生成し確認することもできます。

7. **クライアントデバイスの保護状態の確認**

   クライアントデバイスの保護状態を確認するには、［**管理サーバー**］フォルダーのワークスペースの［**統計**］タブで、下位の［**製品の導入**］または［**脅威の統計**］タブ（ページ）を開き、関連する情報パネルを確認します。または**［緊急イベント］**イベントの抽出を開始して確認することもできます。

8. **データベースでのイベント情報による負荷の評価と制限**

管理対象アプリケーションの動作中に発生したイベントに関する情報は、クライアントデバイスから送信され、管理サーバーデータベースに記録されます。管理サーバーの負荷を軽減するには、データベースに保管される可能性のあるイベント数の最大値を評価し、上限を設定します。

データベースのイベント負荷を評価するには、データベースの容量を計算します。データベースのオーバーフローを回避するため、イベントの最大数を制限することもできます。

9 ライセンス情報の確認

ライセンス情報を確認するには、［**管理サーバー**］フォルダーのワークスペースの［**統計**］タブで、下位の［**製品の導入**］タブ（ページ）を開き、［**ライセンス使用状況**］情報パネルを確認します。または［**ライセンス使用レポート**］生成し確認することもできます。

結果

これらの手順が完了すると、組織のネットワークの保護に関する情報を確認できるようになり、今後のセキュリティ対策の計画や脅威への対応に役立てることができます。

管理コンソールでステータス信号およびログに記録されたイベントを監視する

管理コンソールでは、ステータス信号を確認することで、Kaspersky Security Center と管理対象デバイスの現在のステータスをすぐに参照できます。ステータス信号は、［**管理サーバー**］フォルダーの作業領域の［**監視**］タブに表示されます。このタブには、ステータス信号が表示された 6 つの情報パネルおよびログされたイベントがあります。ステータス信号とは、パネルの左側に表示される色付きの縦線です。ステータス信号が表示された各パネルは、Kaspersky Security Center の特定の機能範囲に対応しています（以下の表を参照）。

管理コンソールのステータス信号の対象範囲

パネル名	ステータス信号の範囲
製品の導入	組織ネットワーク内のデバイスへのネットワークエージェントとセキュリティ製品のインストール
管理スキーム	管理グループの構造。ネットワークのスキャン。デバイス移動ルール
プロテクション設定	セキュリティ製品の機能：保護ステータス、マルウェアスキャン
アップデート	アップデートとパッチ
監視	保護ステータス
管理サーバー	管理サーバーの機能とプロパティ

各ステータス信号は、以下の 5 色で表されます（下表を参照）。ステータス信号の色は、Kaspersky Security Center の現在のステータスと、記録されたイベントに基づきます。

ステータス信号の色コード

ステータス	ステータス信号の色	ステータス信号の色の意味
情報	緑	管理者の介入は必要ありません
警告	黄	管理者の介入が必要です。
緊急	赤	重大な問題が発生しました。問題を解決するには、管理者の介入が必要です。
情報	水色	管理対象デバイスのセキュリティに対する潜在的脅威または実際の脅威とは無関係のイベントが記録されました
情報	灰色	イベントの詳細が不明であるか、まだ取得されていません

［**監視**］タブのすべての情報パネルのステータス信号の色を緑にすることが、管理者の目標となります。

情報パネルには、ステータス信号と Kaspersky Security Center のステータスに影響するログに記録されたイベントも表示されます（下の表を参照）。

ログに記録されたイベントの名前、説明、およびステータス信号の色

ステータス信号の色	イベント種別の表示名	イベント種別	説明
赤	**%1 台のデバイスでライセンスの有効期間が終了しました**	IDS_AK_STATUS_LIC_EXPAIRED	この種別のイベントは、製品版ライセンスの有効期間が終了する時に発生します。 Kaspersky Security Center は 1 日 1 回、デバイスでライセンスの有効期限が切れているかどうかを確認します。 製品版ライセンスの有効期間が終了した場合は、Kaspersky Security Center は基本機能のみを提供します。 Kaspersky Security Center の使用を継続するには、製品版ライセンスを更新してください。
赤	**セキュリティによる保護が実行されていません：%1 台のデバイス**	IDS_AK_STATUS_AV_NOT_RUNNING	このタイプのイベントは、デバイスにインストールされているセキュリティ製品が実行されていない時に発生します。 Kaspersky Endpoint Security がデバイスで実行されていることを確認します。
赤	**プロテクションが無効になっています：%1 台のデバイス**	IDS_AK_STATUS_RTP_NOT_RUNNING	このタイプのイベントは、デバイス上のセキュリティ製品が指定された時間間隔より長く無効になっている場合に発生します。 デバイスのリアルタイム保護の現在のステータスを確認し、必要なすべての保護コンポーネントが有効になっていることを確認します。
赤	**デバイスでソフトウェアの脆弱性が検知されました**	IDS_AK_STATUS_VULNERABILITIES_FOUND	このタイプのイベントは、*脆弱性とアプリケーションのアップデートの検索*タスクが、デバイスにインストールされているアプリケーションで指定された深刻度の脆弱性を検知した時に発生します。 ［**アプリケーションの管理**］フォルダーの［**ソフトウェアのアップデート**］サブフォルダーで、適用可能なアップデートのリストをオンにします。このフォルダーには、管理サーバーが取得した、デバイスへ配信可能な Microsoft アプリケーションやその他のソフトウェア会社の製品のアップデートのリストが含まれます。 適用可能なアップデートの情報を確認した後、アップデートをデバイスにインストールできます。
赤	**緊急イベントが管理サーバーに登録されました**	IDS_AK_STATUS_EVENTS_OCCURED	このタイプのイベントは、管理サーバーの緊急イベントが検知された時に発生します。 管理サーバーに保存されているイベントのリストを確認し、緊急イベントを 1 つずつ修正します。
赤	**エラーが管理サーバーのイベントに登録されました**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	このタイプのイベントは、管理サーバー側で予期しないエラーが記録された時に発生します。 管理サーバーに保存されているイベントのリストを確認し、エラーを 1 つずつ修正します。
赤	**%1 台のデバイスとの接続が切断されました**	IDS_AK_STATUS_ADM_LOST_CONTROL1	このタイプのイベントは、管理サーバーとデバイス間の接続が失われた時に発生します。 切断されたデバイスのリストを表示し、それらを再接続してみてください。
赤	**%1 台のデバイスが管理サーバーに長期間接続されていません**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	このタイプのイベントは、デバイスの電源がオフになっているために、指定された時間内にデバイスが管理サーバーに接続されなかった場合に発生します。 デバイスの電源が入っていて、ネットワークエージェントが実行されていることを確認してください。
赤	**%1 台のデバイスが「OK」以外のステータスです**	IDS_AK_STATUS_HOST_NOT_OK	このタイプのイベントは、管理サーバーに接続されているデバイスの［*OK*］ステータスが［*緊急*］または［*警告*］に変化した時に発生します。

			Kaspersky Security Center のリモート診断ユーティリティを使用して、問題をトラブルシューティングできます。
赤	**定義データベースがアップデートされていません：%1 台のデバイス**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	このタイプのイベントは、定義データベースが指定された時間内にデバイスで更新されなかった場合に発生します。 指示に従って Kaspersky 定義データベースをアップデートします。
赤	**Windows Update 更新プログラムのチェックが長期間実行されていないデバイス：%1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	このタイプのイベントは、*Windows Update の同期の実行*タスクが指定された時間間隔内に実行されなかった時に発生します。 指示に従って、Windows Update の更新プログラムと管理サーバーとの同期を行います。
赤	**Kaspersky Security Center 用の %1 個のプラグインをインストールする必要があります**	IDS_AK_STATUS_PLUGINS_REQUIRED2	このタイプのイベントは、カスペルスキー製品用の追加のプラグインをインストールする必要がある時に発生します。 カスペルスキーのテクニカルサポートの Web ページから、カスペルスキー製品に必要な管理プラグインをダウンロードしてインストールします。

レポート、統計情報、通知の使用

このセクションでは、Kaspersky Security Center でレポート、統計情報、イベントとデバイスの抽出を扱う方法と、管理サーバー通知を設定する方法を説明します。

レポートの使用

Kaspersky Security Center のレポートには、管理対象デバイスのステータスに関する情報が含まれています。レポートは管理サーバーに保存されている情報に基づいて生成されます。次の種類のオブジェクトについて、レポートを作成できます：

- 特定の設定に基づいて作成されたデバイスの抽出
- 管理グループ
- 様々な管理グループに存在する特定のデバイス
- ネットワーク上のすべてのデバイス（導入レポート内に表示）

アプリケーションには、標準レポートテンプレートの抽出があります。カスタムレポートテンプレートを作成することも可能です。レポートはメインウィンドウのコンソールツリーにある［**管理サーバー**］フォルダーに表示されます。

レポートテンプレートの作成

レポートテンプレートを作成するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**レポート**］タブを選択します。
3. ［**新規レポートテンプレート**］をクリックします。

新規レポートテンプレートウィザードが起動します。ウィザードの指示に従ってください。

ウィザードの処理が完了すると、新しく作成されたレポートテンプレートがコンソールツリーで選択した［**管理サーバー**］フォルダーに追加されます。このテンプレートを使用して、レポートの作成と表示ができます。

レポートテンプレートのプロパティの表示と編集

レポートテンプレートについて、レポートテンプレートの名前やレポートに表示されるフィールドなどの基本的なプロパティを表示し、編集できます。

レポートテンプレートのプロパティを表示したり編集するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**レポート**］タブを選択します。
3. レポートテンプレートのリストから、目的のレポートテンプレートを選択します。
4. 選択したレポートテンプレートのコンテキストメニューから［**プロパティ**］を選択します。

   または、まずレポートを生成して、次に［**レポートテンプレートのプロパティを開く**］または［**レポート列の設定**］のいずれかをクリックします。
5. 開いたウィンドウで、レポートテンプレートのプロパティを編集します。各レポートのプロパティには、下記のセクションの一部しか含まれない場合があります。

   - ［**全般**］セクション
     - レポートテンプレート名
     - **表示する項目数の上限**

       このオプションをオンにすると、詳細なレポートデータの表に表示されるエントリ数に、指定した上限値が設定されます。

       レポートのエントリは、レポートテンプレートの［**フィールド**］→［**詳細フィールド**］セクションで指定したルールに従って並べ替えられ、合致するエントリのうち表示順が上のエントリだけが維持されます。詳細レポートのタイトルには、レポートテンプレートで設定したその他の条件に合致するエントリの合計数と表示されている数が表示されます。

       このオプションをオフにすると、詳細なレポートデータの表にはすべての使用可能なエントリが表示されますこのオプションをオフにすることは推奨されません。表示されるレポートエントリの数を制限することにより、DBMS（データベース管理システム）の負荷を減らし、レポートの生成とエクスポートの所要時間を削減できます。一部のレポートではエントリ数が多すぎる場合があります。このような場合、すべてのエントリに目を通し分析することは困難です。また、こうしたレポートの生成中にデバイスのメモリ不足が発生し、レポート自体を表示できない可能性もあります。

       既定では、このオプションはオンです。既定値は 1000 です。

     - **印刷用レイアウトで出力**

       レポートの出力が印刷用に最適化され、読みやすさを考慮して一部の値の間に空白文字が追加されます。

       既定では、このオプションはオンです。

- ［**フィールド**］セクション

  レポートで表示されるフィールド、フィールドの順序を選択し、各フィールドに基づいて情報の並べ替えとフィルター処理を行うかを設定します。

- ［**時間**］セクション

  レポートの対象期間を変更します。次の値を設定できます：

  - 指定した 2 つの日付の間の期間
  - 指定日からレポート作成日までの期間
  - レポート作成日から指定した日数だけ過去にさかのぼった期間

- ［**グループ**］セクション、［**デバイスの抽出**］セクション、［**デバイス**］セクション

  レポートの作成対象にするクライアントデバイスを変更します。レポートテンプレートの作成時に指定した設定に応じて、上記のいずれかのセクションのみが表示されます。

- ［**設定**］セクション

  レポートの設定を変更します。どのような設定項目が存在するかは、レポートごとに異なります。

- ［**セキュリティ**］セクション**管理サーバーから設定を継承する**

  このオプションがオンの場合、レポートのセキュリティ設定は管理サーバーから継承します。

  このオプションがオフの場合、レポートのセキュリティ設定を編集できます。レポートを適用対象に、ロールをユーザーまたはユーザーのグループに割り当てたり、権限をユーザーまたはユーザーのグループに割り当てることができます。

  既定では、このオプションはオンです。

  インターフェイスの設定ウィンドウで［**セキュリティ設定タブの表示**］をオンにすると、［**セキュリティ**］セクションが使用できます。

- ［**管理サーバーの階層**］セクション

  - **セカンダリまたは仮想管理サーバーのデータを含める**

    このオプションをオンにすると、レポートテンプレートを作成する管理サーバーに属するセカンダリ管理サーバーおよび仮想管理サーバーからの情報をレポートに含めます。

    現在の管理サーバーのデータのみを表示する場合は、このオプションをオフにします。

    既定では、このオプションはオンです。

  - **ネスト数の上限**

    対象の管理サーバーに属するセカンダリ管理サーバーおよび仮想管理サーバーのうち、指定したネスト数以内のサーバーのデータをレポートに含めます。

    既定値は 1 です。ツリー内でより下位に位置するセカンダリ管理サーバーの情報を取得する必要がある場合、この値を変更することができます。

  - **データの待機時間（分）**

レポートを生成する前に、レポートテンプレートを作成する管理サーバーは、セカンダリ管理サーバーからデータが送信されるのを、指定した分数だけ待機します。指定した時間が経過してもセカンダリ管理サーバーからデータを取得できなかった場合は、これらのデータを除外してレポートが実行されます。［**セカンダリ管理サーバーのデータをキャッシュする**］を有効にすると、実際のデータの代わりにキャッシュデータがレポートに表示されます。無効にすると、［**該当なし**］と表示されます。

既定値は 5 分です。

- **セカンダリ管理サーバーのデータをキャッシュする**

  セカンダリ管理サーバーからレポートテンプレートを作成する管理サーバーに定期的にデータが送信されます。送信されたデータはキャッシュに保存されます。

  レポートの生成時に現在の管理サーバーがセカンダリ管理サーバーからデータを取得できなかった場合、キャッシュから取得したデータがレポートに表示されます。データがキャッシュに送信された日付も合わせて表示されます。

  このオプションをオンにすると、最新のデータを取得できなかった場合でもセカンダリ管理サーバーの情報を表示できます。ただし、表示されるデータが最新のものではない場合があります。

  既定では、このオプションはオフです。

- **キャッシュの更新頻度（時間）**

  セカンダリ管理サーバーからレポートテンプレートを作成する管理サーバーに定期的にデータが送信されます。この期間は時間単位で指定できます。0 時間を指定すると、レポートの生成時にのみデータが送信されます。

  既定値は 0 です。

- **セカンダリ管理サーバーから詳細情報を転送する**

  生成されたレポートの詳細なレポートデータの表に、レポートテンプレートを作成する管理サーバーのセカンダリ管理サーバーから取得したデータを含めます。

  このオプションをオンにすると、レポートの生成にかかる時間が長くなり、管理サーバー間のトラフィックも増大します。ただし、1つのレポートですべてのデータを表示できるメリットもあります。

  このオプションをオンにする他に、先に詳細なレポートデータを分析してエラーが発生しているセカンダリ管理サーバーを特定した上で、エラーが発生している管理サーバーのみを対象にレポートを生成するという方法も活用できます。

  既定では、このオプションはオフです。

レポートテンプレートでの高度なフィルター形式の使用

Kaspersky Security Center 15.1 では、レポートテンプレートに高度なフィルター形式を適用できます。高度なフィルター形式は、デフォルトのフィルター形式と比べて、より柔軟にフィルターを使用できます。複数のフィルターを組み合わせることで複雑な絞り込み条件を作成し、次のように論理演算子の「AND」だけでなく「OR」を使用して、レポートのデータに条件を適用できます。

Filter[1](Field[1] AND Field[2]...AND Field[n]) OR Filter[2](Field[1] AND Field[2]...AND Field[n]) OR...Filter[n](Field[1] AND Field[2]...AND Field[n])

さらに、高度なフィルター形式を使用することで、フィルター内の特定のフィールドで相対時間を使用して対象期間の値を指定できます（「過去 N 日間」など）。対象期間の指定時に相対時間を使用できるかどうかと、どのような値を指定できるかはレポートテンプレートの種別に応じて異なります。

フィルターの高度なフィルター形式への変換

レポートテンプレートの高度なフィルター形式は、Kaspersky Security Center 12 以降のバージョンでのみサポートされます。既定のフィルターを高度なフィルター形式に変換すると、レポートテンプレートはネットワーク上で古いバージョンの Kaspersky Security Center がインストールされている管理サーバーとの互換性がなくなります。これらの古いバージョンの管理サーバーからの情報は、高度なフィルター形式を使用するレポートに反映されません。

レポートテンプレートの既定のフィルターを高度なフィルター形式に変換するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**レポート**］タブを選択します。
3. レポートテンプレートのリストから、目的のレポートテンプレートを選択します。
4. 選択したレポートテンプレートのコンテキストメニューから［**プロパティ**］を選択します。
5. プロパティウィンドウが開いたら、［**フィールド**］セクションを選択します。
6. ［**詳細フィールド**］タブで、［**フィルターの変換**］をクリックします。
7. ウィンドウが表示されたら、［OK］をクリックします。

   高度なフィルター形式への変換を行ったレポートテンプレートで、この処理を元に戻すことはできません。［**フィルターの変換**］を誤ってクリックした場合、レポートテンプレートのプロパティウィンドウで［**キャンセル**］をクリックして、変換処理を実行しないようにしてください。

8. 変更を適用するには、［OK］をクリックしてレポートテンプレートのプロパティウィンドウを閉じます。

   レポートテンプレートのプロパティウィンドウをもう一度開くと、新たに［**フィルター**］セクションが表示されるようになります。このセクションで、高度なフィルターを設定できます。

高度なフィルターの設定

レポートテンプレートのプロパティで、高度なフィルターを設定するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**レポート**］タブを選択します。
3. レポートテンプレートのリストから、高度なフィルター形式への変換を既に実行しているレポートテンプレートを選択します。
4. 選択したレポートテンプレートのコンテキストメニューから［**プロパティ**］を選択します。
5. プロパティウィンドウが開いたら、［**フィルター**］セクションを選択します。

   該当するレポートテンプレートで高度なフィルター形式への変換を実行していない場合、［**フィルター**］セクションは表示されません。

レポートテンプレートのプロパティウィンドウの［**フィルター**］セクションで、レポートに適用されているフィルターのリストの確認と編集を行えます。リスト内のフィルターはそれぞれ一意の名前を持ち、レポートの対応するフィールドに対して適用する条件によって構成されます。

6. 次のいずれかの方法で、フィルターの設定ウィンドウを開きます：

   - 新しいフィルターを作成するには、［**追加**］をクリックします。
   - 既存のフィルターを編集するには、目的のフィルターを選択し、［**変更**］をクリックします。

7. 表示されるウィンドウで、フィルターの目的のフィールドを選択して値を指定します。

8. ［**OK**］をクリックし、変更内容を保存してウィンドウを閉じます。

   新しいフィルターを作成している場合、［**OK**］をクリックする前に、［**フィルター名**］でフィルターの名前を指定する必要があります。

9. ［**OK**］をクリックしてレポートテンプレートのプロパティウィンドウを閉じます。

   レポートテンプレートで高度なフィルターが設定されます。このレポートテンプレートを使用してレポートを作成できます。

レポートの作成と表示

レポートを作成および表示するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**レポート**］タブを選択します。
3. レポートテンプレートのリストから、目的のレポートテンプレートをダブルクリックします。

   選択したテンプレートのレポートが表示されます。

レポートには次のデータが表示されます：

- レポート名とレポート種別、概要説明、レポート期間、レポートが作成されたデバイスグループに関する情報。
- 代表的なレポートのデータを示している図表。
- 計算されたレポートの指標を含む表。
- 詳細なレポートデータの表。

レポートの保存

作成したレポートを保存するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**レポート**］タブを選択します。
3. レポートテンプレートのリストから、目的のレポートテンプレートを選択します。

4. 選択したレポートテンプレートのコンテキストメニューから［**保存**］を選択します。

   レポート保存ウィザードが起動します。ウィザードの指示に従ってください。

ウィザードが完了すると、レポートファイルを保存したフォルダーが開きます。

レポートを XLS ファイルとして保存すると、ロゴやデータグラムなどのすべての関連画像が個別のファイルとして保存されます。

レポート配信タスクの作成

レポートはメールで送信できます。Kaspersky Security Center は、レポート配信タスクを使用してレポートを配信します。

単一のレポートの配信タスクを作成するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**レポート**］タブを選択します。
3. レポートテンプレートのリストから、目的のレポートテンプレートを選択します。
4. 選択したレポートテンプレートのコンテキストメニューから［**レポートの配信**］を選択します。

   レポート配信タスク作成ウィザードが起動します。ウィザードの指示に従ってください。

複数のレポートの配信タスクを作成するには：

1. コンソールツリーの、目的の管理サーバーの名前の付いたフォルダーで、［**タスク**］フォルダーを選択します。
2. ［**タスク**］フォルダーの作業領域で［**タスクの作成**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

   新たに作成されたレポート配信タスクは、コンソールツリーの［**タスク**］フォルダーに表示されます。

Kaspersky Security Center のインストール時にメール設定を指定した場合、レポート配信タスクが自動的に作成されます。

ステップ 1：タスク種別の選択

［**タスク種別の選択**］ウィンドウで、タスクのリストから［**レポートの配信**］を選択します。

［**次へ**］をクリックして次のステップに進みます。

ステップ 2：レポートテンプレートの種別の選択

［**レポート種別の選択**］ウィドウのタスク作成テンプレートのリストで、レポートの種別を選択します。

［**次へ**］をクリックして次のステップに進みます。

ステップ 3：レポートでの操作

［**レポートに適用する処理**］ウィンドウで、次の設定を指定します：

- **レポートをメールで送信する**

  このオプションをオンにすると、生成されたレポートがアプリケーションからメールで送信されます。

  ［**メール通知の設定**］をクリックすると、メールによるレポート送信を設定できます。このリンクは、チェックボックスをオンにすると使用可能になります。

  このオプションをオフにすると、アプリケーションは指定されたフォルダーにレポートを保存します。

  既定では、このオプションはオフです。

- **レポートを共有フォルダーに保存する**

  このオプションをオンにすると、アプリケーションはチェックボックスの下のフィールドで指定したフォルダーにレポートを保存します。レポートを共有フォルダーに保存するには、フォルダーの UNC パスを指定します。この場合、［**タスクを実行するアカウントの選択**］ウィンドウで、共有フォルダーへのアクセスに使用するユーザーアカウントとパスワードを指定する必要があります。

  このオプションをオフにすると、アプリケーションはフォルダーにレポートを保存せず、代わりにメールで配信します。

  既定では、このオプションはオフです。

- **同じ種別の古いレポートを上書きする**

  このオプションをオンにすると、各タスクの起動時に生成されるレポートが、レポートのフォルダーに保存された前回の起動時のレポートファイルを上書きします。

  このオプションをオフにすると、レポートファイルは上書きされません。各タスクの実行時に、新しいレポートファイルがレポートフォルダーに保存されます。

  このチェックボックスは、［**レポートをフォルダーに保管する**］をオンにすると使用可能になります。

  既定では、このオプションはオフです。

- **共有フォルダーにアクセスするアカウントを指定する**

  このオプションをオンにすると、レポートが保存されるフォルダーのアカウントを指定できます。［**レポートに適用する処理**］ウィンドウの［**レポートをフォルダーに保存する**］設定で共有フォルダーへの UNC パスを指定する場合、そのフォルダーにアクセスするためのユーザーアカウントとパスワードを指定する必要があります。

  このオプションをオフにすると、レポートは管理サーバーのアカウント以下のフォルダーに保存されます。

  このチェックボックスは、［**レポートをフォルダーに保管する**］をオンにすると使用可能になります。

  既定では、このオプションはオフです。

レポートを XLS ファイルとして保存または送信すると、ロゴやデータグラムなどのすべての関連画像が個別のファイルとして保存されます。

［**次へ**］をクリックして次のステップに進みます。

ステップ 4：タスクを開始するアカウントの選択

［**タスクを実行するアカウントの選択**］ウィンドウで、タスクの実行時に使用するアカウントを指定できます。次のいずれかのオプションをオンにします：

- **既定のアカウント**

  タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。

  既定では、このオプションがオンです。

- **アカウントの指定**

  ［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

  - **アカウント**

    タスクを実行するアカウント。

  - **パスワード**

    タスクが実行されるアカウントのパスワード。

［**次へ**］をクリックして次のステップに進みます。

ステップ 5：タスクスケジュールの設定

［**タスクスケジュールの設定**］ウィザードウィンドウで、タスク開始のスケジュールを作成できます。必要に応じて、次の設定を指定します：

- **実行予定：**

  タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

  - **N 時間ごと**

    指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

    既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

  - **N 日ごと**

    日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

    既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

  - **N 週間ごと**

    指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

    既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

- **N 分ごと**

  タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

  既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

- **毎日（サマータイムはサポートしていません）**

  日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を 1 時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

  このスケジュールの使用は推奨されません。Kaspersky Security Center の旧バージョンとの後方互換性を維持するために用意されているオプションとなります。

  既定では、毎日、現在のシステム時刻にタスクが実行されます。

- **毎週**

  毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。

  指定した日付が存在しない月には、月の最終日にタスクを実行します。

  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。

  規定では、日付は選択されていません。規定の開始時間は18:00 です。

- **ウイルスアウトブレイク検知次第**

［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

- ワークステーションとファイルサーバー向けアンチウイルス製品
- 境界防御向けアンチウイルス製品
- メールサーバー向けアンチウイルス製品

既定では、すべてのアプリケーション種別がオンです。

ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

- タスク名で検索するには、検索フィールドにタスク名を入力します。
- 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。

  既定では、タスクはアルファベットの昇順で並べ替えられます。
- フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる(分)**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  既定では、このオプションはオフです。既定の時間は1分です。

ステップ6：タスク名の定義

［**タスク名の定義**］ウィンドウで、作成中のタスク名を指定します。タスク名は100文字以下で、特殊文字（`"*<>?\:|`）を含めることはできません。

［**次へ**］をクリックして次のステップに進みます。

ステップ7：タスクの作成完了

［**タスク作成の終了**］ウィンドウで、［**終了**］をクリックしてウィザードを終了します。

ウィザード終了後にすぐにタスクを開始するには、［**ウィザードの終了後にタスクを実行**］をオンにします。

統計情報の管理

保護システムと管理対象デバイスのステータスの統計は、カスタマイズ可能な情報パネルに表示されます。統計情報は、［**管理サーバー**］フォルダーの作業領域の［**統計**］タブに表示されます。タブにはいくつかの下位レベルのタブ（ページ）があります。各タブページには、統計情報パネルの他、カスペルスキーからのお知らせとその他の資料へのリンクが表示されます。統計情報は情報パネル上で表またはグラフ（円グラフまたは棒グラフ）として表示されます。情報パネルのデータは、アプリケーションの実行中アップデートされ、保護アプリケーションの最新の状態を反映します。

［**統計**］タブの下位に含めるタブ、各タブページの情報パネルの数、情報パネルのデータ表示モードを変更できます。

*［**統計**］タブに情報パネルのある下位のタブを新規追加するには：*

1. ［**統計**］タブの右上にある［**表示のカスタマイズ**］をクリックします。

   統計のプロパティウィンドウが開きます。このウィンドウには、［**統計**］タブ上に表示されるタブページのリストが含まれます。このウィンドウでは、タブのページの表示順序を変更したり、ページを追加または削除したり、［**プロパティ**］をクリックしてページのプロパティの設定ページに移動したりできます。

2. ［**追加**］をクリックします。

   新規ページのプロパティウィンドウを開きます。

3. 新規ページを設定します：

   - ［**全般**］セクションで、ページの名前を指定します：
   - ［**情報パネル**］セクションで、［**追加**］をクリックしてこのページで表示される必要がある情報パネルを追加します。

     ［**情報パネル**］セクション内の［**プロパティ**］をクリックして、追加した情報パネルのプロパティ（名前、種別、パネルの図表の表示方法および図表の基になるデータ）を設定します。

4. ［OK］をクリックします。

［**統計**］タブに、追加した情報パネルのあるタブページが表示されます。設定アイコン（⚙）をクリックすると、ページの設定またはそのページの選択した情報ペインの設定にすぐに移動できます。

イベント通知の設定

Kaspersky Security Center では、クライアントデバイスで発生したイベントについて管理者に通知するように設定し、その通知方法を選択することができます：

- メール：イベントが発生すると、指定されたメールアドレスに通知を送信します。この通知のテキストを編集することができます。
- SMS：イベントが発生すると、指定された電話番号に通知を送信します。メールゲートウェイを使用して SMS 通知を送信するよう設定できます。
- 実行ファイル：デバイスでイベントが発生すると、管理コンピューターで実行ファイルが起動されます。管理者は、実行ファイルを使用して、発生した任意のイベントのパラメータを受信できます。

クライアントデバイスで発生したイベントの通知を設定するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**イベント**］タブを選択します。
3. ［**通知とイベントのエクスポートの設定**］をクリックして、ドロップダウンリストから［**通知の設定**］を選択します。

   ［**プロパティ：イベント**］ウィンドウが表示されます。
4. ［**通知**］セクションで、通知の方法（メール、SMS、ファイルの実行）を選択して通知の設定を定義することができます。

   - **メール**

［**メール**］タブで、イベントのメール通知を設定できます。

［**受信者（メールアドレス）**］に、通知の送信先となるメールアドレスを指定します。このフィールドでは、複数のアドレスをセミコロンで区切って指定することができます。

［**SMTP サーバー**］に、メールサーバーのアドレスをセミコロンで区切って指定します。次の値を使用できます：

- IPv4 / IPv6 アドレス
- デバイスの Windows ネットワーク名（NetBIOS 名）
- SMTP サーバーの DNS 名

［**SMTP サーバーのポート**］に、SMTP サーバーの通信ポート番号を指定します。既定のポート番号は 25 です。

［**DNS MX ルックアップを使用**］を有効にすると、IP アドレスの複数の MX レコードを、SMTP サーバーの同一の DNS 名に使用できます。同一 DNS 名に複数の MX レコードが存在し、各レコードのメール受信の優先度の値が異なる場合があります。管理サーバーは SMTP サーバーへのメール通知の 送信を、MX レコードの優先度の昇順に試行します。既定では、このオプションはオフです。

［**DNS MX ルックアップを使用**］を有効にし、TLS 設定の使用は有効にしない場合、メール通知を保護する追加の方法として、サーバーデバイスで DNSSEC 設定を使用することを推奨します。

［**設定**］をクリックし、通知の詳細設定を指定します：

- 件名（メールの件名）
- 送信者のメールアドレス
- ESMTP 認証設定

SMTP サーバーの ESMTP 認証オプションを有効にする場合、SMTP サーバーの認証用アカウントを指定する必要があります。

- SMTPサーバーの TLS 設定：
  - **TLS を使用しない**

    メールの暗号化を無効にする場合に、このオプションを選択できます。
  - **TLS を使用する（SMTP サーバーがサポートする場合）**

    SMTP サーバーに TLS 接続を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは TLS を使用せずに SMTP サーバーへ接続します。
  - **常に TLS を使用し、サーバー証明書の有効性をチェックする**

    TLS 認証設定を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは SMTP サーバーへ接続できません。

SMTP サーバーの接続の保護をより強化する目的で、このオプションを使用することを推奨します。このオプションを選択すると、TLS 接続の認証設定を指定できます。

［**常に TLS を使用し、サーバー証明書の有効性をチェックする**］を選択した場合は、SMTP サーバーの認証用の証明書を指定し、TLS の任意のバージョンを介した通信を有効にするか、TLS 1.2 以降のバージョンのみを介した通信を有効にするかを選択できます。また、SMTP サーバーでクライアント認証に使用する証明書を指定することもできます。

SMTP サーバーの TLS 設定を指定できます：

- SMTP サーバーの証明書ファイルを参照します：

信頼できる証明書認証局から証明書のリストを含むファイルを受け取り、ファイルを管理サーバーへアップロードできます。Kaspersky Security Center は、SMTP サーバーの証明書も信頼できる証明書認証局によって署名されているかどうかをチェックします。信頼できる証明書認証局から SMTP サーバーの証明書を受け取っていない場合、Kaspersky Security Center は SMTP サーバーに接続できません。

- クライアント証明書ファイルを参照します：

信頼できる認証局など、任意の発行元から受け取った証明書を使用できます。次のいずれかの証明書タイプを使用して、証明書とその秘密鍵を指定する必要があります：

- X-509証明書：

証明書を含むファイルと秘密鍵を含むファイルを指定する必要があります。両方のファイルは相互に依存せず、ファイルを読み込む順序は重要ではありません。両方のファイルを読み込む時は、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

- pkcs12 コンテナー：

証明書とその秘密鍵を含む単一のファイルをアップロードする必要があります。ファイルの読み込み時に、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

［**通知メッセージ**］には、イベント発生時に送信される、イベントに関する情報を含む標準的なメッセージが表示されます。このメッセージには、イベント名、デバイス名、ドメイン名といった代替パラメータが含まれます。イベントに関連する詳細情報の代替パラメータを追加して、メッセージを編集できます。代替パラメータのリストは、このフィールドの右側にあるボタンをクリックすると表示されます。

通知テキストにパーセント記号「%」が含まれる場合、メッセージを送信するには 2 つ続けて入力する必要があります。たとえば、「CPU の負荷 100%%」のように入力します。

［**通知数の上限を設定する**］をクリックし、指定した時間内に送信できる最大通知数を指定します。

［**テストメッセージの送信**］をクリックし、通知の設定が適切かどうかをチェックします。指定したメールアドレスに、テストの通知が送信されます。

- SMS

［**SMS**］タブでは、携帯電話へ送信する様々なイベントの SMS 通知を設定できます。SMS メッセージはメールゲートウェイを通して送信されます。

［**宛先（メールアドレス）**］に、通知の送信先となるメールアドレスを指定します。このフィールドでは、複数のアドレスをセミコロンで区切って指定することができます。通知は、指定したメールアドレスに関連付けられている電話番号に送信されます。

［**SMTP サーバー**］に、メールサーバーのアドレスをセミコロンで区切って指定します。次の値を使用できます：

- IPv4 / IPv6 アドレス
- デバイスの Windows ネットワーク名（NetBIOS 名）
- SMTP サーバーの DNS 名

［**SMTP サーバーのポート**］に、SMTP サーバーの通信ポート番号を指定します。既定のポート番号は 25 です。

［**設定**］をクリックし、通知の詳細設定を指定します：

- 件名（メールの件名）
- 送信者のメールアドレス
- ESMTP 認証設定

必要に応じて、SMTP サーバーの ESMTP 認証オプションを有効にする場合、SMTP サーバーの認証用アカウントを指定できます。

- SMTPサーバーの TLS 設定

TLS の使用を無効にしたり、SMTP サーバーがこのプロトコルをサポートしている場合に TLS を使用するように設定したり、TLS のみの使用を強制したりすることができます。TLS のみを使用する場合は、SMTP サーバーの認証用の証明書を指定し、TLS の任意のバージョンを介した通信を有効にするか、TLS 1.2 以降のバージョンのみを介した通信を有効にするかを選択できます。また、TLS のみを使用する場合、SMTP サーバーのクライアント認証に使用する証明書を指定できます。

- SMTP サーバーの証明書ファイルを参照します

信頼できる証明書認証局から証明書のリストを含むファイルを受け取り、ファイルを Kaspersky Security Center にアップロードできます。Kaspersky Security Center は、SMTP サーバーの証明書も信頼できる証明書認証局によって署名されているかどうかをチェックします。信頼できる証明書認証局から SMTP サーバーの証明書を受け取っていない場合、Kaspersky Security Center は SMTP サーバーに接続できません。

証明書とその秘密鍵を含む単一のファイルをアップロードする必要があります。ファイルの読み込み時に、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。［**通知メッセージ**］には、イベント発生時に送信される、イベントに関する情報を含む標準的なメッセージが表示されます。このメッセージには、イベント名、デバイス名、ドメイン名といった代替パラメータが含まれます。イベントに関連する詳細情報の代替パラメータを追加して、メッセージを編集できます。代替パラメータのリストは、このフィールドの右側にあるボタンをクリックすると表示されます。

通知テキストにパーセント記号「%」が含まれる場合、メッセージを送信するには 2 つ続けて入力する必要があります。たとえば、「CPU の負荷 100%%」のように入力します。

［**通知数の上限を設定する**］をクリックし、指定した時間内に送信できる最大通知数を指定します。

［**テストメッセージの送信**］をクリックし、通知が正しく設定されているかチェックします。指定した受信者に、テストの通知が送信されます。

- 実行ファイル

この通知方法を選択すると、イベントの発生時に起動するアプリケーションを入力フィールドで選択できます。

［**通知数の上限を設定する**］をクリックすると、指定した時間内に送信できる最大通知数を指定できます。

［**テストメッセージの送信**］をクリックすると、通知が正しく設定されているか確認することができます。指定したメールアドレスにテスト通知が送信されます。

5. ［**通知メッセージ**］で、イベント発生時にアプリケーションが送信するテキストを入力します。

   テキストフィールドの右にあるドロップダウンリストを使用して、イベントの詳細（イベントの説明や発生時刻など）に置換される文字列を追加できます。

   通知テキストにパーセント記号（%）が含まれる場合、メッセージが送信されるようにするには、この記号を 2 回続けて入力する必要があります。たとえば、「CPU の負荷 100%%」のように入力します。

6. ［**テストメッセージの送信**］をクリックして、通知が正しく設定されたかどうかを確認します。

   指定されたユーザーにテストの通知が送信されます。

7. ［**OK**］をクリックして変更内容を保存します。

クライアントデバイスで発生するすべてのイベントに、再調整された通知設定が適用されます。

管理サーバーの設定、ポリシーの設定、またはアプリケーションの設定で、［**イベントの設定**］で指定された設定を特定のイベントについて上書きできます。

SMTP サーバー用の証明書の作成

SMTP サーバー用の証明書を作成するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**イベント**］タブを選択します。
3. ［**通知とイベントのエクスポートの設定**］をクリックして、ドロップダウンリストから［**通知の設定**］を選択します。

   イベントのプロパティウィンドウが開きます。
4. ［**メール**］タブで、［**設定**］をクリックして、［**設定**］ウィンドウを開きます。
5. ［**設定**］ウィンドウで、［**証明書を指定**］をクリックして、［**署名用の証明書**］ウィンドウを開きます。
6. ［**署名用の証明書**］ウィンドウで、［**参照**］をクリックします。

   ［**証明書**］ウィンドウが表示されます。
7. ［**証明書の種別**］で、証明書の種別について、プライベート証明書か公開証明書かを指定します。

   - プライベート証明書（**PKCS #12 コンテナー**）を選択した場合は、証明書ファイルを指定してパスワードを設定します。

- 公開証明書（**X.509 証明書**）を選択した場合：

  a. 秘密鍵ファイルを指定します（拡張子が *.prk または *.pem のファイル）。

  b. 秘密鍵のパスワードを指定します。

  c. 公開鍵のパスワードを指定します（拡張子が *.cer のファイル）。

8. ［**OK**］をクリックします。

SMTP サーバー用の証明書が発行されます。

イベントの抽出

Kaspersky Security Center と管理対象アプリケーションの動作中に発生するイベントに関する情報は、管理サーバーデータベースと Microsoft Windows システムログの両方に保存されます。管理サーバーデータベースに保存されている情報は、［**管理サーバー**］フォルダーの作業領域内の［**イベント**］タブで確認できます。

［**イベント**］タブの情報は、イベントの抽出のリストとして表示されます。各抽出には、特定の種別のイベントのみが含まれます。たとえば、［デバイスのステータスが「緊急」］の抽出は、デバイスのステータスが「緊急」に変更された記録のみを含みます。アプリケーションのインストール後、［**イベント**］タブには標準のイベント抽出がいくつか含まれています。イベントの抽出を追加（カスタム）で作成したり、イベント情報をファイルにエクスポートしたりすることができます。

イベントの抽出の表示

イベントの抽出を表示するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**イベント**］タブを選択します。
3. ［**イベントの抽出**］で、該当するイベントの抽出を選択します。

   ワークスペースにこの抽出を継続的に表示させる場合は、この抽出の隣にある星アイコン (☆) をクリックします。

作業領域に、管理サーバーに保管されている、選択した種類のイベントのリストが表示されます。

イベントのリストに含まれる情報は、任意の列で昇順または降順に並べ替えることができます。

イベントの抽出のカスタマイズ

イベントの抽出をカスタマイズするには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**イベント**］タブを選択します。
3. ［**イベント**］タブで、関連するイベントの抽出を開きます。

4. ［**抽出のプロパティ**］をクリックします。

イベントの抽出のプロパティウィンドウが開いたら、イベントの抽出を設定します。

イベントの抽出の作成

イベントの抽出を作成するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**イベント**］タブを選択します。
3. ［**抽出の作成**］をクリックします。
4. ［**新規のイベントの抽出**］ウィンドウが開いたら、新しい抽出の名前を入力して［**OK**］をクリックします。

［**イベントの抽出**］内で、指定した名前の抽出が作成されます。

作成したイベントの抽出には、管理サーバーに保存されているすべてのイベントが既定で含まれています。必要なイベントのみが抽出に表示されるようにするは、その抽出をカスタマイズする必要があります。

イベントの抽出のテキストファイルへのエクスポート

イベントの抽出をテキストファイルにエクスポートするには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**イベント**］タブを選択します。
3. ［**インポート / エクスポート**］をクリックします。
4. ドロップダウンリストから［**イベントをファイルにエクスポート**］を選択します。

イベントエクスポートウィザードが起動します。ウィザードの指示に従ってください。

抽出からのイベントの削除

抽出からイベントを削除するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**イベント**］タブを選択します。
3. マウスと、**Shift** キーまたは **Ctrl** キーを使用して、削除するイベントを選択します。
4. 次のいずれかの方法で、選択したイベントを削除します：

- 選択したイベントのコンテキストメニューで［**削除**］を選択します。

  コンテキストメニューで［**すべて削除**］を選択すると、削除するよう選択したイベントに関係なく、表示されているすべてのイベントが抽出から削除されます。

- イベントの情報ボックスで［**イベントの削除**］をクリックします。イベントの削除

選択したイベントが削除されます。

ユーザーからの要求に基づいてアプリケーションを除外に追加する

誤ってブロックされているアプリケーションのブロックを解除してほしいという要求をユーザーから受け取った場合、これらのアプリケーションのアダプティブセキュリティルールから除外を作成できます。これにより、ユーザーのデバイスで該当するアプリケーションはブロックされなくなります。ユーザーからの要求の数を、管理サーバーの［**監視**］タブで追跡できます。

Kaspersky Endpoint Security によってブロックされたアプリケーションを、ユーザーからの要求に基づいて除外に追加するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**イベント**］タブを選択します。
3. ［**イベントの抽出**］ドロップダウンリストで、［**ユーザー要求**］を選択します。
4. 除外に追加するアプリケーションを含むユーザー要求（複数選択可）を右クリックし、［**除外の追加**］を選択します。

   これにより、［除外の追加］ウィザードが起動します。表示される指示に従ってください。

クライアントデバイスと管理サーバーの次回の同期後に選択したアプリケーションは［**「スマートトレーニング」ステータスのルール適用条件**］の検知結果リスト（コンソールツリーの［**リポジトリ**］フォルダー内）から除外され、表示されなくなります。

デバイスの抽出

デバイスのステータスに関する情報は、コンソールツリーの［**デバイスの抽出**］フォルダーに表示されます。

［**デバイスの抽出**］フォルダーの情報は、デバイスの抽出のリストとして表示されます。各抽出に、特定の条件を満たすデバイスが含まれています。たとえば、［**「緊急」ステータスのデバイス**］には、ステータスが「*緊急*」のデバイスのみが含まれます。アプリケーションのインストール後、［**デバイスの抽出**］フォルダーには標準の抽出がいくつか含まれています。デバイスの抽出を追加で作成したり、抽出の設定をファイルにエクスポートしたりすることができます。また、他のファイルからインポートした設定を使用して抽出を作成することもできます。

デバイスの抽出の表示

デバイスの抽出を表示するには：

1. コンソールツリーで、［**デバイスの抽出**］フォルダーを選択します。

2. このフォルダーの作業領域で、［**抽出されたデバイス**］から、目的のデバイスの抽出を選択します。

3. ［**抽出を実行**］をクリックします。

4. ［**抽出の結果**］タブをクリックします。

作業領域に、抽出条件を満たすデバイスのリストが表示されます。

デバイスのリストに含まれる情報は、任意の列で昇順または降順に並べ替えることができます。

デバイスの抽出の設定

デバイスの抽出を設定するには：

1. コンソールツリーで、［**デバイスの抽出**］フォルダーを選択します。

2. 作業領域で［**抽出**］タブをクリックし、ユーザーの抽出のリストから目的のデバイスの抽出を選択します。

3. ［**抽出のプロパティ**］をクリックします。

4. 表示されるプロパティウィンドウで、次を設定します：

   - 抽出の全般設定
   - この抽出に含めるデバイスが満たす必要のある条件の設定：条件名を選択して［**プロパティ**］をクリックすることで、条件を編集できます
   - セキュリティ設定

5. ［OK］をクリックします。

   設定が適用され保存されます。

以下に、デバイスを抽出に割り当てる条件について説明します。条件は論理演算子「OR」を使用して結合されます。抽出には、少なくとも1つの条件を満たすデバイスが含まれます。

全般

［**全般**］セクションでは、抽出条件の名前を変更したり、条件を反転させたりすることができます：

抽出の条件を反転させる

このオプションをオンにすると、指定した抽出条件の選択状態が反転します。指定した条件に合致しないすべてのデバイスが、抽出に含まれるようになります。

既定では、このオプションはオフです。

ネットワーク

［**ネットワーク**］セクションでは、ネットワークデータを基にデバイスを抽出に含める場合に使用する基準を指定できます：

- **デバイス名または IP アドレス**

  デバイスの Windows ネットワーク名（NetBIOS 名）、あるいは IPv4 アドレスまたは IPv6 アドレス。

- **Windows ドメイン**

  指定した Windows ドメインに含まれるデバイスをすべて表示します。

- **管理グループ**

  指定した管理グループに含まれるデバイスを表示します。

- **説明**

デバイスのプロパティウィンドウ（［**全般**］セクションの［**説明**］）のテキスト。
［**説明**］で検索に使用する表現として、次の文字を使用できます：

- 1つの単語：
  - ***** -文字数不定の任意の文字列を表します。

    例：

    Server または **Server's** などの単語を記述するには、**Server*** と入力します。
  - **?** -任意の1文字を表します。

    例：

    Window または **Windows** などの単語を記述するには、**Windo?** と入力します。
    アスタリスク（*****）または疑問符（**?**）は、クエリの先頭文字としては使用できません。
- 複数の単語による検索：
  - スペース -指定した単語のいずれかがコメントに含まれているデバイスがすべて表示されます。

    例：

    Secondary または **Virtual** という単語が含まれている語句を検索する場合は、クエリに **Secondary Virtual** と入力します。
  - **+** -単語の前にプラス記号を付けると、すべての検索結果にその単語が含まれます。

    例：

    Secondary と **Virtual** の両方が含まれた語句を検索するには、クエリに **+Secondary+Virtual** と入力します。
  - **-** -単語の前にマイナス記号を付けると、すべての検索結果にその単語が含まれません。

    例：

    Secondary が含まれ、**Virtual** が含まれない語句を検索するには、クエリに **+Secondary-Virtual** と入力します。
  - **"<任意のテキスト>"** -引用符で囲まれたテキストを含むテキストが検索されます。

    例：

    Secondary Server という語句を検索する場合は、クエリに **"Secondary Server"** と入力します。

- **IP アドレス範囲**

  このオプションをオンにすると、検索されるデバイスが属する IP アドレス範囲の最初と最後の IP アドレスを入力できます。
  既定では、このオプションはオフです。

タグ

［**タグ**］セクションでは、管理対象デバイスの説明に追加済みのキーワード（タグ）を基にデバイスを抽出に含めるための基準を設定できます：

- **少なくとも 1 個のタグが一致する場合に適用する**

  このオプションをオンにすると、選択されたタグを 1 つ以上説明に含むデバイスが検索結果に表示されます。

  このオプションをオフにすると、選択されたすべてのタグを説明に含むデバイスのみが検索結果に表示されます。

  既定では、このオプションはオフです。

- **タグを含む**

  このオプションをオンにすると、検索結果には、選択したタグが説明内に含まれるデバイスが表示されます。デバイスを検索するため、文字数不定の任意の文字列を表すアスタリスクを使用できます。

  既定では、このオプションがオンです。

- **タグを含まない**

  このオプションをオンにすると、検索結果には、選択したタグが説明内に含まれないデバイスが表示されます。デバイスを検索するため、文字数不定の任意の文字列を表すアスタリスクを使用できます。

Active Directory

［**Active Directory**］セクションでは、Active Directory データを基にデバイスを抽出に含めるための基準を設定できます：

- **デバイスが配置されている Active Directory 組織単位**

  このオプションをオンにすると、抽出には、入力フィールドで指定した Active Directory 組織単位のデバイスが含まれます。

  既定では、このオプションはオフです。

- **子組織単位を含める**

  このオプションをオンにすると、抽出には、指定したドメイン組織単位のすべての子組織単位（OU）のデバイスが含まれます。

  既定では、このオプションはオフです。

- **デバイスが属している Active Directory グループ**

  このオプションを有効にすると、抽出には、入力フィールドで指定した Active Directory グループのデバイスが含まれます。

  既定では、このオプションはオフです。

ネットワーク活動

［**ネットワーク活動**］セクションでは、ネットワークアクティビティを基にデバイスを抽出に含める場合に使用する基準を指定できます：

- **ディストリビューションポイント**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：
  - **はい**：ディストリビューションポイントとして動作するデバイスが抽出に含まれます。
  - ［**いいえ**］。ディストリビューションポイントとして機能するデバイスが抽出に含まれません。
  - **値を選択しない**：基準は適用されません。

- **管理サーバーから切断しない**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：
  - **有効**：［**管理サーバーから切断しない**］をオンにしたデバイスが抽出に含まれます。
  - **無効**：［**管理サーバーから切断しない**］をオフにしたデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

- **接続プロファイルの切り替え**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：
  - **はい**：接続プロファイルを切り替えた結果として管理サーバーに接続されたデバイスが抽出に含まれます。
  - ［**いいえ**］。接続プロファイルを切り替えた結果として管理サーバーに接続されたデバイスが抽出に含まれません。
  - **値を選択しない**：基準は適用されません。

- **前回の管理サーバーへの接続**

  このチェックボックスを使用して、管理サーバーに前回接続した日時によるデバイスの検索の基準を設定できます。

  このチェックボックスをオンにすると、入力フィールドで、クライアントデバイスにインストールされたネットワークエージェントと管理サーバーとの間に前回接続が確立された日時の範囲を指定できます。指定された間隔内のデバイスが抽出に含まれます。

  このチェックボックスをオフにすると、この基準は適用されません。

  既定では、このチェックボックスはオフです。

- **ネットワークポーリングで検出された新規デバイス**

過去数日間のネットワークポーリングで検出された新規デバイスを検索します。

このオプションをオンにすると、［**検出期間（日）**］フィールドで指定した期間中のデバイスの検索で検出された新規デバイスのみが、抽出に含まれます。

このオプションをオフにすると、デバイスの検索で検出された新規デバイスがすべて抽出に含まれます。

既定では、このオプションはオフです。

- **デバイスが可視**

検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：

- **はい**：ネットワークで現在可視のデバイスを抽出に含めます。
- ［**いいえ**］。ネットワークで現在不可視のデバイスを抽出に含めます。
- **値を選択しない**：基準は適用されません。

アプリケーション

［**アプリケーション**］セクションでは、選択した管理対象アプリケーションを基にデバイスを抽出に含めるための基準を設定できます：

- **アプリケーション名**

カスペルスキー製品の名前で検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます。

リストには、管理コンピューターに管理プラグインがインストールされているアプリケーションの名前のみが表示されます。

アプリケーションが選択されていない場合、この基準は適用されません

- **アプリケーションのバージョン**

カスペルスキー製品のバージョン番号で検索を実行する場合、抽出に含めるデバイスの基準を、入力フィールドで設定できます。

バージョン番号が指定されていない場合、この基準は適用されません。

- **重要なアップデート名**

製品の名前またはアップデートパッケージ番号で検索する場合の、抽出に含めるデバイスの基準を、入力フィールドで設定できます。

このフィールドが空白の場合、この基準は適用されません。

- **前回のモジュールアップデート**

このオプションを使用して、デバイスにインストールされているソフトウェアモジュールの前回のアップデート日時でデバイスを検索する基準を設定できます。

このチェックボックスをオンにすると、入力フィールドで、デバイスにインストールされているアプリケーションモジュールの前回のアップデートが実行された日時の範囲を指定できます。

このチェックボックスをオフにすると、この基準は適用されません。

既定では、このチェックボックスはオフです。

- **デバイスを Kaspersky Security Center で管理する**

  ドロップダウンリストで、Kaspersky Security Center で管理されているデバイスを抽出に含めることができます：

  - **はい**Kaspersky Security Center で管理されているデバイスが抽出に含まれます。
  - ［**いいえ**］。Kaspersky Security Center により管理されていないデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

- **セキュリティ製品がインストールされている**

  ドロップダウンリストで、セキュリティ製品がインストールされているすべてのデバイスを抽出に含めることができます：

  - **はい**：セキュリティ製品がインストールされているすべてのデバイスが抽出に含まれます。
  - ［**いいえ**］。セキュリティ製品がインストールされていないすべてのデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

オペレーティングシステム

［**オペレーティングシステム**］セクションでは、オペレーティングシステム種別を基にデバイスを抽出に含める場合に使用する基準を指定できます。

- **オペレーティングシステムのバージョン**

  このチェックボックスをオンにすると、オペレーティングシステムをリストから選択できます。指定したオペレーティングシステムがインストールされたデバイスが検索結果に含まれます。

- **OS のビット数**

  ドロップダウンリストで、オペレーティングシステムのアーキテクチャを選択できます。これによって、デバイスに対する移動ルールの適用方法が決定されます（［**不明**］、［**x86**］、［**AMD64**］、［**IA64**］）。既定では、リストでオプションが選択されていないため、オペレーティングシステムのアーキテクチャは定義されていません。

- **OS サービスパックのバージョン**

このフィールドでは、オペレーティングシステムのパッケージバージョンを「*X.Y*」形式で指定できます。これによって、デバイスに対する移動ルールの適用方法が決定されます。既定では、バージョンの値は指定されていません。

- **OS のビルド**

  この設定は Windows オペレーティングシステムにのみ適用できます。

  オペレーティングシステムのビルド番号です。選択したオペレーティングシステムのビルド番号が、入力したビルド番号と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したビルド番号を除くすべてのビルド番号を検索するようにも設定できます。

- **OS のリリース ID**

  この設定は Windows オペレーティングシステムにのみ適用できます。

  オペレーティングシステムのリリース ID です。選択したオペレーティングシステムのリリース ID が、入力したリリース ID と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したリリース ID を除くすべてのリリース ID を検索するようにも設定できます。

デバイスのステータス

［**デバイスのステータス**］セクションでは、管理対象アプリケーションからのデバイスのステータスの説明を基にデバイスを抽出に含めるための基準を設定できます：

- **デバイスのステータス**

  ドロップダウンリストからデバイスのステータス（「*OK*」「*緊急*」「警告」）を選択します。

- **デバイスのステータスの説明**

  このフィールドで、「*OK*」「*緊急*」「*警告*」のいずれかのステータスをデバイスに割り当てる条件に対応するチェックボックスをオンにできます。

- **製品が定義したデバイスのステータス**

  リアルタイム保護のステータスを選択できるドロップダウンリスト。指定されたリアルタイム保護ステータスのデバイスが抽出に含まれます。

保護コンポーネント

［**保護コンポーネント**］セクションでは、保護ステータスを基にデバイスを抽出に含めるための基準を設定できます：

- **定義データベースの公開日時**

  このオプションをオンにすると、定義データベースの公開日時でクライアントデバイスを検索できます。入力フィールドで設定した期間に基づいて検索が実行されます。

  既定では、このオプションはオフです。

- **前回のスキャン**

  このオプションをオンにすると、前回マルウェアスキャンを実行した日時でクライアントデバイスを検索できます。入力フィールドで、前回マルウェアスキャンを実行した期間を指定できます。

  既定では、このオプションはオフです。

- **検知した脅威の数**

  このオプションをオンにすると、検知されたウイルスの数でクライアントデバイスを検索できます。入力フィールドで、ウイルス検知数の上下のしきい値を設定できます。

  既定では、このオプションはオフです。

アプリケーションレジストリ

［**アプリケーションレジストリ**］セクションでは、インストール済みのアプリケーションを基にデバイスを検索するための基準を設定できます：

- **アプリケーション名**

  アプリケーションを選択できるドロップダウンリスト。指定したアプリケーションがインストールされているデバイスが抽出に含まれます。

- **アプリケーションのバージョン**

  選択したアプリケーションのバージョンを指定できる入力フィールド。

- **製造元**

  デバイスにインストールされているアプリケーションの製造元を選択できるドロップダウンリスト。

- **アプリケーションのステータス**

  アプリケーションのステータス（*インストール済み*、*未インストール*）を選択できるドロップダウンリスト。指定のアプリケーションがインストール済みまたは未インストールのデバイスが、選択したステータスに応じて抽出に含まれます。

- **アップデートによって検索**

このオプションをオンにすると、該当するデバイスにインストールされているアプリケーションのアップデートに関する情報を使用して検索が実行されます。このチェックボックスをオンにすると、［**アプリケーション名**］、［**アプリケーションのバージョン**］、［**アプリケーションのステータス**］というフィールドがそれぞれ、［**アップデート名**］、［**アップデートのバージョン**］、［**ステータス**］に変わります。

既定では、このオプションはオフです。

- **競合するセキュリティ製品**

  サードパーティのセキュリティ製品を選択できるドロップダウンリスト。指定したアプリケーションがインストールされているデバイスが、検索時に抽出に含まれます。

- **アプリケーションタグ**

  このドロップダウンリストでは、アプリケーションタグを選択できます。選択したタグが説明にあるアプリケーションをインストール済みのすべてのデバイスが、デバイスの抽出に含まれます。

- **指定したタグのないデバイスに適用する**

  このオプションをオンにすると、選択したタグがいずれも説明に含まれないデバイスが抽出に含まれます。

  このオプションをオフにすると、基準が適用されません。

  既定では、このオプションはオフです。

ハードウェアレジストリ

［**ハードウェアレジストリ**］セクションでは、取り付けたハードウェアを基にデバイスを抽出に含めるための基準を設定できます：

- **デバイス**

  このドロップダウンリストでは、装置の種別を選択できます。その装置を備えたすべてのデバイスが検索結果に含まれます。

  このフィールドでは全文検索が可能です。

- **製造元**

  このドロップダウンリストで、装置の製造元の名前を選択できます。その装置を備えたすべてのデバイスが検索結果に含まれます。

  このフィールドでは全文検索が可能です。

- **デバイス名**

  デバイスの Windows ネットワークでの名前。指定された名前のデバイスが抽出に含まれます。

- **説明**

デバイスまたはハードウェア装置の説明。このフィールドで指定された説明が付けられたデバイスが抽出に含まれます。

デバイスの説明は、そのデバイスのプロパティウィンドウにあらゆる形式で入力できます。このフィールドでは全文検索が可能です。

- **デバイスの製造元**

  デバイスの製造元の名前。このフィールドで指定された製造元のデバイスが抽出に含まれます。

  コンピューターの製造元名は、デバイスのプロパティウィンドウで入力できます。

- **シリアル番号**

  このフィールドで指定されたシリアル番号が付けられたすべてのハードウェアユニットが抽出に含まれます。

- **インベントリ番号**

  このフィールドで指定されたインベントリ番号が付けられた機器が抽出に含まれます。

- **ユーザー**

  このフィールドで指定されたユーザーのすべてのハードウェアユニットが抽出に含まれます。

- **場所**

  デバイスまたはハードウェアユニットの場所（本社、支社など）。このフィールドで指定された場所に導入されるコンピューターまたはその他のデバイスが抽出に含まれます。

  デバイスの場所は、そのデバイスのプロパティウィンドウにおいて、あらゆる形式で記載できます。

- **CPU の周波数(MHz)**

  CPU の周波数範囲。これらのフィールドで指定された CPU の周波数範囲に適合するデバイスが抽出に含まれます。

- **仮想 CPU コア**

  仮想 CPU コア数の範囲。これらのフィールドで指定された CPU の範囲に適合するデバイスが抽出に含まれます。

- **ハードディスク容量（GB）**

  デバイスのハードディスクの容量の範囲。これらの入力フィールドで指定されたハードディスクの容量の範囲に適合するデバイスが抽出に含まれます。

- **RAM サイズ（MB）**

デバイスの RAM サイズの値の範囲。この範囲の値（指定した値を含む）のサイズの RAM を実装するデバイスが抽出に含まれます。

仮想マシン

［**仮想マシン**］セクションでは、仮想マシンであるか仮想デスクトップインフラストラクチャ（VDI）の一部であるかによってデバイスを抽出に含めるための基準を設定できます：

- **仮想マシン**

  このドロップダウンリストで、次のオプションを選択できます：
  - **判断しない**。
  - ［**いいえ**］。仮想マシンでないデバイスを検索します。
  - **はい**：仮想マシンであるデバイスを検索します。

- **仮想マシンの種別**

  このドロップダウンリストで、仮想マシンの製造元を選択できます。
  このドロップダウンリストは、［**仮想マシン**］の値が［**はい**］または［**判断しない**］である場合に使用できます。

- **仮想デスクトップインフラストラクチャの一部**

  このドロップダウンリストで、次のオプションを選択できます：
  - **判断しない**。
  - ［**いいえ**］。仮想デスクトップインフラストラクチャの一部でないデバイスを検索します。
  - **はい**：仮想デスクトップインフラストラクチャ（VDI）の一部であるデバイスを検索します。

脆弱性とアップデート

［**脆弱性とアップデート**］セクションでは、Windows Update をどこから取得するかを基にデバイスを抽出に含める場合に使用する基準を指定できます：

Windows Update エージェントの管理サーバーへの切り替え

このドロップダウンリストから、次のいずれかを選択できます：
- **はい**：これを選択すると、Windows Update の更新プログラムを管理サーバーから受信するデバイスが検索結果に含まれます。
- ［**いいえ**］。これを選択すると、Windows Update の更新プログラムを他の提供元から受信するデバイスが検索結果に含まれます。

ユーザー

［**ユーザー**］セクションでは、オペレーティングシステムにログインしたユーザーのアカウントを基にデバイスを抽出に含めるための基準を設定できます。

- **前回システムにログインしたユーザー**

  このオプションをオンにする場合は、［**参照**］をクリックしてユーザーアカウントを指定します。指定したユーザーがシステムの前回のログインを実行したデバイスが検索結果に含まれます。

- **少なくとも1回システムにログインしたユーザー**

  このオプションをオンにする場合は、［**参照**］をクリックしてユーザーアカウントを指定します。指定したユーザーがシステムに少なくとも1回ログインしたデバイスが検索結果に含まれます。

管理対象アプリケーションのステータスに影響がある問題

［**管理対象アプリケーションのステータスに影響がある問題**］セクションでは、管理対象アプリケーションで検知される可能性のある問題のリストを基にデバイスを抽出に含めるために使用する基準を設定できます：選択した問題のうち1つ以上の問題が存在するデバイスが抽出に含まれます複数のアプリケーションを対象とする問題については、同じ問題をすべてのアプリケーションのリストで自動的に選択するオプションがあります。

デバイスステータスの説明

管理対象アプリケーションからのステータスの説明に対応するチェックボックスをオンにできます。これらのステータスが受信されると、デバイスが抽出に含まれます。複数のアプリケーションを対象とするステータスについては、同じステータスをすべてのアプリケーションのリストで自動的に選択するオプションがあります。

管理対象アプリケーションのコンポーネントのステータス

［**管理対象アプリケーションのコンポーネントのステータス**］セクションでは、管理対象アプリケーションのコンポーネントのステータスを基にデバイスを抽出に含めるための基準を設定できます：

- **データ漏洩対策のステータス**

  データ漏洩対策のステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **コラボレーションサーバーの保護ステータス**

  サーバーコラボレーションの保護ステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **メールサーバーの保護ステータス**

メールサーバーの保護のステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **Endpoint Sensor のステータス**

  Endpoint Sensor のステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

暗号化

暗号化アルゴリズム

Advanced Encryption Standard（AES）対称ブロック暗号アルゴリズム。ドロップダウンリストから、暗号化キーのサイズ（56 ビット、128 ビット、192 ビット、または 256 ビット）を選択できます。

指定可能な値：*AES56*、*AES128*、*AES192*、または *AES256*。

クラウドセグメント

［**クラウドセグメント**］セクションでは、それぞれのクラウドセグメントを基にデバイスを抽出に含めるための基準を設定できます：

- **デバイスがクラウドセグメント内にある**

  このオプションを有効にすると、［**参照**］をクリックして、検索するセグメントを指定できます。

  ［**子オブジェクトも含む**］オプションも有効にする場合は、指定したセグメントのすべての子オブジェクトに対して検索が実行されます。

  検索結果には、指定したセグメントのデバイスしか含まれません。

- **API を使用して検出されたデバイス**

  ドロップダウンリストで、API ツールによりデバイスが検出されるかどうかを選択できます：

  - **AWS**：AWS API を使用して検出されたデバイスで、これはデバイスが間違いなく AWS クラウド環境にあることを意味します。
  - **Azure**：Azure API を使用して検出されたデバイスで、これはデバイスが間違いなく Azure クラウド環境にあることを意味します。
  - **Google Cloud**：Google API を使用して検出されたデバイスで、これはデバイスが間違いなく Google Cloud 環境にあることを意味します。
  - ［**いいえ**］。デバイスは AWS API、Azure API、Google API のいずれでも検出できません。これはデバイスがクラウド環境外にあるか、クラウド環境内にあるが API では検出できないことを意味します。
  - **値なし**：この条件は当てはまりません。

製品コンポーネント

このセクションでは、対応する管理プラグインが管理コンソールにインストールされているアプリケーションのコンポーネントのリストが表示されます。

［**製品コンポーネント**］セクションでは、選択したアプリケーションの管理下にあるコンポーネントのステータスとバージョン番号を基にデバイスを抽出に含めるための基準を設定できます：

- **ステータス**

  アプリケーションから管理サーバーに送信されたコンポーネントのステータスに基づいてデバイスを検索します。*デバイスからのデータなし*、*停止*、*開始中*、*一時停止*、*実行中*、*エラー*、*未インストール*のいずれかのステータスを選択できます。管理対象デバイスにインストールされたアプリケーションの選択したコンポーネントのステータスが指定したステータスと一致する場合、そのデバイスが抽出に含まれます。

  製品から送信されるステータス：

  - *開始中* - コンポーネントが利用開始プロセスを実行中です。
  - *実行中* - コンポーネントが有効で正常に動作しています。
  - *一時停止* - コンポーネントの動作が中断中です（例：管理対象製品でユーザーが保護を一時停止した）。
  - *エラー* - コンポーネントの動作中にエラーが発生しました。
  - *停止* - コンポーネントが無効で、現在動作していません。
  - *未インストール* - 製品のカスタムインストールの設定時に、ユーザーがコンポーネントをインストール対象として選択しませんでした。

  他のステータスとは異なり、［*デバイスからのデータなし*］ステータスはアプリケーションから送信されたものではありません。このステータスは、選択したコンポーネントのステータスについて、アプリケーションに情報がないことを示します。たとえば、デバイスにインストールされているアプリケーションのいずれにも選択したコンポーネントが属していない場合や、デバイスの電源がオフの場合などです。

- **バージョン**

  リストで選択したコンポーネントのバージョン番号に基づいてデバイスを検索します。`3.4.1.0` などのバージョン番号を入力し、選択したコンポーネントのバージョン番号がこれと「等しい」「それより古い」「それより新しい」かを指定できます。また、指定したバージョンを除くすべてのバージョンを検索するようにも設定できます。

デバイスの抽出の設定をファイルにエクスポート

デバイスの抽出の設定をテキストファイルにエクスポートするには：

1. コンソールツリーで、［**デバイスの抽出**］フォルダーを選択します。

2. 作業領域で［**抽出**］タブをクリックし、ユーザーの抽出のリストから目的のデバイスの抽出を選択します。

ユーザーが作成したデバイスの抽出からのみ、設定のエクスポートが可能です。

3. ［**抽出を実行**］をクリックします。

4. ［**抽出の結果**］タブで、［**設定のエクスポート**］をクリックします。

5. ［**名前を付けて保存**］ウィンドウが表示されたら、抽出の設定をエクスポートするファイルの名前を指定し、そのファイルを保存するフォルダーを指定して［**保存**］をクリックします。

デバイスの抽出の設定が、指定したファイルに保存されます。

デバイスの抽出の作成

デバイスの抽出を作成するには：

1. コンソールツリーで、［**デバイスの抽出**］フォルダーを選択します。

2. このフォルダーの作業領域で、［**詳細**］をクリックし、ドロップダウンリストから［**抽出の作成**］を選択します。

3. ［**新規のデバイスの抽出**］ウィンドウが開いたら、新しい抽出の名前を入力して［**OK**］をクリックします。

入力した名前を持つ新しいフォルダーがコンソールツリーの［**デバイスの抽出**］フォルダーに表示されます。新規のデバイスの抽出には、その抽出が作成された管理サーバーの管理グループに含まれるすべてのデバイスが既定で格納されます。必要なデバイスのみが抽出に表示されるようにするには、［**抽出のプロパティ**］をクリックして抽出を設定します。

インポートした設定に従ったデバイスの抽出の作成

インポートした設定に従ってデバイスの抽出を作成するには：

1. コンソールツリーで、［**デバイスの抽出**］フォルダーを選択します。

2. このフォルダーの作業領域で、［**詳細**］をクリックし、ドロップダウンリストから［**抽出をファイルからインポート**］を選択します。

3. ウィンドウが開いたら、インポートする抽出の設定を含むファイルのパスを指定します。［**開く**］をクリックします。

［**新規の抽出**］エントリが［**デバイスの抽出**］フォルダーに作成されます。新しい抽出の設定が指定したファイルからインポートされます。

［**デバイスの抽出**］フォルダーに［**新規の抽出**］という名前の抽出が既に存在する場合は、抽出の名前の末尾に、**(1)**、**(2)** のように「**(<次の連番>)**」が追加されます。

抽出で管理グループからデバイスを削除

デバイスの抽出作業を行う場合は、デバイスを削除する必要がある管理グループに切り替えずに、この抽出に含まれる管理グループからデバイスを削除することができます。

管理グループからデバイスを削除するには：

1. コンソールツリーで、［**デバイスの抽出**］フォルダーを選択します。
2. **Shift** キーまたは **Ctrl** キーを使用して、削除するデバイスを選択します。
3. 次のいずれかの方法で、選択したデバイスを管理グループから削除します：
   - 選択した任意のデバイスのコンテキストメニューで［**削除**］を選択します。
   - ［**処理を実行**］をクリックし、ドロップダウンリストから［**グループから削除**］を選択します。

選択したデバイスが対応する管理グループから削除されます。

製品のインストールとアンインストールの監視

特定のアプリケーション（例：特定のブラウザーなど）を対象に、インストールとアンインストールを監視できます。この機能を使用するために、監視対象のアプリケーションのリストに、アプリケーションレジストリからアプリケーションを追加できます。監視対象のアプリケーションがインストールまたはアンインストールされると、ネットワークエージェントがイベントを記録します（「**監視対象アプリケーションがインストールされました**」または「**監視対象アプリケーションがアンインストールされました**」）。これらのイベントを、イベントの抽出またはレポートを使用して監視できます。

これらのイベントは、管理サーバーのデータベースに保存されている場合にのみ監視できます。

監視対象のアプリケーションのリストにアプリケーションを追加するには：

1. コンソールツリーの［**詳細**］フォルダーで、［**アプリケーションの管理**］フォルダーから［**アプリケーションレジストリ**］サブフォルダーを選択します。
2. 表示されているアプリケーションの上で、［**アプリケーションレジストリのプロパティウィンドウの表示**］をクリックします。
3. ［**監視対象アプリケーション**］ウィンドウが表示されたら、［**追加**］をクリックします。
4. ［**アプリケーションの選択**］ウィンドウが表示されたら、インストールとアンインストールを監視するアプリケーションをアプリケーションレジストリから選択します。
5. ［**アプリケーションの選択**］ウィンドウで、［**OK**］をクリックします。

監視対象のアプリケーションのリストの設定が完了すると、イベント抽出の「最近のイベント」を使用するなどして、組織内の管理対象デバイスで監視対象のアプリケーションのインストールまたはアンインストールが行われたというイベントを監視できます。

Kaspersky Security Center のコンポーネントでのイベント

Kaspersky Security Center の各コンポーネントには、独自のイベント種別のセットがあります。このセクションでは、Kaspersky Security Center 管理サーバーとネットワークエージェント、iOS MDM サーバーで発生するイベントの種別について説明します。カスペルスキー製品で発生する可能性のあるイベントの種別は、このセクションの説明には含まれていません。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

イベント種別のデータ構造の説明

イベント種別ごとに、表示名、識別子（ID）、英字コード、内容の説明、既定の保管期間を記載しています。

- **イベント種別の表示名**：イベントを設定してそれが発生すると、この列のテキストが Kaspersky Security Center で表示されます。
- **イベント種別の ID**：イベント解析用のサードパーティ製品を使用してイベントを処理すると、この列の数字コードが使用されます。
- **イベント種別**（英字コード）：Kaspersky Security Center データベースで提供されるパブリックビューを使用してイベントの参照と処理を行う場合とイベントを SIEM システムにエクスポートする場合に、この列のコードが使用されます。
- **説明**：この列では、イベントが発生する状況と可能な対応が説明されています。
- **既定の保管期間**：この列には、イベントが管理サーバーデータベースに保管され、管理サーバーのイベントリストに表示される日数が記載されています。この期間が過ぎると、イベントが削除されます。イベントの保管期間の値が「0」の場合、これらのイベントについては検知のみが行われ、管理サーバーのイベントリストへの表示は行われません。こうしたイベントをオペレーティングシステムのイベントログに保存するように設定した場合、それらの保存先でイベントを確認できます。

  イベントの保存期間を変更できます：

  - 管理コンソール：イベントの保管期間の設定
  - Kaspersky Security Center Web コンソール：イベントの保管期間の設定

その他のデータには次のフィールドが含まれることがあります：

- **event_id**：自動で生成および割り当てられたデータベース内のイベントの一意な数字。**イベント種別の ID** とは異なります。
- **task_id**：イベントを発生させたタスクの識別子（該当する場合）
- **severity**：以下のセキュリティレベル（重要度の昇順）のうちの 1 つ：

  0) 無効なセキュリティレベル

  1) 情報

  2) 警告

  3) エラー

  4) 重要

管理サーバーのイベント

このセクションには、管理サーバーに関するイベントの情報が記載されています。

管理サーバーの緊急イベント

次の表は、重要度が「**緊急**」に分類される Kaspersky Security Center 管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

管理コンソールの［管理サーバーのプロパティ］ウィンドウでポートを指定した場合、**Kaspersky Security Center は、監視およびアラート用のシステムである Prometheus によって取得されるメトリクス**と緊急イベントを公開します。Prometheus はメトリクスと緊急イベントを取得し、イベントごとにアラートを生成します。

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

管理サーバーの緊急イベント

イベント種別の表示名	イベント種別の ID	イベント種別	説明	既定の保管期間
ライセンス数の上限を超えました	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	1 日に 1 回、Kaspersky Security Center はライセンス管理の上限の超過が発生していないかどうかを確認します。	180 日間

			この種別のイベントは、クライアントデバイスにインストールされているカスペルスキー製品で、ライセンスの上限の超過を管理サーバーが検出しており、単一のライセンスに紐付けられていて現在使用中のライセンス単位数がそのライセンスで本来許可されている合計ライセンス単位数の 110% を超えている場合に記録されます。 このイベントが発生した場合でも、クライアントデバイスの保護は継続されます。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストを確認します。使用されていないデバイスを削除します。 • 製品を使用できるデバイス数の上限が増えるように、ライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。 Kaspersky Security Center では、ライセンス数の上限を超過した時にイベントを生成するルールを指定できます。	
ウイルスアウトブレイク	26（ファイル脅威対策の場合）	GNRL_EV_VIRUS_OUTBREAK	この種別のイベントは、複数の管理対象デバイスで検知された悪意のあるオブジェクトの数が短期間のうちにしきい値を超えた場合に記録されます。 このイベントには、次の方法で対応できます： • 対象となるしきい値を管理サーバーのプロパティで編集します。 • このイベントの発生時に有効になるより基準の厳しいポリシーを作成したり、イベント発生時に実行されるタスクを作成します。	180 日間
ウイルスアウトブレイク	27（メール脅威対策の場合）	GNRL_EV_VIRUS_OUTBREAK	この種別のイベントは、複数の管理対象デバイスで検知された悪意のあるオブジェクトの数が短期間のうちにしきい値を超えた場合に記録されます。 このイベントには、次の方法で対応できます： • 対象となるしきい値を管理サーバーのプロパティで編集します。 • このイベントの発生時に有効になるより基準の厳しいポリシーを作成したり、イベント発生時に実行されるタスクを作成します。	180 日間
ウイルスアウトブレイク	28（ファイアウォールの場合）	GNRL_EV_VIRUS_OUTBREAK	この種別のイベントは、複数の管理対象デバイスで検知された悪意のあるオブジェクトの数が短期間のうちにしきい値を超えた場合に記録されます。 このイベントには、次の方法で対応できます： • 対象となるしきい値を管理サーバーのプロパティで編集します。 • このイベントの発生時に有効になるより基準の厳しいポリシーを作成したり、イベント発生時に実行されるタスクを作成します。	180 日間
デバイスが管理対象外になりました	4111	KLSRV_HOST_OUT_CONTROL	この種別のイベントは、デバイスはネットワーク上で可視だが管理サーバーに接続していない状態が指定期間を超えて継続すると記録されます。 デバイス上でネットワークエージェントの正常な動作を妨げている要素を特定します。原因としては、ネットワークの問題や、ネットワークエージェントがデバイスから削除された状況などが考えられます。	180 日間
デバイスのステータスが「緊急」です	4113	KLSRV_HOST_STATUS_CRITICAL	この種別のイベントは、管理対象デバイスに「*緊急*」ステータスが割り当てられると記録されます。デバイスのステータスが「*緊急*」に切り替わる条件を設定できます。	180 日間
このライセン	4124	KLSRV_LICENSE_BLACKLISTED	この種別のイベントは、使用しているアクティベーションコードまたはライセンス情報ファイルがカスペルスキーで拒否	180 日間

ス情報ファイルは拒否リストに追加されています			リストに登録されると記録されます。 詳細は、テクニカルサポートに問い合わせてください。	
機能が制限されています	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	この種別のイベントは、Kaspersky Security Center の動作モードが変更されて基本機能のみが使用可能になり、脆弱性とパッチ管理機能およびモバイルデバイス管理機能が使用できない時に記録されます。 イベントが発生する理由と対応は次の通りです： • ライセンスの有効期限が終了している：Kaspersky Security Center の全機能を使用できるモードで必要なライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。 • ライセンスの上限で指定された台数を超過して管理サーバーでデバイスを管理している：管理サーバーの管理グループから別の管理サーバーの管理グループにデバイスを移動します（移動先の管理サーバーのライセンスの上限内で）。	180 日間
ライセンスの有効期間がまもなく終了します	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	この種別のイベントは、製品版ライセンスの有効期限が近づいている時に発生します。 1 日に 1 回、Kaspersky Security Center はライセンス有効期間の終了日が近づいているかどうかを確認します。この種別のイベントは、ライセンスの有効期限まで残り 30 日、15 日、5 日および 1 日となった時に発生します。日数は変更できません。管理サーバーがライセンスの有効期限より前に指定された日にオフになった場合は翌日までイベントは発生しません。 製品版ライセンスの有効期間が終了した場合は、Kaspersky Security Center は基本機能のみを提供します。 このイベントには、次の方法で対応できます： • 予備のライセンスが管理サーバーに追加されていることを確認します。 • 定額制サービスをご利用の場合は、必ず更新してください。支払い期日までに決済された場合、無制限の定額制サービスは自動的に更新されます。	180 日間
証明書の有効期間が終了しています	4132	KLSRV_CERTIFICATE_EXPIRED	このタイプのイベントは、モバイルデバイス管理用の管理サーバー証明書の有効期間が終了すると発生します。 期限切れの証明書をアップデートする必要があります。	180 日間
カスペルスキー製品モジュールのアップデートが取り消されました	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	この種別のイベントは、カスペルスキーのテクニカルスペシャリストにより、より新しいバージョンの製品にアップデートする必要があるなどの理由でシームレスアップデートの利用が拒否された場合（アップデートのステータスとして「*取り消し*」が表示）に記録されます。このイベントは、Kaspersky Security Center のアップデートパッチを対象としており、管理対象のカスペルスキー製品モジュールとの関連はありません。イベントでは、シームレスアップデートがインストールされなかった理由に関する情報が提供されます。	180 日間
監査：SIEM へエクスポートできませんでした	5130	KLAUD_EV_SIEM_EXPORT_ERROR	このタイプのイベントは、SIEM システムとの接続エラーが原因で SIEM システムへのイベントのエクスポートが失敗した場合に発生します。	180 日間

管理サーバーの機能エラーイベント

次の表は、重要度が「**機能エラー**」に分類される Kaspersky Security Center 管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

管理サーバーの機能エラーイベント

イベント種別の表示名	イベント種別の ID	イベント種別	説明	既定の保管期間
実行時エラー	4125	KLSRV_RUNTIME_ERROR	この種別のイベントは、不明な問題が生じた時に記録されます。 ほとんどの場合、問題は DBMS の問題、ネットワークの問題、またはソフトウェアやハードウェアの問題から発生しています。 エラー情報の詳細は、イベントの説明で参照できます。	180 日間
インストール数の上限を超えたライセンス認証済みアプリケーショングループがあります	4126	KLSRV_INVLICPROD_EXCEDED	この種別のイベントは、管理サーバーによって 1 時間ごとに生成されます。この種別のイベントは、Kaspersky Security Center でサードパーティ製品を管理していて、サードパーティ製品のライセンスで設定された上限を超えると記録されます。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストを確認します。該当するサードパーティ製品が使用されていないデバイスからサードパーティ製品を削除します。 • 製品を使用できるデバイス数の上限が増えるように、サードパーティ製品のライセンスを追加します。 ライセンス認証済みアプリケーショングループ機能を使用することで、サードパーティ製品のライセンスを管理できます。ライセンス認証済みアプリケーショングループには、管理者が設定した基準を満たすサードパーティ製品が含まれます。	180 日間
クラウドセグメントのポーリングに失敗しました	4143	KLSRV_KLCLOUD_SCAN_ERROR	この種別のイベントは、管理サーバーがクラウド環境でネットワークセグメントのポーリングに失敗した時に発生します。イベントの説明に記載されている詳細情報を読み、適宜対応します。	保管されません
指定フォルダーにアップデートをコピーできませんでした	4123	KLSRV_UPD_REPL_FAIL	この種別のイベントは、ソフトウェアアップデートが指定したフォルダーでなく共有フォルダーにコピーされた場合に記録されます。 このイベントには、次の方法で対応できます： • 指定したフォルダーへのアクセスに使用されたユーザーアカウントに、書き込み権限があるかどうかを確認します。 • フォルダーにアクセスするためのユーザー名とパスワードが変更されていないかどうか確認します。 • インターネット接続がイベント発生の原因の可能性もあるので、これをチェックします。定義データベースとソフトウェアモジュールのアップデート手順に従って操作します。	180 日間
ディスクに空き容量がありません	4107	KLSRV_DISK_FULL	この種別のイベントは、管理サーバーがインストールされているデバイスのハードディスクの空き容量が不足すると発生します。	180 日間

			デバイスのディスク領域を解放します。	
共有フォルダーが使用できません	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	この種別のイベントは、管理サーバーの共有フォルダーが利用できない場合に記録されます。 このイベントには、次の方法で対応できます： • （共有フォルダーのある）管理サーバーが起動されていて利用可能な状態であることを確認します。 • フォルダーにアクセスするためのユーザー名とパスワードが変更されていないかどうか確認します。 • ネットワーク接続の問題がないか確認します。	180 日間
管理サーバーデータベースが使用できません	4109	KLSRV_DATABASE_UNAVAILABLE	この種別のイベントは、管理サーバーのデータベースが利用できなくなっている場合に記録されます。 このイベントには、次の方法で対応できます： • SQL サーバーがインストールされているリモートサーバーが利用できる状態になっているかを確認します。 • DBMS ログを確認し、管理サーバーデータベースを使用できなくなっている理由を特定します。たとえば、メンテナンスの実施が原因となって、SQL サーバーがインストールされているリモートサーバーが利用できなくなっている可能性などがあります。	180 日間
管理サーバーデータベースに空き容量がありません	4110	KLSRV_DATABASE_FULL	この種別のイベントは、管理サーバーのデータベースに空き容量がないと記録されます。 管理サーバーのデータベースが容量の上限に達してデータベースへの情報の記録ができなくなると、管理サーバーが正常に機能しなくなります。 このイベントが発生する主な原因は使用中の DBMS の種別に応じて 2 つあり、それぞれ適切な対応方法が異なります： • SQL Server Express Edition を DBMS として使用している場合： SQL Server Express のヘルプを参照して、使用中のバージョンのデータベースサイズの上限を確認します。管理サーバーのデータベースが、このデータベースサイズの上限に達した可能性があります。 管理サーバーデータベースに保存されるイベントの数を制限してください。 管理サーバーデータベースにアプリケーションコントロールコンポーネントから送信されたイベントの数が多すぎます。これには、管理サーバーデータベースでのアプリケーションコントロールイベントの保管期間に関する Kaspersky Endpoint Security for Windows ポリシーの設定を変更することで対応できます。 • SQL Server Express Edition 以外の DBMS を使用している場合： 管理サーバーのデータベースに保存されるイベントの数を制限しないでください。 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください。 DBMS の選定に関する情報を確認します。	180 日間

管理サーバーの警告イベント

次の表は、重要度が「**警告**」に分類される Kaspersky Security Center 管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

管理サーバーの警告イベント

イベント種別の表示名	イベント種別の ID	イベント種別	説明	既定の保管期間
頻出イベントが検出されました		KLSRV_EVENT_SPAM_EVENTS_DETECTED	このタイプのイベントは、管理サーバーが管理対象デバイスで頻出イベントを検知した時に発生します。詳細については、次のセクションを参照してください：「頻出イベントのブロック」。	90 日間
ライセンス数の上限を超えました	4098	KLSRV_EV_LICENSE_CHECK_100_110	1 日に 1 回、Kaspersky Security Center はライセンス管理の上限の超過が発生していないかどうかを確認します。 この種別のイベントは、クライアントデバイスにインストールされているカスペルスキー製品でライセンスの上限の超過が発生していることを管理サーバーが検知し、なおかつ単一のライセンスに紐付けられていて現在使用中のライセンス単位数がそのライセンスで本来許可されている合計ライセンス単位数の 100% から 110% の範囲内の場合に記録されます。 このイベントが発生した場合でも、クライアントデバイスの保護は継続されます。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストを確認します。使用されていないデバイスを削除します。 • 製品を使用できるデバイス数の上限が増えるように、ライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。 Kaspersky Security Center では、ライセンス数の上限を超過した時にイベントを生成するルールを指定できます。	90 日間
デバイスがネットワーク上で長期間アクティブになっていません	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	この種別のイベントは、管理対象デバイスが一定時間休止状態である場合に発生します。 このイベントが最も高頻度で発生するのは、管理対象デバイスが廃止された場合です。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストからデバイスを手動で削除します。 • 管理コンソールを使用して、または Kaspersky Security Center Web コンソールを使用して［**デバイスがネットワーク上で長期間アクティブになっていません**］イベントが作成されるまでの期間を指定します。 • 管理コンソールを使用して、または Kaspersky Security Center Web コンソールを使用して、デバイスがグループから自動的に削除されるまでの期間を指定します。	90 日間
デバイスの名前が競合しています	4102	KLSRV_EVENT_HOSTS_CONFLICT	この種別のイベントは、管理サーバーが 2 つ以上の管理対象デバイスを単一のデバイスと判断した場合に発生します。 このイベントが最も高頻度で発生するのは、クローンされたハードディスクが管理対象デバイスでのソフトウェアの導入に使用され、ネットワークエージェントを参照デバイスの専用ディスククローンモードに切り替えなかった場合です。 この問題を回避するには、このデバイスのハードディスクを複製する前に、参照デバイスでネットワークエージェントをディスククローンモードに切り替えます。	90 日間

デバイスのステータスが「警告」です	4114	KLSRV_HOST_STATUS_WARNING	この種別のイベントは、管理対象デバイスに「*警告*」ステータスが割り当てられると記録されます。デバイスのステータスが「*警告*」に切り替わる条件を設定できます。	90 日間
インストール数が上限に近づいているライセンス認証済みアプリケーショングループがあります	4127	KLSRV_INVLICPROD_FILLED	この種別のイベントは、ライセンス認証済みアプリケーショングループに含まれるサードパーティ製品のインストール数が、ライセンスのプロパティで指定された最大許容値の 90% に達すると発生します。 このイベントには、次の方法で対応できます： • 一部の管理対象デバイスでサードパーティ製品を使用していない場合は、これらのデバイスからアプリケーションを削除します。 • サードパーティ製品のインストール数が近い将来に許可される最大数を超えることが予想される場合は、事前にサードパーティのライセンスを取得する対象デバイスの数を増やすことを検討してください。 ライセンス認証済みアプリケーショングループ機能を使用することで、サードパーティ製品のライセンスを管理できます。	90 日間
証明書が要求されました	4133	KLSRV_CERTIFICATE_REQUESTED	この種別のイベントは、モバイルデバイス管理用の証明書を自動的に再発行できない場合に発生します。 考えられるイベントの原因と適切な対応について以下に示します。 • ［**可能であれば証明書を自動で再発行**］がオフにされている証明書に対して自動再発行が開始されました。これは、証明書の作成中に発生したエラーが原因であると考えられます。証明書の手動再発行が必要になる場合があります。 • 公開鍵インフラストラクチャと統合している場合、PKI との統合および証明書の発行に使用されるアカウントの SAM-Account-Name 属性の欠落が原因であると考えられます。アカウントのプロパティを確認します。	90 日間
証明書が削除されました	4134	KLSRV_CERTIFICATE_REMOVED	この種別のイベントは、管理者がモバイルデバイス管理用の任意の種別の証明書（一般、メール、VPN）を削除した場合に発生します。 証明書を削除すると、この証明書を介して接続されたモバイルデバイスは、管理サーバーへの接続に失敗します。 このイベントは、モバイルデバイスの管理に関連した誤動作を調査する際に有用な場合があります。	90 日間
APNs 証明書の有効期間が終了しています	4135	KLSRV_APN_CERTIFICATE_EXPIRED	この種別のイベントは、APNs証明書の有効期限が切れた場合に発生します。 手動で APNs 証明書を更新し、iOS MDM サーバーにインストールする必要があります。	保管されません
APNs 証明書の有効期間がまもなく終了します	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	この種別のイベントは、APNs 証明書の有効期限が切れるまでの残日数が 14日未満の場合に発生します。 APNs 証明書の有効期限が切れた場合は、手動で APNs 証明書を更新し、iOS MDM サーバーにインストールする必要があります。 有効期限に達する前に APNs 証明書の更新スケジュールを設定することを推奨します。	保管されません
モバイルデバイスに FCM メッセージを送信できませんでした	4138	KLSRV_GCM_DEVICE_ERROR	この種別のイベントは、Android オペレーティングシステムを搭載した管理対象のモバイルデバイスに接続するために Firebase Cloud Messaging（FCM）を使用するようにモバイルデバイス管理が設定されており、FCM サーバーが管理サーバーから受信したリクエストの一部を処理できない場合に発生します。これは、一部の管理対象モバイルデバイスがプッシュ通知を受信しないことを意味します。	90 日間

			イベントの説明の詳細に記載されている HTTP コードを読み、適宜対応します。FCM サーバーから受信した HTTP コードと関連エラーの詳細については、Firebase サービスのドキュメントを参照してください（「ダウンストリームメッセージのエラー応答コード」の章を参照）。	
FCM メッセージを FCM サーバーに送信している時に HTTP エラーが発生しました	4139	KLSRV_GCM_HTTP_ERROR	この種別のイベントは、モバイルデバイス管理が Android オペレーティングシステムを搭載した管理対象モバイルデバイスに接続するために Firebase Cloud Messaging（FCM）を使用するように設定されており、FCM サーバーが 200（OK）以外の HTTP コードで管理サーバーのリクエストに応答する場合に発生します。 考えられるイベントの原因と適切な対応について以下に示します。 • FCM サーバー側の問題。イベントの説明の詳細に記載されている HTTP コードを読み、適宜対応します。FCM サーバーから受信した HTTP コードと関連エラーの詳細については、Firebase サービスのドキュメントを参照してください（「ダウンストリームメッセージのエラー応答コード」の章を参照）。 • プロキシサーバー側の問題（プロキシサーバーを使用している場合）。イベントの説明の詳細に記載されている HTTP コードを読み、適宜対応します。	90 日間
FCM メッセージを FCM サーバーに送信できませんでした	4140	KLSRV_GCM_GENERAL_ERROR	この種別のイベントは、Firebase Cloud Messaging HTTP プロトコルを使用する際の管理サーバー側での予期しないエラーが原因で発生します。 イベントの説明に記載されている詳細情報を読み、適宜対応します。 ご自分で問題の解決方法を見つけられない場合は、カスペルスキーのテクニカルサポートへのお問い合わせを推奨します。	90 日間
ハードディスクの空き容量が残りわずかです	4105	KLSRV_NO_SPACE_ON_VOLUMES	この種別のイベントは、管理サーバーがインストールされているデバイスのハードディスク容量が不足した場合に発生します。 デバイスのディスク領域を解放します。	90 日間
管理サーバーデータベースに空き容量が残りわずかです	4106	KLSRV_NO_SPACE_IN_DATABASE	この種別のイベントは、管理サーバーのデータベースの空き容量が非常に少なくなっている場合に記録されます。状況を修正しないと、すぐに管理サーバーデータベースの容量が上限に達し、管理サーバーが正常に動作しなくなります。 使用されている DBMS の種別に応じた、このイベントが発生する原因と適切な対応方法を次に示します。 SQL Server Express Edition を DBMS として使用している場合： • SQL Server Express のヘルプを参照して、使用中のバージョンのデータベースサイズの上限を確認します。管理サーバーのデータベースが、もうすぐこのデータベースサイズの上限に達する可能性があります。 • 管理サーバーデータベースに保存されるイベントの数を制限してください。 • 管理サーバーデータベースにアプリケーションコントロールコンポーネントから送信されたイベントの数が多すぎます。これには、管理サーバーデータベースでのアプリケーションコントロールイベントの保管期間に関する Kaspersky Endpoint Security for Windows ポリシーの設定を変更することで対応できます。 SQL Server Express Edition 以外の DBMS を使用している場合：	90 日間

			• 管理サーバーのデータベースに保存されるイベントの数を制限しないでください • 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください DBMS の選定に関する情報を確認します。	
セカンダリ管理サーバーとの接続が中断されました	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	この種別のイベントは、セカンダリ管理サーバーへの接続が中断された場合に発生します。 セカンダリ管理サーバーがインストールされているデバイスの Kaspersky イベントログを読み、適宜対応します。	90 日間
プライマリ管理サーバーとの接続が中断されました	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	この種別のイベントは、プライマリ管理サーバーへの接続が中断された場合に発生します。 プライマリ管理サーバーがインストールされているデバイスの Kaspersky イベントログを読み、適宜対応します。	90 日間
カスペルスキー製品モジュールの新しいアップデートが登録されました	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	この種別のイベントは、インストールの承認が必要な管理対象デバイスにインストールされているカスペルスキーソフトウェアの新しいアップデートを管理サーバーが登録する場合に発生します。 管理コンソールまたは Kaspersky Security Center Web コンソールを使用して、アップデートを承認または拒否します。	90 日間
データベースのイベントの上限数を超えました。イベントの削除が開始されました	4145	KLSRV_EVP_DB_TRUNCATING	この種別のイベントは、管理サーバーのデータベース容量が上限に達して、データベース内の古いイベントの削除が開始された時に記録されます。 このイベントには、次の方法で対応できます： • 管理サーバーデータベースに保管されるイベント数の上限を変更してください • 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください	保管されません
データベースのイベントの上限数を超えました。このイベントは削除されました	4146	KLSRV_EVP_DB_TRUNCATED	この種別のイベントは、管理サーバーのデータベース容量が上限に達して、データベース内の古いイベントが削除された時に記録されます。 このイベントには、次の方法で対応できます： • 管理サーバーデータベースに保管できるイベント数の上限を変更してください • 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください	保管されません

管理サーバーの情報イベント

次の表は、重要度が「**情報**」に分類される Kaspersky Security Center 管理サーバーのイベントを示します。

管理サーバーの情報イベント

イベント種別の表示名	イベント種別の ID	イベント種別	既定の保管期間	備考
ライセンス使用率が 90% を超えています	4097	KLSRV_EV_LICENSE_CHECK_90	30 日間	
新しいデバイスが検出されました	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 日間	
デバイスが自動的にグループに追加されました	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 日間	
デバイスがルールに従って自動的に移動されました	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 日間	

デバイスがグループから削除されました：ネットワーク上で長期間アクティブになっていません	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 日間	
インストール数が上限に近づいている（95% を超える数を使用済み）ライセンス認証済みアプリケーショングループがあります	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 日間	
カスペルスキーへ分析のために送付するファイルが見つかりました	4131	KLSRV_APS_FILE_APPEARED	30 日間	
このモバイルデバイス上で FCM 送信者 ID が変更されました	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 日間	
指定のフォルダーにアップデートがコピーされました	4122	KLSRV_UPD_REPL_OK	30 日間	
セカンダリ管理サーバーとの接続が確立されました	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 日間	
プライマリ管理サーバーとの接続が確立されました	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 日間	
定義データベースがアップデートされました	4144	KLSRV_UPD_BASES_UPDATED	30 日間	
監査：管理サーバーとの接続が確立されました	4147	KLAUD_EV_SERVERCONNECT	30 日間	
監査：オブジェクトが変更されました	4148	KLAUD_EV_OBJECTMODIFY	30 日間	このイベントは次のオブジェクトの変更を追跡します： • 管理グループ • セキュリティグループ • ユーザー • パッケージ • タスク • ポリシー • サー

				バー • 仮想サーバー
監査：オブジェクトのステータスが変更されました	4150	KLAUD_EV_TASK_STATE_CHANGED	30 日間	たとえば、このイベントはタスクがエラーで失敗した時に発生します。
監査：グループ設定が変更されました	4149	KLAUD_EV_ADMGROUP_CHANGED	30 日間	
監査：管理サーバーへの接続が切断されました	4151	KLAUD_EV_SERVERDISCONNECT	30 日間	
監査：オブジェクトのプロパティが変更されました	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 日間	このイベントは、次のプロパティの変更を追跡します： • ユーザー • ライセンス • サーバー • 仮想サーバー
監査：ユーザーの権限が変更されました	4153	KLAUD_EV_OBJECTACLMODIFIED	30 日間	
監査：管理サーバーから暗号化キーがインポートまたはエクスポートされました	5100	KLAUD_EV_DPEKEYSEXPORT	30 日間	

ネットワークエージェントのイベント

このセクションには、ネットワークエージェントに関するイベントの情報が記載されています。

ネットワークエージェントの機能エラーイベント

次の表は、重要度が「**機能エラー**」に分類される Kaspersky Security Center ネットワークエージェントのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

ネットワークエージェントの機能エラーイベント

イベント種別の表示名	イベント種別の ID	イベント種別	説明	既定の保管期間
アップデートのインストールエラー	7702	KLNAG_EV_PATCH_INSTALL_ERROR	この種別のイベントは、Kaspersky Security Center コンポーネントの自動アップデートおよびパッチ適用に失敗した時に記録されます。このイベントは、管理対象のカスペルスキー製品のアップデートとの関連はありません。 イベントの説明を確認します。管理サーバーで Windows 関連の問題がこのイベントの原因となっている可能性があります。イベントの説明で Windows の設定に関する問題が言及されている場合、その問題を解決してください。	30 日間
サードパーティ製品のアップデートをインストールできませんでした	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	この種別のイベントは、脆弱性とパッチ管理とモバイルデバイス管理を使用していて、サードパーティ製品のアップデートに失敗した時に記録されます。 サードパーティ製品へのリンクが有効かどうかを確認します。イベントの説明を確認します。	30 日間
Windows Update 更新プログラムをインストールできませんでした	7717	KLNAG_EV_WUA_INSTALL_ERROR	この種別のイベントは、Windows の更新プログラムの適用に失敗した時に記録されます。ネットワークエージェントポリシーで Windows アップデートの設定を行ってください。 イベントの説明を確認します。該当するエラーに関する説明がマイクロソフト サポート技術情報で提供されていないかを検索してください。問題の解決が困難な場合は、マイクロソフトのテクニカルサポートにお問い合わせください。	30 日間
ユーザー管理：エラー	7723	KLNAG_EV_USR_MNG_ERR	一般警告イベント。	30 日間
Sudo ファイルを参照値に復元できませんでした	7726	KLNAG_EV_SUDOER_RESTORED_ERR	イベントには、ファイル sudoers の置換エラーの説明が含まれています。	30 日間
ルート証明書をインストールできませんでした	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	イベントには、証明書のインストールエラーの説明が含まれます。	30 日間
ルート証明書を削除できません	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	イベントには、証明書削除エラーの説明が含まれます。	30 日間

ネットワークエージェントの警告イベント

次の表は、重要度が「**警告**」に分類される Kaspersky Security Center のネットワークエージェントのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

ネットワークエージェントの警告イベント

イベント種別の表示名	イベント種別の ID	イベント種別	既定の保管期間
ソフトウェアモジュールのアップデートのインストール中に警告が発生しました	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 日間
サードパーティ製品のアップデートのインストールが警告を出力して完了しました	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 日間
サードパーティ製品のアップデートのインストールが延期されました	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 日間
セキュリティ問題が発生しました	549	GNRL_EV_APP_INCIDENT_OCCURED	30 日間
KSN プロキシサーバーが起動しました。KSN 可用性をチェックできませんでした	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 日間
ユーザー管理：警告	7722	KLNAG_EV_USR_MNG_WRN	30 日間
検出された Sudo ファイルは参照値と一致しません	7724	KLNAG_EV_SUDOER_DIFFERENT	30 日間

ネットワークエージェントの情報イベント

次の表は、重要度が「**情報**」に分類される Kaspersky Security Center のネットワークエージェントのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

ネットワークエージェントの情報イベント

イベント種別の表示名	イベント種別の ID	イベント種別	既定の保管期間
ソフトウェアモジュールのアップデートがインストールされました	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 日間
ソフトウェアモジュールのアップデートのインストールを開始しました	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 日間
アプリケーションがインストールされました	7703	KLNAG_EV_INV_APP_INSTALLED	30 日間
アプリケーションがアンインストールされました	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 日間
監視対象アプリケーションがインストールされました	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 日間
監視対象アプリケーションがアンインストールされました	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 日間
サードパーティ製品がインストールされました	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 日間
新しいデバイスが追加されました	7708	KLNAG_EV_DEVICE_ARRIVAL	30 日間
デバイスが削除されました	7709	KLNAG_EV_DEVICE_REMOVE	30 日間
新しいデバイスが検出されました	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 日間
デバイスが認証されました	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 日間
Windows デスクトップ共有：ファイルが読み取られま	7712	KLUSRLOG_EV_FILE_READ	30 日

した			間
Windows デスクトップ共有：ファイルが変更されました	7713	KLUSRLOG_EV_FILE_MODIFIED	30 日間
Windows デスクトップ共有：アプリケーションが起動しました	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 日間
Windows デスクトップ共有：開始しました	7715	KLUSRLOG_EV_WDS_BEGIN	30 日間
Windows デスクトップ共有：停止しました	7716	KLUSRLOG_EV_WDS_END	30 日間
サードパーティ製品のアップデートがインストールされました	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 日間
サードパーティ製品のアップデートのインストールを開始しました	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 日間
KSN プロキシサーバーが起動しました。KSN 可用性チェックが完了しました	7719	KSNPROXY_STARTED_CON_CHK_OK	30 日間
KSN プロキシが停止しました	7720	KSNPROXY_STOPPED	30 日間

iOS MDM サーバーイベント

このセクションには、iOS MDM サーバーに関するイベントの情報が記載されています。

iOS MDM サーバーの機能エラーイベント

次の表は、重要度が「**機能エラー**」に分類される Kaspersky Security Center iOS MDM サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

iOS MDM サーバーの機能エラーイベント

イベント種別の表示名	イベント種別	既定の保管期間
プロファイルのリストをリクエストできませんでした	PROFILELIST_COMMAND_FAILED	30 日間
プロファイルをインストールできませんでした	INSTALLPROFILE_COMMAND_FAILED	30 日間
プロファイルを削除できませんでした	REMOVEPROFILE_COMMAND_FAILED	30 日間
プロビジョニングプロファイルのリストをリクエストできませんでした	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 日間
プロビジョニングプロファイルをインストールできませんでした	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 日間
プロビジョニングプロファイルを削除できませんでした	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 日間
デジタル証明書のリストをリクエストできませんでした	CERTIFICATELIST_COMMAND_FAILED	30 日間
インストール済みアプリケーションのリストをリクエストできませんでした	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 日間
モバイルデバイスに関する一般情報をリクエストできませんでした	DEVICEINFORMATION_COMMAND_FAILED	30 日間
セキュリティ情報をリクエストできませんでした	SECURITYINFO_COMMAND_FAILED	30 日間
モバイルデバイスをロックできませんでした	DEVICELOCK_COMMAND_FAILED	30 日間
パスワードをリセットできませんでした	CLEARPASSCODE_COMMAND_FAILED	30 日間

モバイルデバイスのデータを消去できませんでした	ERASEDEVICE_COMMAND_FAILED	30 日間
アプリをインストールできませんでした	INSTALLAPPLICATION_COMMAND_FAILED	30 日間
アプリのリデンプションコードを設定できませんでした	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 日間
管理対象アプリのリストをリクエストできませんでした	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 日間
管理対象アプリを削除できませんでした	REMOVEAPPLICATION_COMMAND_FAILED	30 日間
ローミング設定が拒否されました	SETROAMINGSETTINGS_COMMAND_FAILED	30 日間
アプリの動作でエラーが発生しました	PRODUCT_FAILURE	30 日間
コマンドの結果に無効なデータが含まれています	MALFORMED_COMMAND	30 日間
プッシュ通知を送信できませんでした	SEND_PUSH_NOTIFICATION_FAILED	30 日間
コマンドを送信できませんでした	SEND_COMMAND_FAILED	30 日間
デバイスが見つかりません	DEVICE_NOT_FOUND	30 日間

iOS MDM サーバーの警告イベント

次の表は、重要度が「**警告**」に分類される Kaspersky Security Center iOS MDM サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

iOS MDM サーバーの警告イベント

イベント種別の表示名	イベント種別	既定の保管期間
ロックされたモバイルデバイスを接続する試行を検出しました	INACTICE_DEVICE_TRY_CONNECTED	30 日間
プロファイルが削除されました	MDM_PROFILE_WAS_REMOVED	30 日間
クライアント証明書を再使用する試行を検出しました	CLIENT_CERT_ALREADY_IN_USE	30 日間
非アクティブなデバイスを検出しました	FOUND_INACTIVE_DEVICE	30 日間
リデンプションコードが必要です	NEED_REDEMPTION_CODE	30 日間
デバイスから削除されたポリシーにプロファイルが含まれていました	UMDM_PROFILE_WAS_REMOVED	30 日間

iOS MDM サーバーの情報イベント

次の表は、重要度が「**情報**」に分類される Kaspersky Security Center iOS MDM サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

iOS MDM サーバーの情報イベント

イベント種別の表示名	イベント種別	既定の保管期間
新しいモバイルデバイスが接続されました	NEW_DEVICE_CONNECTED	30 日間
プロファイルのリストをリクエストしました	PROFILELIST_COMMAND_SUCCESSFULL	30 日間
プロファイルがインストールされました	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 日間

プロファイルが削除されました	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 日間
プロビジョニングプロファイルのリストをリクエストしました	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 日間
プロビジョニングプロファイルがインストールされました	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 日間
プロビジョニングプロファイルが削除されました	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 日間
デジタル証明書のリストをリクエストしました	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 日間
インストール済みアプリケーションのリストをリクエストしました	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 日間
モバイルデバイスに関する一般情報をリクエストしました	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 日間
セキュリティ情報をリクエストしました	SECURITYINFO_COMMAND_SUCCESSFULL	30 日間
モバイルデバイスをロックしました	DEVICELOCK_COMMAND_SUCCESSFULL	30 日間
パスワードがリセットされました	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 日間
データがモバイルデバイスから削除されました	ERASEDEVICE_COMMAND_SUCCESSFULL	30 日間
アプリがインストールされました	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 日間
アプリのリデンプションコードが設定されました	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 日間
管理対象アプリのリストをリクエストしました	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 日間
管理対象アプリが削除されました	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 日間
ローミング設定が適用されました	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 日間

頻出イベントのブロック

このセクションでは、頻出イベントに関する情報、また頻出イベントのブロックおよびブロック解除、および頻出イベントのリストをファイルにエクスポートする方法について説明します。

頻出イベントのブロックについて

単一または複数の管理対象デバイスにインストールされた Kaspersky Endpoint Security for Windows などの管理対象アプリケーションは、管理サーバーに対して同様の種別のイベントを大量に送信することがあります。頻出イベントを受信すると、管理サーバーのデータベース高負荷がかかり、他のイベントが上書きされる場合があります。管理サーバーは、受信したイベントの総量がデータベースで指定した制限を超えた場合、頻出イベントをブロックします。

管理サーバーは頻出イベントの受信を自動的にブロックします。ユーザー自身による頻出イベントのブロックや、ブロックするイベントの選択はできません。

イベントがブロックされているかどうかをチェックしたい場合、そのイベントが管理サーバーのプロパティの［**頻出イベントのブロック**］セクションに存在するかどうかを確認できます。イベントがブロックされている場合、次を実行します：

- データベースの上書きを防止したい場合、このような種別のイベントの受信のブロックを継続できます。
- たとえば、管理サーバーに頻出イベントが送信される原因を見つける場合などには、頻出イベントのブロックを解除してこの種別のイベントの受信を継続できます。
- 頻出イベントの受信が再度ブロックされるまで受信を継続する場合は、頻出イベントのブロック対象から削除することができます。

頻出イベントのブロックの管理

管理サーバーは頻出イベントの受信を自動的にブロックしますが、ブロックを解除してイベントの受信を継続することができます。また、以前にブロック解除したイベントを再度ブロックすることもできます。

頻出イベントのブロックを管理するには：

1. Kaspersky Security Center のコンソールツリーで、［**管理サーバー**］フォルダーのコンテキストメニューを開いて、［**プロパティ**］を選択します。
2. 管理サーバーのプロパティウィンドウの［**セクション**］ペインに移動して、［**頻出イベントのブロック**］を選択します。
3. ［**頻出イベントのブロック**］セクションで次の操作を実行します：
   - 受信をブロックするイベントの［**イベント種別**］をオンにします。
   - 受信するイベントの［**イベント種別**］をオフにします。
4. ［**適用**］をクリックします。
5. ［**OK**］をクリックします。

管理サーバーは、［**イベント種別**］をオフにした頻出イベントを受信し、［**イベント種別**］をオンにした頻出イベントの受信をブロックします。

頻出イベントのブロックの解除

頻出イベントのブロックを解除して、管理サーバーが再度ブロックするまでイベントを受信できます。

頻出イベントのブロックを解除するには：

1. Kaspersky Security Center のコンソールツリーで、［**管理サーバー**］フォルダーのコンテキストメニューを開いて、［**プロパティ**］を選択します。
2. 管理サーバーのプロパティウィンドウの［**セクション**］ペインに移動して、［**頻出イベントのブロック**］を選択します。
3. ［**頻出イベントのブロック**］セクションで、ブロックを解除するイベントの行をクリックします。
4. ［**削除**］をクリックします。

イベントは頻出イベントのリストから削除されます。管理サーバーはこの種別のイベントを受信します。

頻出イベントのリストのファイルへのエクスポート

頻出イベントのリストをファイルにエクスポートするには：

1. Kaspersky Security Center のコンソールツリーで、［**管理サーバー**］フォルダーのコンテキストメニューを開いて、［**プロパティ**］を選択します。

2. 管理サーバーのプロパティウィンドウの［**セクション**］ペインに移動して、［**頻出イベントのブロック**］を選択します。

3. ［**ファイルへのエクスポート**］をクリックします。

4. 表示される［**名前を付けて保存**］ウィンドウで、リストの保存先となるファイルのパスを指定します。

5. ［**保存**］をクリックします。

すべての頻出イベントのリストの記録がファイルにエクスポートされます。

仮想マシンのステータスの変更管理

管理サーバーは、ハードウェアレジストリやインストールされているアプリケーションのリストなど管理対象デバイスのステータスと、管理対象のアプリケーション、タスク、ポリシーの設定に関する情報を保存します。仮想マシンが管理対象デバイスとして動作している場合、ユーザーが以前に作成した仮想マシンのスナップショットを使用して仮想マシンのステータスを復元することがあります。管理サーバー上の仮想マシンのステータスに関する情報が、最新でなくなることがあります。

たとえば、管理者が午後 12:00 に管理サーバーで保護ポリシーを作成し、午後 12:01 に仮想マシン VM_1 でその保護ポリシーを開始します。午後 12:30 に仮想マシン VM_1 のユーザーが、午前 11:00 に作成されたスナップショットを復元して仮想マシンのステータスを変更します。この場合、仮想マシンでの保護ポリシーの適用が停止します。ただし、管理サーバーに保管される古くなった情報には、仮想マシン VM_1 では保護ポリシーの適用が継続していることが示されます。

Kaspersky Security Center により、仮想マシンのステータスの変更を監視することができます。

デバイスとの同期後に毎回、管理サーバーは固有 ID を生成し、その固有 ID はデバイスと管理サーバーに保管されます。次の同期開始前に、管理サーバーは両方の ID を比較します。ID が一致しない場合、管理サーバーは仮想マシンがスナップショットから復元されたと認識します。管理サーバーは、仮想マシン側でアクティブなポリシーおよびタスクの設定をすべてリセットし、最新のポリシーとグループタスクのリストを仮想マシンに送信します。

システムレジストリの情報を使用したアンチウイルスによる保護ステータスの監視

クライアントデバイスのオペレーティングシステム種別に応じて、ネットワークエージェントによって記録された情報を使用してクライアントデバイス上のアンチウイルスによる保護ステータスをモニターするには：

- Windows で動作しているデバイスの場合：

  1. クライアントデバイスのシステムレジストリを開きます（たとえば、ローカルで［**スタート**］→［**ファイル名を指定して実行**］で regedit コマンドを使用します）。

  2. 次のレジストリエントリに移動します：

     - 32 ビットシステム：

       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

- 64 ビットシステム：

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Stati

  クライアントデバイスのアンチウイルスによる保護ステータス情報がシステムレジストリに表示されます。

- Linux で動作しているデバイスの場合：

  - データの種別ごとに 1 ファイルずつ、情報が「/var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/」のテキストファイルに保存されています。

- macOS で動作しているデバイスの場合：

  - データの種別ごとに 1 ファイルずつ、情報が「/Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/」のテキストファイルに保存されています。

アンチウイルスによる保護ステータスは、次の表で説明するキーの値に対応します：

レジストリキーと可能な値

キー（データ種別）	値	説明
Protection_LastConnected (REG_SZ)	DD-MM-YYYY HH-MM-SS	前回の管理サーバー接続日時（UTC 形式）
Protection_AdmServer (REG_SZ)	IP、DNS 名、NetBIOS 名のいずれか	デバイスを管理する管理サーバーの名前
Protection_NagentVersion (REG_SZ)	a.b.c.d	デバイスにインストールされているネットワークエージェントのビルド番号
Protection_NagentFullVersion (REG_SZ)	a.b.c.d (patch1; patch2; ...; patchN)	デバイスにインストールされているネットワークエージェントのバージョン（パッチまで含む完全な数字）
Protection_HostId (REG_SZ)	デバイス ID	デバイスの ID
Protection_DynamicVM (REG_DWORD)	0 — いいえ 1 — はい	ネットワークエージェントが VDI 向けダイナミックモードでインストールされている
Protection_AvInstalled (REG_DWORD)	0 — いいえ 1 — はい	セキュリティ製品がデバイスにインストールされている
Protection_AvRunning (REG_DWORD)	0 — いいえ 1 — はい	デバイスでリアルタイム保護が有効になっている
Protection_HasRtp (REG_DWORD)	0 — いいえ 1 — はい	リアルタイム保護がインストールされている
Protection_RtpState (REG_DWORD)	リアルタイム保護のステータス：	
	0	不明
	1	無効
	2	一時停止
	3	開始中
	4	有効
	5	有効、保護レベル高（最大の保護）
	6	有効、保護レベル低（速度重視）
	7	有効、既定の設定（推奨設定）を適用
	8	有効、カスタム設定を適用
	9	動作エラー

Protection_LastFscan (REG_SZ)	DD-MM-YYYY HH-MM-SS	前回の完全スキャン実行日時（UTC 形式）
Protection_BasesDate (REG_SZ)	DD-MM-YYYY HH-MM-SS	定義データベースの公開日時（UTC 形式）

デバイスが不可視の時の処理の表示と設定

グループ内のクライアントデバイスがアクティブでない場合、通知を受け取ることができます。こうしたデバイスを自動的に削除することもできます。

グループ内のデバイスがアクティブでない場合の処理を表示したり設定するには：

1. コンソールツリーで、目的の管理グループの名前を右クリックします。
2. コンテキストメニューから［**プロパティ**］を選択します。
   管理グループのプロパティウィンドウが開きます。
3. ［**プロパティ**］ウィンドウで、［**デバイス**］セクションに移動します。
4. 必要に応じて、次のオプションの有効と無効を切り替えます：

- **次の期間デバイスが不可視の場合管理者に通知（日）**

  このオプションをオンにすると、管理者が非アクティブなデバイスについて通知を受け取ります。［**デバイスがネットワーク上で長期間アクティブになっていません**］イベントが作成されるまでの期間を指定できます。既定の期間は 7 日です。

  既定では、このオプションはオンです。

- **次の期間デバイスが不可視の場合グループから削除（日）**

  このオプションをオンにすると、デバイスをグループから自動的に削除するまでの期間を指定できます。既定の期間は 60 日です。

  既定では、このオプションはオンです。

- **親グループから継承する**

  クライアントデバイスが属する親グループからこのセクションの設定が継承されます。このオプションをオンにすると、［**ネットワーク上のデバイスのアクティビティ**］の設定がロックされ変更できなくなります。

  このオプションは管理グループに親グループが存在する場合にのみ利用できます。

  既定では、このオプションはオンです。

- **子グループへ強制的に継承する**

  設定値が子グループに配信され、子グループのプロパティではそれらの設定がロックされます。

  既定では、このオプションはオフです。

5. ［**OK**］をクリックします。

変更内容が保存され、適用されます。

カスペルスキーからの通知を無効にする

Kaspersky Security Center Web コンソールでは、カスペルスキーからの通知セクション（［**監視とレポート**］→［**カスペルスキーからの通知**］）には、Kaspersky Security Center のバージョンと、管理対象デバイスにインストールされている管理対象アプリケーションに関連する情報が提供されます。通知が必要ない場合は、この機能を無効にできます。

カスペルスキーからの通知には、セキュリティに関するものとマーケティングに関するものの 2 種類の情報があります。これらのお知らせは、種類ごとに無効にできます。

セキュリティ関連告知を無効にするには：

1. コンソールツリーで、セキュリティ関連告知を無効にする管理サーバーを選択します。
2. 表示されるコンテキストメニューを右クリックして、［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウが表示されるので、［**カスペルスキーからの通知**］セクションで［**カスペルスキーからの通知の表示を Kaspersky Security Center Web コンソールで有効にする**］を無効にします。
4. ［**OK**］をクリックします。

カスペルスキーからの通知が無効になります。

マーケティング関連の告知は既定で無効になっています。マーケティング関連の告知は Kaspersky Security Network (KSN) を有効にした場合のみ受け取ります。KSN を無効にすることでこの種類のお知らせは無効にできます。

ディストリビューションポイントと接続ゲートウェイの調整

Kaspersky Security Center の管理グループ構造では、次の機能が実行されます：

- ポリシー範囲の設定

  関連する設定をデバイスに適用する別の方法として、*ポリシーのプロファイル*を使用する方法があります。この場合、ポリシーの範囲は、タグ、Active Directory 組織単位内のデバイスの場所、またはActive Directory セキュリティグループの所属で設定します。

- グループタスク範囲の設定

  管理グループの階層に基づいていない、グループタスク範囲の定義方法が存在します。これは、デバイス選択用のタスクと特定のデバイス用のタスクを使用することです。

- デバイス、仮想管理サーバー、およびセカンダリ管理サーバーへのアクセス権限の設定

- ディストリビューションポイントの割り当て

管理グループ構造を構築する際には、ディストリビューションポイントを最適に割り当てるために、組織ネットワークのトポロジーを考慮する必要があります。ディストリビューションポイントを最適に分散配置すると、組織ネットワークのトラフィック量を軽減できます。

組織の組織図とネットワークトポロジーに応じて、管理グループ構造に次の標準設定を適用できます：

- 単一のオフィス
- 複数の小規模なリモートオフィス

ディストリビューションポイントとして動作するデバイスについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

ディストリビューションポイントの標準設定：単一のオフィス

標準の「単一のオフィス」設定では、すべてのデバイスが組織ネットワーク内に置かれているため、お互いを「見る」ことができます。組織ネットワークは、いくつかの部分に区切られ（ネットワークまたはネットワークセグメント）、狭い帯域幅によって連結されるかたちで構成されている場合があります。

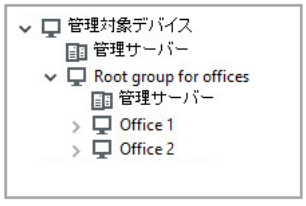
管理グループの構造は、次の方法で構築することが可能です：

- ネットワークトポロジーを考慮に入れて管理グループの構造を構築します。管理グループの構造が、厳密にネットワークトポロジーを反映していなくても問題ありません。ネットワークが区切られた各部分と特定の管理グループの間に一致があれば十分です。ディストリビューションポイントの自動割り当てを使用するか、または手動で割り当てることができます。
- ネットワークトポロジーを考慮に入れずに管理グループの構造を構築します。この場合は、ディストリビューションポイントの自動割り当てを無効にしてから、ディストリビューションポイントとして動作する1台以上のデバイスをネットワークの区切られた各部分のルート管理グループ（たとえば、**管理対象デバイス**グループ）に対して割り当てる必要があります。ディストリビューションポイントは、すべて同じレベルに置かれ、組織ネットワーク内のすべてのデバイスを包含する同じ範囲を対象とします。この場合、各ネットワークエージェントは最短経路のディストリビューションポイントに接続します。ディストリビューションポイントへの経路は、tracert ユーティリティによって追跡できます。

ディストリビューションポイントの標準設定：複数の小規模なリモートオフィス

この標準設定は、インターネットを介して本社と通信する可能性のある多数の小規模なリモートオフィス向けの設定です。各リモートオフィスは NAT を介するようにその背後に配置されています。つまり、2 つのオフィスはお互いに分離されているため、お互いに接続することはできません。

管理グループ構造内で設定を反映させる必要があります。つまり、各リモートオフィスに対して、個別の管理グループを作成する必要があります（下の図のグループ［**Office 1**］と［**Office 2**］）。



管理グループ構造に含まれているリモートオフィス

1つのオフィスに対応する各管理グループに対して、1つまたは複数個のディストリビューションポイントを割り当てる必要があります。ディストリビューションポイントは、空きディスク容量が十分なリモートオフィスにあるデバイスである必要があります。たとえば、［**Office 1**］グループに導入されているデバイスは、［**Office 1**］管理グループに割り当てられているディストリビューションポイントにアクセスできます。

ノート PC を持ち運んでオフィス間を移動するユーザーが存在する場合は、各リモートオフィスで 2 台以上のデバイス（既存のディストリビューションポイントに加えて）を選択し、それらのデバイスをトップレベルの管理グループ（上の図の［**Root group for offices**］）用のディストリビューションポイントとして動作するように割り当てる必要があります。

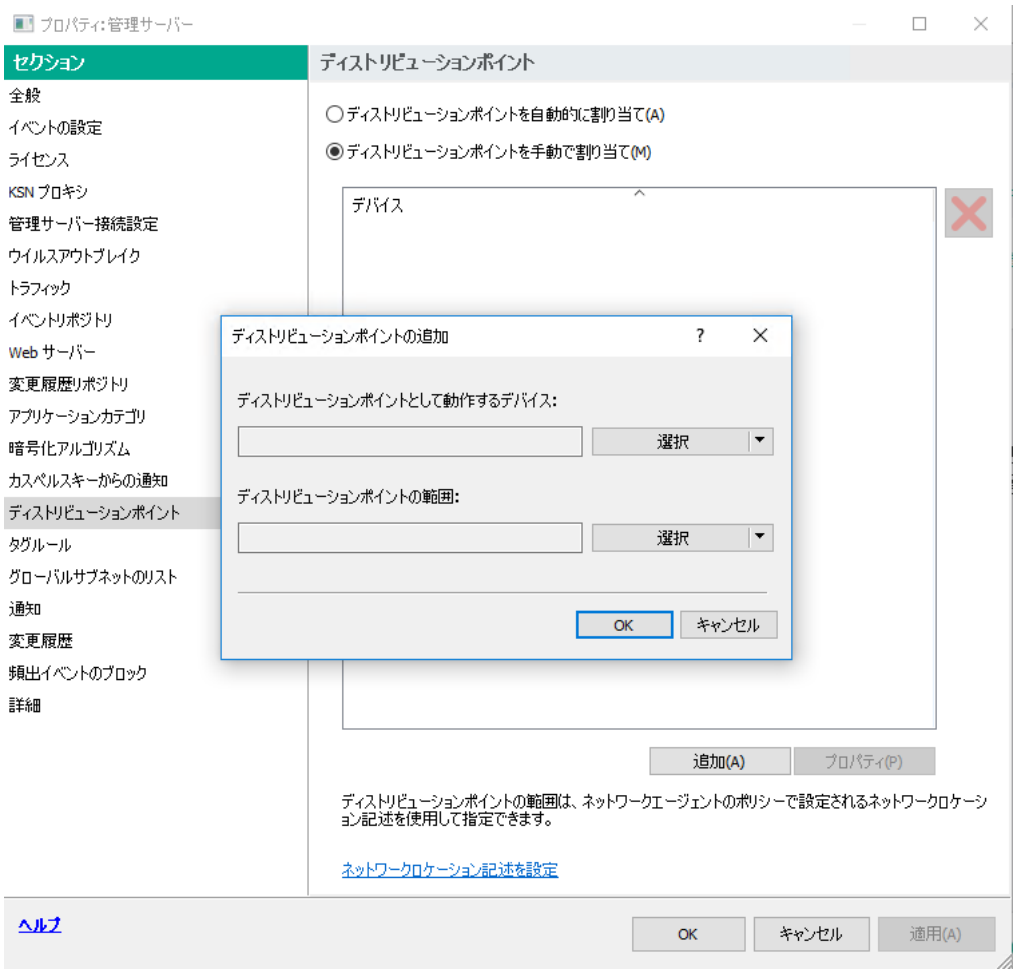
例：［**Office 1**］管理グループ内にノート PC を導入しましたが、［**Office 2**］管理グループに対応するオフィスにマシンを持って移動するとします。ノート PC を移動させると、ネットワークエージェントは［**Office 1**］グループに割り当てられているネットワークエージェントへのアクセスを試行しますが、これらのディストリビューションポイントは使用不可の状態です。次に、ネットワークエージェントは、［**Root group for offices**］に割り当てられているディストリビューションポイントへのアクセスの試行を開始します。リモートオフィスはお互いに分離されているため、［**Root group for offices**］管理グループに割り当てられているディストリビューションポイントへのアクセスの試行は、ネットワークエージェントが［**Office 2**］グループ内にあるディストリビューションポイントへのアクセスを試行した際にのみ正常に実行されます。つまり、ノート PC は最初のオフィスに対応する管理グループ内に残りますが、ディストリビューションポイントについては移動後のオフィスに存在するディストリビューションポイントを使用します。

ディストリビューションポイントとして動作する管理対象デバイスの割り当て

デバイスを管理グループ向けのディストリビューションポイントとして動作するように手動で割り当てたり、管理コンソールの接続ゲートウェイとして設定したりすることができます。

デバイスを管理グループのディストリビューションポイントに割り当てるには：

1. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウで［**ディストリビューションポイント**］セクションを選択します。
4. ウィンドウの右側で、［**ディストリビューションポイントを手動で割り当て**］をオンにします。
5. ［**追加**］をクリックします。



ディストリビューションポイントの手動での割り当て

［**ディストリビューションポイントの追加**］ウィンドウが表示されます。

6. ［**ディストリビューションポイントの追加**］ウィンドウで、次の操作を実行します：

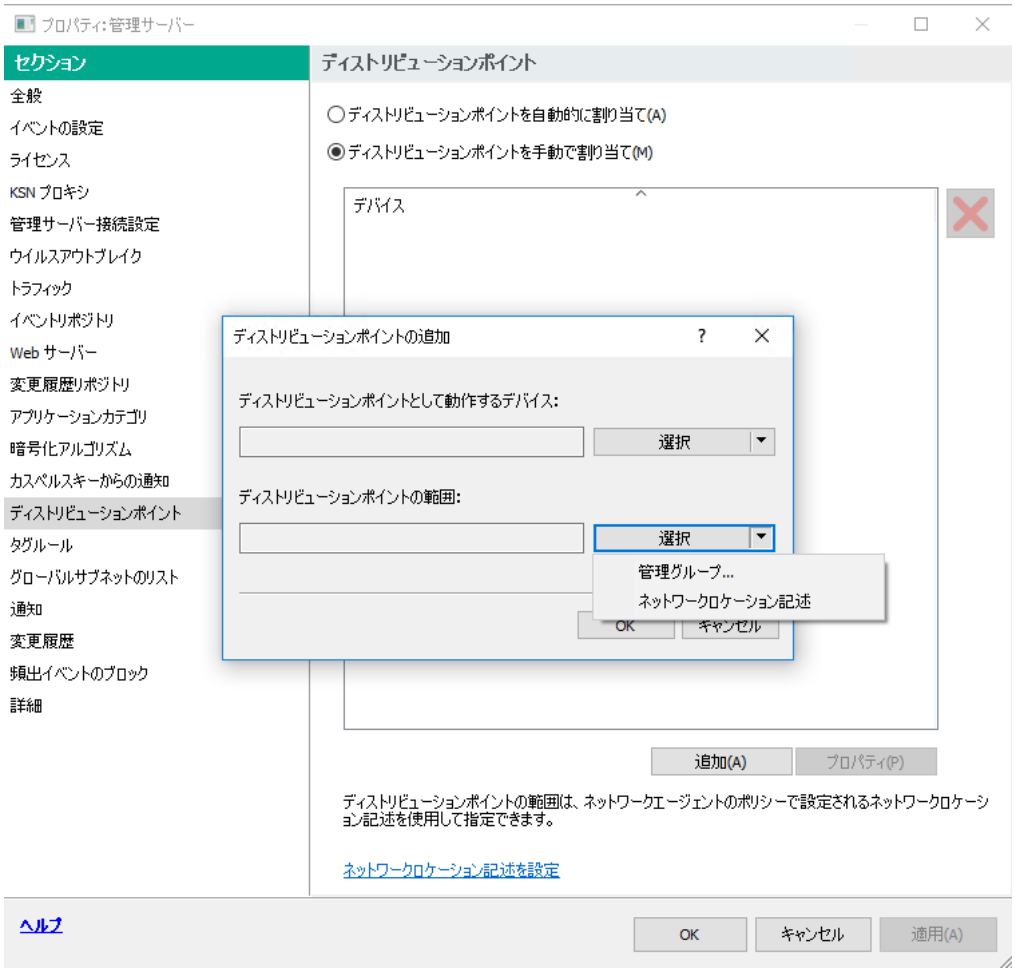
   a. ［**ディストリビューションポイントとして機能するデバイス**］で、［**選択**］にある下矢印（）をクリックします。**グループからデバイスを追加**をオンにします。

   b. 開いた［**デバイスの選択**］ウィンドウで、ディストリビューションポイントとして機能するデバイスをオンにします。

   c. ［**ディストリビューションポイントの範囲**］で、［**選択**］にある下矢印（）をクリックします。

   d. ディストリビューションポイントがアップデートを配信するデバイスを指定します。管理グループまたはネットワークロケーションの説明を指定できます。

   e. ［OK］をクリックして［**ディストリビューションポイントの追加**］ウィンドウを終了します。



ディストリビューションポイントの範囲の選択

追加されたディストリビューションポイントが、［**ディストリビューションポイント**］セクションのディストリビューションポイントのリストに表示されます。

ネットワークエージェントをインストールして仮想管理サーバーに最初に接続したデバイスが、ディストリビューションポイントとして動作するように自動的に割り当てられ、接続ゲートウェイとして設定されます。

非武装地帯のゲートウェイとして Linux デバイスを接続

Linux デバイスを非武装地帯（DMZ）のゲートウェイとして接続するには：

1. Linux デバイスにネットワークエージェントをダウンロードしてインストールします。
2. ポストインストールスクリプトを実行し、ウィザードに従ってローカル環境設定をセットアップします。
   コマンドプロンプトで、次のコマンドを実行します：
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```
3. ネットワークエージェントモードを要求するステップで、［**接続ゲートウェイとして使用する**］をオンにします。
4. 管理サーバーのコンテキストメニューにある MMC ベースの管理コンソールから［**プロパティ**］を選択します。

5. 開いた［管理サーバーのプロパティ］ウィンドウで、［**ディストリビューションポイント**］セクションを選択します。

6. 開いた［**ディストリビューションポイント**］ウィンドウの右側で：

   a. ［**ディストリビューションポイントを手動で割り当て**］をオンにします。

   b. ［**追加**］をクリックします。

   ［**ディストリビューションポイントの追加**］ウィンドウが表示されます。

7. ［**ディストリビューションポイントの追加**］ウィンドウで、次の操作を実行します：

   a. ［**ディストリビューションポイントとして機能するデバイス**］で、［**選択**］にある下矢印（）をクリックし、［**Add connection gateway in DMZ by address**］をオンにします。

   b. ［**ディストリビューションポイントの範囲**］で、［**選択**］にある下矢印（）をクリックします。

   c. ディストリビューションポイントがアップデートを配信するデバイスを指定します。管理グループを指定できます。

   d. ［**OK**］をクリックして［**ディストリビューションポイントの追加**］ウィンドウを終了します。

8. 追加されたディストリビューションポイントが、［**ディストリビューションポイント**］セクションのディストリビューションポイントのリストに表示されます。

9. Kaspersky Security Center への接続が正常に設定されているかどうかを確認するために klnagchk ユーティリティを実行します。コマンドプロンプトで、次のコマンドを実行します：
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

10. メインメニューで Kaspersky Security Center に移動し、デバイスを検出します。

11. ウィンドウが表示されたら、<デバイス名> をクリックします。

12. ドロップダウンリストで、［**グループへ移動**］を選択します。

13. 開いた［**グループの選択**］ウィンドウで、［**ディストリビューションポイント**］リンクをクリックします。

14. ［**OK**］をクリックします。

15. コマンドプロンプトで次のコマンドを実行して、Linux クライアントでネットワークエージェントサービスを再起動します。
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
   ```

Linux デバイスの DMZ のゲートウェイとしての接続が完了します。

その後、構成された接続ゲートウェイを介して Linux デバイスを管理サーバーに接続できるようになります。これらの手順は、メインのインストールシナリオを完了した後にのみ実行してください。

接続ゲートウェイを介して Linux デバイスを管理サーバーに接続

接続ゲートウェイを使用すると、クライアントデバイスを非武装地帯（DMZ）から管理サーバーに接続できます。Windows ベースおよび Linux ベースのデバイスは、接続ゲートウェイとして機能できます。接続ゲートウェイを接続して構成した後、このゲートウェイを使用して Linux デバイスを管理サーバーに接続できます。以下の手順は、メインのインストールシナリオが完了してから行ってください。

接続ゲートウェイを介して Linux デバイスを管理サーバーに接続するには、このデバイスで次の操作を実行します：

1. Linux デバイスにネットワークエージェントをダウンロードしてインストールします。
2. コマンドプロンプトで次のコマンドを実行して、ネットワークエージェントのポストインストールスクリプトを実行します。
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```
3. ネットワークエージェントモードを要求するステップで、［**接続ゲートウェイを使用してサーバーに接続する**］をオンにして、接続ゲートウェイのアドレスを入力します。
4. コマンドプロンプトで次のコマンドを使用して、Kaspersky Security Center および接続ゲートウェイとの接続を確認します：
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
   接続ゲートウェイアドレスが出力表示されます。

接続ゲートウェイを介した Linux デバイスの管理サーバーへの接続が完了しました。このデバイスを使用して、アプリケーションのリモートインストールの配信のアップデートや、ネットワークに接続されたデバイスに関する情報の収集が可能です。

DMZ にディストリビューションポイントとして接続ゲートウェイを追加

接続ゲートウェイは、管理サーバーへの接続を確立せず、管理サーバーからの接続を待機します。これは、接続ゲートウェイが DMZ 内のデバイスにインストールされた直後に、管理サーバーが管理対象デバイスの中にそのデバイスをリストしないことを意味します。したがって、管理サーバーが接続ゲートウェイへの接続を開始するようにするには、特別な手順が必要です。

接続ゲートウェイを持つデバイスをディストリビューションポイントとして追加するには：

1. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウで［**ディストリビューションポイント**］セクションを選択します。
4. ウィンドウの右側で、［**ディストリビューションポイントを手動で割り当て**］をオンにします。
5. ［**追加**］をクリックします。
   ［**ディストリビューションポイントの追加**］ウィンドウが表示されます。
6. ［**ディストリビューションポイントの追加**］ウィンドウで、次の操作を実行します：
   a. ［**ディストリビューションポイントとして機能するデバイス**］で、［**選択**］にある下矢印（▾）をクリックし、**アドレスに基づいて DMZ 内の接続ゲートウェイを追加**をオンにします。
   b. 表示される［**接続ゲートウェイアドレスの入力**］ウィンドウで、接続ゲートウェイの IP アドレスを入力します（または、接続ゲートウェイに名前でアクセスできる場合は名前を入力します）。

c. ［**ディストリビューションポイントの範囲**］で、［**選択**］にある下矢印（）をクリックします。

d. ディストリビューションポイントがアップデートを配信するデバイスを指定します。管理グループまたはネットワークロケーションの説明を指定できます。

外部管理対象デバイス用に別のグループを作成することを推奨します。

これらの処理の実行後には、ディストリビューションポイントのリストに、「**接続ゲートウェイの一時的な登録**」という名前の新しいエントリが含まれています。

管理サーバーは、指定したアドレスで接続ゲートウェイへの接続をほぼ即座に試行します。成功すると、エントリ名が接続ゲートウェイデバイスの名前に変わります。このプロセスには最大 5 分かかります。

接続ゲートウェイの一時的な登録が名前付きエントリに変換されている間、接続ゲートウェイは**未割り当てデバイス**グループにも表示されます。

以前に構成したネットワークに接続ゲートウェイを追加するには、新しく追加した接続ゲートウェイに接続するデバイスにネットワークエージェントを再インストールします。

ディストリビューションポイントの自動的な割り当て

ディストリビューションポイント用デバイスは、自動的に割り当てることを推奨します。自動で行う場合、ディストリビューションポイントに指定するデバイスを Kaspersky Security Center が選択します。

ディストリビューションポイントを自動的に割り当てるには：

1. メインウィンドウを開きます。
2. コンソールツリーで、ディストリビューションポイントを自動的に割り当てる必要がある管理サーバーの名前が付けられたフォルダーを選択します。
3. 管理サーバーのコンテキストメニューから［**プロパティ**］をクリックします。
4. 管理サーバーのプロパティウィンドウの［**セクション**］ペインで、［**ディストリビューションポイント**］を選択します。
5. ウィンドウの右側で、［**ディストリビューションポイントを自動的に割り当て**］をオンにします。

ディストリビューションポイントとしてのデバイスの自動割り当てが有効な場合、手動でディストリビューションポイントを設定したりディストリビューションポイントのリストを編集したりすることはできません。

6. ［OK］をクリックします。

管理サーバーが自動的にディストリビューションポイントを割り当てて設定します。

ディストリビューションポイントとして選択されたデバイスへのネットワークエージェントのローカルインストールについて

接続ゲートウェイとして動作するため、ディストリビューションポイントによって選択されたデバイスが仮想管理サーバーと直接通信できるようにするには、このデバイスにネットワークエージェントをローカルインストールする必要があります。

ディストリビューションポイントに割り当てたデバイスにネットワークエージェントをローカルインストールする手順は、その他のネットワークデバイスへのネットワークエージェントのローカルインストール手順と同じです。

ディストリビューションポイントとして選択されるデバイスは、次の条件を満たしている必要があります：

- ネットワークエージェントのローカルインストール時に、セットアップウィザードの［**管理サーバー**］ウィンドウの［**サーバーアドレス**］に、デバイスを管理する仮想管理サーバーのアドレスを入力します。デバイスの IP アドレスまたは Windows ネットワークでのデバイス名を使用できます。

  仮想管理サーバーのアドレスには次の構文が用いられます：<仮想サーバーが従属する物理管理サーバーのフルアドレス>/<仮想管理サーバーの名前>

- デバイスを接続ゲートウェイとして動作させるには、管理サーバーとの通信に必要なポートをすべて開きます。

指定した設定に従いネットワークエージェントをデバイスにインストールすると、Kaspersky Security Center は自動的に次のアクションを実行します：

- このデバイスを仮想管理サーバーの**管理対象デバイス**グループに含める
- このデバイスを仮想管理サーバーの**管理対象デバイス**グループのディストリビューションポイントに割り当てる

ネットワークエージェントは、組織のネットワーク上にある**管理対象デバイス**グループのディストリビューションポイントに割り当てたデバイスにローカルインストールする必要があります。ネットワークエージェントは、ネストされた管理グループでディストリビューションポイントとして動作するデバイスにリモートでインストールすることができます。これを実行するには、**管理対象デバイス**のディストリビューションポイントを接続ゲートウェイとして使用します。

ディストリビューションポイントの接続ゲートウェイとしての使用について

管理サーバーが DMZ（非武装地帯）の外にある場合、ネットワークエージェントが DMZ から管理サーバーに接続することはできません。

ネットワークエージェントを使用して管理サーバーに接続する場合、ディストリビューションポイントを接続ゲートウェイとして使用できます。ディストリビューションポイントは、接続を確立するために管理サーバーへのポートを開きます。管理サーバーが開始されると、管理サーバーはディストリビューションポイントに接続し、セッション中、この接続を維持します。

管理サーバーからの信号を受信すると、ディストリビューションポイントは管理サーバーへの接続を許可するために UDP 信号をネットワークエージェントに送信します。ネットワークエージェントはこの信号を受信すると、ディストリビューションポイントに接続し、ディストリビューションポイントはネットワークエージェントと管理サーバーとの間で情報を交換します。情報は IPv4 または IPv6 ネットワークで交換できます。

接続ゲートウェイには特定のデバイスを使用することを推奨します。また、その接続ゲートウェイに配置するクライアントデバイス（モバイルデバイスを含む）は 10,000 台以下とすることを推奨します。

以前に構成したネットワークに接続ゲートウェイを追加するには、次の手順を実行します：

1. ネットワークエージェントを接続ゲートウェイモードでインストールします。
2. 新しく追加した接続ゲートウェイに接続するデバイスにネットワークエージェントを再インストールします。

ディストリビューションポイントによってポーリングされる範囲のリストに IP 範囲を追加します

ディストリビューションポイントがポーリングする範囲のリストに IP 範囲を追加できます。

ポーリング範囲のリストに IP 範囲を追加するには：

1. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。
2. フォルダーのコンテキストメニューで、［**プロパティ**］を選択します。
3. 開いた［管理サーバーのプロパティ］ウィンドウで、［**ディストリビューションポイント**］セクションを選択します。
4. リストから目的のディストリビューションポイントを選択し、［**プロパティ**］をクリックします。
5. ディストリビューションポイントのプロパティウィンドウが表示されたら、［**セクション**］ペインの左で、［**デバイスの検索**］→［**IP アドレス範囲**］の順に選択します。
6. ［**IP アドレス範囲のポーリングを有効にする**］をオンにします。
7. ［**追加**］をクリックします。
   ［**IP アドレス範囲のポーリングを有効にする**］がオンの場合のみ、［**追加**］が有効になります。
   ［**IP アドレス範囲**］ウィンドウが表示されます。
8. ［**IP アドレス範囲**］ウィンドウに、新しい IP アドレス範囲の名前を入力します（既定では「新規アドレス範囲」）。
9. ［**追加**］をクリックします。
10. 次のいずれかの手順を実行します：
    - 開始アドレスと終了アドレスを使用して IP アドレス範囲を指定する
    - アドレスとサブネットマスクを使用して IP アドレス範囲を指定する
    - ［**参照**］をクリックして、サブネットのグローバルリストからサブネットを追加する
11. ［**OK**］をクリックします。
12. ［**OK**］をクリックすると、指定した名前で新しい範囲が追加されます。

新しい範囲は、ポーリングされた範囲のリストに表示されます。

ディストリビューションポイントのプッシュサーバーとしての使用

Kaspersky Security Center で、ディストリビューションポイントをモバイルプロトコルを使用して管理されているデバイスおよび Network Agent により管理されているデバイスのプッシュサーバーとして動作させることができます。たとえば、KasperskyOS デバイスと管理サーバー間の強制同期を実行可能にする時に、プッシュサーバーを有効にする必要があります。プッシュサーバーの管理デバイスの範囲は、プッシュサーバーを有効にするディストリビューションポイントの範囲と同じです。同一の管理グループに複数のディストリビューションポイントを割り当てている場合は、各ディストリビューションポイントに対してプッシュサーバーを有効に設定できます。この場合、管理サーバーはディストリビューション間の負荷を分散します。

プッシュサーバーは、最大 50,000 件の同時接続の負荷をサポートします。

ディストリビューションポイントをプッシュサーバーとして使用して、管理対象デバイスと管理サーバー間の継続的な接続を確認できます。ローカルタスクの実行と停止、管理対象アプリケーションの統計の受信、トンネルの作成など、一部の操作には継続的な接続が必要です。ディストリビューションポイントをプッシュサーバーとして使用する場合は、管理対象デバイスで［**管理サーバーから切断しない**］をオンにしたり、ネットワークエージェントの UDP ポートにパケットを送信したりする必要はありません。

ディストリビューションポイントをプッシュサーバーとして使用するには：

1. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。
2. フォルダーのコンテキストメニューで、［**プロパティ**］を選択します。
3. 開いた［管理サーバーのプロパティ］ウィンドウで、［**ディストリビューションポイント**］セクションを選択します。
4. リストから目的のディストリビューションポイントを選択し、［**プロパティ**］をクリックします。
5. ディストリビューションポイントのプロパティウィンドウが表示されたら、［**全般**］セクション（［**セクション**ペインの左側）で、［**ディストリビューションポイントをプッシュサーバーとして使用する**］をオンにします。
6. プッシュサーバーのポート番号を指定します。ディストリビューションポイントのこのポートが、クライアントデバイスの接続に使用されます。

   既定では、ポート 13295 が使用されます。
7. ［OK］をクリックして、ディストリビューションポイントのプロパティウィンドウを閉じます。
8. ネットワークエージェントのポリシーの設定ウィンドウを開きます。
9. ［**接続**］セクションで、［**ネットワーク**］サブセクションへ移動します。
10. ［**ネットワーク**］サブセクションで、［**ディストリビューションポイントを使用して管理サーバーへ強制的に接続する**］をオンにします。
11. ［OK］をクリックして、ウィンドウを閉じます。

ディストリビューションポイントがプッシュサーバーとしての動作を開始します。クライアントデバイスへのプッシュ通知が送信可能になります。

KasperskyOS をデバイスにインストール済みか、インストールする予定がある場合、ディストリビューションポイントをプッシュサーバーとして使用する必要があります。クライアントデバイスへプッシュ通知を送信する場合も、ディストリビューションポイントをプッシュサーバーとして使用できます。

その他の定期作業

このセクションでは、Kaspersky Security Center での定期作業に関する推奨事項について説明します。

管理サーバーの管理

このセクションでは、管理サーバーの操作方法と設定方法について説明します。

管理サーバーの階層の作成：セカンダリ管理サーバーの追加

管理サーバーをセカンダリ管理サーバーとして追加し、プライマリとセカンダリの階層を確立することができます。セカンダリとしての使用を目的としている管理サーバーが、管理サーバーから接続可能であるかどうかに依存せず、セカンダリ管理サーバーの追加が可能です。

2 つの管理サーバーを 1 つの階層内で組み合わせる時は、ポート 13291 が両方の管理サーバーで開放されていることを確認してください。管理コンソールから管理サーバーへの接続を確立するには、ポート 13291 が必要です。

管理サーバーをセカンダリとしてプライマリ管理サーバーに接続する

管理サーバーをセカンダリとして追加するには、プライマリ管理サーバーのポート 13000 に接続します。プライマリ管理サーバーとセカンダリ管理サーバーの両方の管理サーバーに TCP ポート 13291 で接続できる管理コンソールがインストールされたデバイスが必要です。

管理コンソールから接続できる管理サーバーをセカンダリとして追加するには：

1. プライマリ管理サーバーとして指定する管理サーバーのポート 13000 にセカンダリ管理サーバーから接続できることを確認します。
2. 管理コンソールを使用してプライマリ管理サーバーに接続します。
3. セカンダリ管理サーバーを追加する管理グループを選択します。
4. 選択したグループの［**管理サーバー**］フォルダーの作業領域で［**セカンダリ管理サーバーの追加**］をクリックします。

   セカンダリ管理サーバー追加ウィザードが起動します。
5. ウィザードの最初のステップ（グループに追加する管理サーバーのアドレスの入力）で、セカンダリ管理サーバーのネットワーク名を入力します。
6. ウィザードの指示に従ってください。

プライマリとセカンダリの階層が構築されます。プライマリ管理サーバーがセカンダリ管理サーバーから接続されます。

両方の管理サーバーに TCP ポート 13291 でアクセスできる管理コンソールがインストールされたデバイスがない場合（たとえば、セカンダリ管理サーバーがリモートオフィスにあって、そのオフィスのシステム管理者がセキュリティ上の理由からポート 13291 をインターネットアクセスに対して開けない場合）でも、セカンダリ管理サーバーを追加できます。

管理コンソールから接続できない管理サーバーをセカンダリとして追加するには：

1. プライマリ管理サーバーのポート 13000 にセカンダリ管理サーバーから接続できることを確認します。
2. プライマリ管理サーバーの証明書ファイルを外付けドライブ（フラッシュドライブなど）に書き出すか、管理サーバーがあるリモートオフィスのシステム管理者に送信します。

   管理サーバーの証明書ファイルは、その管理サーバーの %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer にあります。
3. セカンダリ管理サーバーの証明書ファイルを外付けドライブ（フラッシュドライブなど）に書き出します。セカンダリ管理サーバーがリモートオフィスにある場合、そのオフィスのシステム管理者に連絡して、証明書の送信を要求します。

   管理サーバーの証明書ファイルは、その管理サーバーの %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer にあります。
4. 管理コンソールを使用してプライマリ管理サーバーに接続します。
5. セカンダリ管理サーバーを追加する管理グループを選択します。
6. ［**管理サーバー**］フォルダーの作業領域で［**セカンダリ管理サーバーの追加**］をクリックします。

   セカンダリ管理サーバー追加ウィザードが起動します。
7. ウィザードの最初のステップ（アドレスの入力）で、［**セカンダリ管理サーバーアドレス（任意）**］を空白にします。
8. ［**セカンダリ管理サーバーの証明書ファイル**］ウィンドウで、［**参照**］をクリックし、保存したセカンダリ管理サーバーの証明書ファイルを選択します。
9. ウィザードが完了したら、別の管理コンソールを使用してセカンダリ管理サーバーに接続します。この管理サーバーがリモートオフィスにある場合、そのオフィスのシステム管理者に連絡して、セカンダリ管理サーバーに接続して以後の手順を実行するよう要求します。
10. ［**管理サーバー**］フォルダーのコンテキストメニューで［**プロパティ**］を選択します。
11. 管理サーバーのプロパティで［**詳細**］セクションの［**管理サーバーの階層**］サブセクションに移動します。
12. ［**この管理サーバーをセカンダリ管理サーバーとして使用する**］をオンにします。

    データの入力と編集が可能なフィールドが表示されます。
13. ［**プライマリ管理サーバーのアドレス**］に、プライマリ管理サーバーのネットワーク名を入力します。
14. ［**参照**］をクリックして、保存したプライマリ管理サーバーの証明書ファイルを選択します。
15. ［**OK**］をクリックします。

プライマリとセカンダリの階層が構築されます。管理コンソールからセカンダリ管理サーバーに接続できます。プライマリ管理サーバーがセカンダリ管理サーバーから接続されます。

プライマリ管理サーバーからセカンダリ管理サーバーへの接続

新規管理サーバーをセカンダリとして追加し、プライマリ管理サーバーからセカンダリ管理サーバーへポート 13000 で接続できます。これは、たとえばセカンダリ管理サーバーが DMZ にある場合に有用です。

プライマリ管理サーバーとセカンダリ管理サーバーの両方の管理サーバーに TCP ポート 13291 で接続できる管理コンソールがインストールされたデバイスが必要です。

新規管理サーバーをセカンダリとして追加し、ポート 13000 でプライマリ管理サーバーに接続するには：

1. セカンダリ管理サーバーのポート 13000 にプライマリ管理サーバーから接続できることを確認します。
2. 管理コンソールを使用してプライマリ管理サーバーに接続します。
3. セカンダリ管理サーバーを追加する管理グループを選択します。
4. 目的のグループの［**管理サーバー**］フォルダーの作業領域で［**セカンダリ管理サーバーの追加**］をクリックします。

   セカンダリ管理サーバー追加ウィザードが起動します。
5. ウィザードの最初のステップ（グループに追加する管理サーバーのアドレスの入力）で、セカンダリ管理サーバーのネットワーク名を入力し、［**プライマリ管理サーバーを DMZ 内のセカンダリ管理サーバーに接続する**］をオンにします。
6. プロキシサーバーを使用してセカンダリ管理サーバーに接続する場合、ウィザードの最初のステップで［**プロキシサーバーを使用する**］をオンにし、接続設定を指定します。
7. ウィザードの指示に従ってください。

管理サーバーの階層が作成されます。セカンダリ管理サーバーがプライマリ管理サーバーから接続されます。

管理サーバーへの接続と管理サーバーの切り替え

Kaspersky Security Center が起動されると、管理サーバーへの接続が試行されます。ネットワーク上で複数の管理サーバーが利用できる場合、Kaspersky Security Center が前回のセッションで接続した管理サーバーが要求されます。

Kaspersky Security Center がインストール後に初めて起動された場合、インストール時に指定された管理サーバーへの接続が試行されます。

管理サーバーへの接続が確立されると、そのサーバーのフォルダーツリーがコンソールツリーに表示されます。

コンソールツリーに複数の管理サーバーが追加されている場合は、それらのサーバーを切り替えることができます。

管理コンソールは、それぞれの管理サーバーの作業に必要です。新しい管理サーバーへ初めて接続する前に、管理コンソールからの接続を受信するポート 13291 が開放されていることを確認してください。それ以外のすべてのポートは、管理サーバーと Kaspersky Security Center の他の機能の通信に必要です。

別の管理サーバーに切り替えるには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。

2. フォルダーのコンテキストメニューで、［**管理サーバーに接続**］の順に選択します。

3. 開かれる［**接続設定**］ウィンドウの［**管理サーバーアドレス**］で、接続する管理サーバーの名前を指定します。管理サーバーの名前として、IP アドレスまたは Windows ネットワーク上でのデバイスの名前を指定できます。［**詳細**］をクリックして管理サーバーへの接続を設定することができます（次の図を参照）。

   既定とは別のポートから管理サーバーに接続するには、<管理サーバー名>:<ポート> 形式で［**管理サーバーアドレス**］に値を入力します。

   仮想管理サーバーに接続するには、［**管理サーバーアドレス**］フィールドに <管理サーバーのアドレス>/<仮想サーバー名> の形式で値を入力します。

   読み取り 権限がないユーザーは管理サーバーへのアクセスを拒否されます。

管理サーバーへの接続

4. サーバーの切り替えを完了するには、［**OK**］をクリックします。

管理サーバーに接続すると、コンソールツリーで対応するノードのフォルダーツリーが更新されます。

管理サーバーとそのオブジェクトへのアクセス権限

Kaspersky Security Center のインストール時に、**KLAdmins** グループおよび **KLOperators** グループが自動的に作成されます。これらのグループには、管理サーバーに接続し、管理サーバーオブジェクトを処理するための権限が与えられます。

Kaspersky Security Center のインストール時に使用されるアカウントの種類に応じて、**KLAdmins** グループと **KLOperators** グループが次のようにして作成されます：

- ドメイン内に含まれるユーザーアカウントを使用してインストールする場合、グループは管理サーバーを含むドメインと管理サーバー自体に作成されます。

- システムアカウントでインストールする場合、グループは管理サーバーのみで作成されます。

オペレーティングシステムの標準的な管理ツールを使用して、**KLAdmins** および **KLOperators** グループを表示し、**KLAdmins** および **KLOperators** グループに属するユーザーのアクセス権限を変更できます。

KLAdmins グループにはすべてのアクセス権限が付与され、**KLOperators** グループには読み取り権限と実行権限のみが付与されます。**KLAdmins** グループに付与される権限はロックされています。

KLAdmins グループに属するユーザーは *Kaspersky Security Center 管理者*と呼ばれ、**KLOperators** グループのユーザーは *Kaspersky Security Center オペレーター*と呼ばれます。

KLAdmins グループのユーザーに加え、管理サーバーがインストールされているデバイスのローカル管理者にも Kaspersky Security Center の管理者権限が付与されます。

ローカル管理者は、Kaspersky Security Center 管理者の権限を有するユーザーのリストから除外できます。

Kaspersky Security Center の管理者によって開始される操作はすべて、管理サーバーアカウントの権限で実行されます。

個々の **KLAdmins** グループは、ネットワークの各管理サーバーに作成できます。作成されたグループはその管理サーバーだけのための必要な権限を持ちます。

1つのドメイン内の複数のデバイスが、異なる管理サーバーで構成される複数の管理グループに含まれる場合、このドメインの管理者はこれらのグループすべての Kaspersky Security Center 管理者になります。**KLAdmins** グループはこれらの管理グループで同一であり、最初の管理サーバーのインストール時に作成されます。Kaspersky Security Center 管理者によって開始される操作は、それらの操作が向けられた管理サーバーのアカウント権限を使用して実行されます。

アプリケーションのインストール後、Kaspersky Security Center の管理者は以下の処理を実行できます：

- **KLOperators** グループに付与された権限を変更する
- Kaspersky Security Center の機能にアクセスする権限を、管理コンピューターに登録されている他のセキュリティグループまたは個別ユーザーに付与する
- 各管理グループ内のユーザーにアクセス権限を割り当てる

Kaspersky Security Center 管理者は、選択したオブジェクトのプロパティウィンドウにある［**セキュリティ**］セクションで、各管理グループまたは管理サーバーの他のオブジェクトにアクセス権限を割り当てることができます。

管理サーバーの動作におけるイベントのレコードを使用すると、ユーザーアクティビティを追跡できます。イベントのレコードは［**管理サーバー**］フォルダーの［**イベント**］タブに表示されます。これらのイベントには、重要度（［**情報イベント**］で示される）とイベント種別（［**監査**］で始まる）が含まれます。

インターネット経由で管理サーバーに接続する条件

管理サーバーがリモートであり、企業ネットワークの外にある場合、クライアントデバイスはインターネット経由で管理サーバーに接続できます。

デバイスがインターネット経由で管理サーバーに接続するには、次の条件を満たしている必要があります：

- リモート管理サーバーに外部 IP アドレスを設定し、受信ポート 13000 を開放しておく必要があります（ネットワークエージェントの接続用）。UDP ポート 13000 の開放も推奨します（デバイスのシャットダウン通知の受信用）。

- ネットワークエージェントをデバイスにインストールします。

- デバイスにネットワークエージェントをインストールする時に、リモート管理サーバーの外部 IP アドレスを指定します。インストールパッケージを使用してインストールする場合は、インストールパッケージのプロパティの［**設定**］セクションに、外部 IP アドレスを手動で指定します。

- リモート管理サーバーを使用してデバイスのアプリケーションとタスクを管理するには、デバイスのプロパティウィンドウの［**全般**］セクションで、［**管理サーバーから切断しない**］をオンにします。その後、管理サーバーがリモートデバイスと同期されるまで待ちます。管理サーバーと常時接続できるクライアントデバイスの数は最大 300 です。

リモート管理サーバーによって開始されるタスクのパフォーマンスを高めるには、デバイスのポート 15000 を開きます。この場合、管理サーバーは、タスクを実行する際、デバイスとの同期が完了するまで待つことなく、ポート 15000 経由でネットワークエージェントに特別なパケットを送信します。

管理サーバーへの暗号化された接続

クライアントデバイスと管理サーバー間のデータ交換、および管理コンソールと管理サーバー間の接続は、TLS（Transport Layer Security）プロトコルを使用して実行されます。TLS によって、交信する双方の識別、送信データの暗号化、送信データ通信中の改竄防止が可能になります。TLS プロトコルは、交信する双方の認証とデータの暗号化のために公開鍵を使用します。

デバイス接続時の管理サーバーの認証

クライアントデバイスが管理サーバーに初めて接続する場合、デバイスのネットワークエージェントは管理サーバー証明書のコピーをダウンロードし、それをローカルに保存します。

> ネットワークエージェントをデバイスにローカルにインストールする場合は、管理サーバー証明書を手動で選択できます。

以降の接続では、管理サーバーの権限の検証にダウンロードされた証明書のコピーが使用されます。

以降のセッションでは、デバイスから管理サーバーへの接続ごとに、ネットワークエージェントが管理サーバー証明書を要求して、ローカルコピーと比較します。コピーが一致しない場合、デバイスから管理サーバーへのアクセスは許可されません。

管理コンソール接続時の管理サーバーの認証

管理サーバーへの初回接続時に、管理サーバー証明書が管理コンソールによって要求され、管理コンピューターのローカルに保存されます。それ以降、管理コンソールがその管理サーバーへ接続を試行するたびに、管理サーバーが証明書のコピーに基づいて識別されます。

管理サーバー証明書が管理コンピューターに保存されているコピーと一致しない場合は、指定された名前の管理サーバーへの接続を確認し、証明書を新たにダウンロードするよう要求するメッセージが表示されます。接続が成功すると、管理コンソールによって新しい管理サーバー証明書のコピーが保存されます。以降は、このコピーが管理サーバーの識別に使用されます。

管理サーバーに接続するための IP アドレスの許可リストの設定

既定では、ユーザーは、Kaspersky Security Center Web コンソール（以降、Web コンソールと表記）または MMC ベースの管理コンソールを開くことができる任意のデバイスで Kaspersky Security Center にログインできます。ただし、管理サーバーを設定することで、ユーザーが許可された IP アドレスを持つデバイスからのみ管理サーバーに接続できるように設定できます。こうすると、侵入者が Kaspersky Security Center アカウントを盗んだとしても、侵入者のデバイスの IP アドレスが許可リストに登録されていないため、Kaspersky Security Center にログインすることはできません。

ユーザーが Kaspersky Security Center にログインするか、Kaspersky Security Center OpenAPI を介して管理サーバーと連携するアプリケーションを実行した場合に IP アドレスが検証されます。この時点で、ユーザーのデバイスは管理サーバーとの接続を確立しようとします。デバイスの IP アドレスが許可リストにない場合、認証エラーが発生し、KLAUD_EV_SERVERCONNECT イベントが管理サーバーとの接続が確立されていないことを通知します。

IP アドレスの許可リストの要件

次のアプリケーションが管理サーバーに接続しようとした際にのみ IP アドレスが検証されます：

- Web コンソールサーバー

  1 つのデバイスで Web コンソールにログインして、Web コンソールサーバーが別のデバイス上にインストールされている場合、オペレーティングシステムの標準の方法で Web コンソールがインストールされているデバイスにファイアウォールを設定することができます。誰かが Web コンソールにログインを試みた場合、ファイアウォールが侵入者の干渉防止に役立ちます。

- 管理コンソール

- Klakaut 自動化オブジェクト経由で管理サーバーと連携しているアプリケーション

- Kaspersky Anti Targeted Attack Platform または Kaspersky Security for Virtualization のような、OpenAPI 経由で管理サーバーと連携するアプリケーション

このため、上のリストにあるアプリケーションがインストールされているデバイスのアドレスを指定してください。

IPv4 と IPv6 アドレスを指定できます。IP アドレスの範囲を指定することはできません。

IP アドレスの許可リストを設定する方法

事前に許可リストを設定していなかった場合は、次の手順に従ってください。

Kaspersky Security Center にログインするための IP アドレスの許可リストを設定するには：

1. 管理サーバーデバイスで、管理者権限を持つアカウントでコマンドプロンプトを実行します。
2. カレントディレクトリを Kaspersky Security Center のインストールフォルダ（通常は <ディスク>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center）に変更します。
3. 管理者権限を使用して次のコマンドを入力します：
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP アドレス>" -t s`

前述の要件を満たす IP アドレスを指定します。複数の IP アドレスを指定する場合はセミコロンで区切ります。

単一のデバイスに対して管理サーバーへの接続を許可する方法の例：

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s
```

複数のデバイスに対して管理サーバーへの接続を許可する方法の例：

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s
```

4. 管理サーバーサービスを再起動します。

管理サーバーのイベントログで、IP アドレスの許可リストが正常に設定されているかどうかを確認できます：

IP アドレスの許可リストを変更する方法

最初に許可リストを作成した方法と同じ方法で許可リストを変更できます。同じコマンドを実行して新しい許可リストの名前を指定します。

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP アドレス>" -t s
```

許可リストから一部の IP アドレスを削除する場合は、書き直します。たとえば、許可リストに IP アドレス「198.51.100.0; 203.0.113.0」が含まれているとします。IP アドレス「198.51.100.0」を削除したいとします。この場合、コマンドプロンプトで次のコマンドを入力します：

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

管理サーバーサービスを忘れずに再起動してください。

設定済みの IP アドレスの許可リストをリセットする方法

既に設定済みの IP アドレスの許可リストをリセットするには：

1. 管理者権限を使用し、コマンドプロンプトで次のコマンドを入力します：
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`
2. 管理サーバーサービスを再起動します。

その後、IP アドレスは検証されなくなります。

klscflag を使用したポートの閉鎖

管理サーバーのポート 13291 は管理コンソールからの接続を受け取るために使用されます。このポートは既定で開かれています。MMC ベースの管理コンソールまたは klakaut ユーティリティを使用しない場合は、klscflag ユーティリティを使用してこのポートを閉じることができます。このユーティリティは KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN パラメータの値を変更します。

ポート 13291 を閉じるには：

1. Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

2. コマンドラインで次のコマンドを実行します：
   ```
   klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
   ```

3. Kaspersky Security Center 管理サーバーサービスを再起動します。

ポート 13291 が閉じます。

ポート 13291 が正常に閉じたことを確認するには：

コマンドラインで次のコマンドを実行します：

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

このコマンドは次の結果を返します：

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

値「`false`」はポートが閉じられていることを意味します。それ以外の場合は値「`true`」が表示されます。

管理サーバーからの切断

管理サーバーから切断するには：

1. コンソールツリーで、切断する管理サーバーに対応するフォルダーを選択します。

2. フォルダーのコンテキストメニューで、［**管理サーバーから切断**］を選択します。

コンソールツリーへの管理サーバーの追加

コンソールツリーに管理サーバーを追加するには：

1. Kaspersky Security Center のメインウィンドウで、コンソールツリーの［**Kaspersky Security Center**］フォルダーを選択します。

2. フォルダーのコンテキストメニューで、［**新規作成**］→［**管理サーバー**］の順に選択します。

［**管理サーバー - <デバイス名>（接続されていません）**］というフォルダーがコンソールツリーに作成され、そのフォルダーからネットワーク上にインストールされている任意の管理サーバーに接続できるようになります。

コンソールツリーからの管理サーバーの削除

コンソールツリーから管理サーバーを削除するには：

1. コンソールツリーで、削除する管理サーバーに対応するフォルダーを選択します。
2. フォルダーのコンテキストメニューで［**削除**］を選択します。

コンソールツリーへの仮想管理サーバーの追加

コンソールツリーに仮想管理サーバーを追加するには：

1. コンソールツリーで、仮想管理サーバーを作成する必要がある管理サーバーの名前が付けられたフォルダーを選択します。
2. 仮想管理サーバーノードで、［**管理サーバー**］フォルダーを選択します。
3. ［**管理サーバー**］フォルダーの作業領域で［**仮想管理サーバーの追加**］をクリックします。
   新規仮想管理サーバーウィザードが起動します。
4. ［**仮想管理サーバー名**］ウィンドウ、作成する仮想管理サーバーの名前を指定します。
   仮想管理サーバーの名前は 255 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. ［**デバイスを仮想管理サーバーに接続するアドレスの入力**］ウィンドウで、デバイス接続アドレスを指定します。
   仮想管理サーバーの接続アドレスは、デバイスを接続するネットワークアドレスです。接続アドレスは 2 つのパート：物理管理サーバーのネットワークアドレスと仮想管理サーバー名がスラッシュで区分されます。仮想管理サーバー名は自動登録されます。指定されたアドレスが、ネットワークエージェントのインストールパッケージ内の既定のアドレスとして仮想管理サーバーに使用されます。
6. ［**仮想管理サーバーの管理者アカウントの作成**］ウィンドウで、仮想サーバー管理者の役割を果たすユーザーをリストから割り当てるか、［**作成**］をクリックして、新しい管理者アカウントを追加します。
   複数アカウントを指定できます。

   ［**管理サーバー – <仮想管理サーバーの名前>**］という名前のフォルダーがコンソールツリーに作成されます。

管理サーバーのサービスアカウントの変更：klsrvswch ユーティリティ

Kaspersky Security Center のインストール時に設定した管理サーバーのサービスアカウント設定を変更する必要がある場合は、管理サーバーアカウントを変更する klsrvswch ユーティリティを使用できます。

このユーティリティは、Kaspersky Security Center をインストールする時にアプリケーションインストールフォルダーに自動的にコピーされます。

ユーティリティの起動数は基本的に無制限です。

> 管理サーバーのインストールに使用した管理者権限を持つアカウントで、管理サーバーデバイス上で klsrvswch ユーティリティを起動する必要があります。

klsrvswch ユーティリティを使用してアカウント種別を変更できます：たとえば、ローカルアカウントからドメインアカウントや管理対象サービスアカウントへの変更が行えます。klsrvswch ユーティリティでは、アカウントの種別をグループ管理対象サービスアカウント（gMSA）に変更することはできません。

Windows Vista 以降のバージョンの Windows では、管理サーバーでローカルシステムアカウントを使用できません。これらのバージョンの Windows では、［**ローカルシステムアカウント**］は無効になります。

管理サーバーのサービスアカウントをドメインアカウントに変更するには：

1. Kaspersky Security Center のインストールフォルダーから klsrvswch ユーティリティを起動します。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

   この処理によって、管理サーバーのサービスアカウントを変更するウィザードが起動されます。ウィザードの指示に従ってください。

2. ［**管理サーバーのサービスアカウント**］ウィンドウで、［**ローカルシステムアカウント**］を選択します。

ウィザードが完了すると、管理サーバーアカウントが変更されます。管理サーバーのサービスは、*ローカルシステムアカウント*とこれに対応する権限で開始されます。

Kaspersky Security Center を正しく動作させるには、管理サーバーのサービスの開始に必要なアカウントに、管理サーバーデータベースのホスト先リソースに対する管理者権限を付与する必要があります。

管理サーバーのサービスアカウントをユーザーアカウントまたは管理対象サービスアカウントに変更するには：

1. Kaspersky Security Center のインストールフォルダーから klsrvswch ユーティリティを起動します。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

   この処理によって、管理サーバーのサービスアカウントを変更するウィザードが起動されます。ウィザードの指示に従ってください。

2. ［**管理サーバーのサービスアカウント**］ウィンドウで、［**カスタムアカウント**］を選択します。

3. ［**今すぐ検索**］をクリックします。

   ［**ユーザーの選択**］ウィンドウが表示されます。

4. ［**ユーザーの選択**］ウィンドウで、［**オブジェクトの種類**］をクリックします。

5. オブジェクトの種類のリストから、［**ユーザー**］（ユーザーアカウントの場合）または［**サービスアカウント**］（管理対象サービスアカウントの場合）を選択し、［**OK**］をクリックします。

6. オブジェクト名フィールドで、アカウント名またはアカウント名の一部を入力し、［**名前の確認**］をクリックします。

7. 合致する名前のリストから目的の名前を選択し、［**OK**］をクリックします。

8. ［**サービスアカウント**］を選択した場合は、［**パスワード**］ウィンドウで、［**パスワード**］と［**パスワードの確認**］は空白のままにします。［**ユーザー**］を選択した場合は、ユーザー用に新しいパスワードを入力して確認します。

管理サーバーのサービスアカウントが選択したアカウントに変更されます。

Windows ツールによるユーザーアカウントの認証を前提とするモードで Microsoft SQL Server を使用する場合は、データベースへのアクセス権を付与してください。このユーザーアカウントには、Kaspersky Security Center データベースの所有者のステータスを割り当てる必要があります。既定では、dbo スキームが使用されます。

DBMS 資格情報の変更

たとえば、セキュリティ目的で資格情報のローテーションを実行するために、DBMS の資格情報の変更が必要になる場合があります。

Windows 環境で klsrvswch.exe を使用して DBMS 資格情報を変更するには：

1. Kaspersky Security Center のインストールフォルダーにある klsrvswch ユーティリティを起動します。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

   管理サーバーのインストールに使用した管理者権限を持つアカウントで、管理サーバーデバイス上で klsrvswch ユーティリティを起動する必要があります。

2. ［**DBMS へのアクセスの資格情報を変更する**］に到達するまで、ウィザードの［**次へ**］をクリックします。

3. ウィザードの［**DBMS へのアクセスの資格情報を変更する**］ステップで、次の操作を実行します：

   Windows 認証が使用されている場合、ウィザードの **DBMS へのアクセスの資格情報を変更する** 手順はスキップされます。

   - ［**新しい資格情報を適用**］を選択します。
   - ［**アカウント**］に新しいアカウント名を入力します。
   - ［**パスワード**］にアカウントの新しいパスワードを入力します。
   - ［**パスワードの確認**］で先ほど入力した新しいパスワードをもう一度入力します。

   DBMS に存在するアカウントの資格情報を指定する必要があります。

4. ［**次へ**］をクリックします。

ウィザードが終了すると、DBMS 資格情報が変更されます。

klsrvswch ユーティリティは、SQL 認証のアカウントのパスワードを変更するためにのみ使用できます。認証方法の変更はサポートされていません。認証方法を変更するには、管理サーバーを再インストールし、必要な設定を指定します。

管理サーバーの共有フォルダーからの変更

管理サーバーの共有フォルダは、管理サーバーのインストール中に指定されます。また、管理サーバーのプロパティで、共有フォルダーの場所を変更することもできます。

共有フォルダを変更するには：

1. ネットワーク共有フォルダーを作成し、共有とフォルダー構造のアクセス許可を設定して、［**Everyone**］サブグループにフルコントロール権限を許可します。
2. Kaspersky Security Center のコンソールツリーで、［**管理サーバー**］フォルダーのコンテキストメニューを開いて、［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウにある［**セクション**］ペインで、［**詳細**］→［**管理サーバーの共有フォルダー**］の順に選択します。
4. ［**管理サーバーの共有フォルダー**］セクションで、［**変更**］をクリックします。
5. 共有として使用するフォルダーを選択します。
6. ［**OK**］をクリックして、管理サーバーのプロパティウィンドウを閉じます。
7. 共有として選択したフォルダの**みんな**サブグループに読み取り権限を割り当てます。

管理サーバーフォルダーに関するトラブルシューティング

管理コンソールの画面左側にあるコンソールツリーに、管理サーバーフォルダーが含まれています。必要な数の管理サーバーをコンソールツリーに追加できます。

コンソールツリー内の管理サーバーフォルダーのリストは、Microsoft 管理コンソールの MSC 形式のファイルのシャドウコピーとして保存されています。このファイルのシャドウコピーは、管理コンソールをインストールしたデバイスの %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ フォルダーに保存されています。各管理サーバーフォルダーについて、ファイルには次の情報が含まれています。

- 管理サーバーアドレス
- ポート番号
- TLS の使用

  このパラメータは、管理コンソールと管理サーバーの接続に使用されているポート番号によって異なります。
- ユーザー名
- 管理サーバー証明書

トラブルシューティング

管理コンソールから管理サーバーへの接続時、ローカルで保存されている証明書と管理サーバーの証明書が照合されます。証明書が一致しない場合、管理コンソールでエラーが生成されます。証明書の不一致は、たとえば管理サーバーの証明書を置き換えた場合などに発生することがあります。この場合、コンソール内で管理サーバーフォルダーを再作成してください。

管理サーバーフォルダーを再作成するには：

1. Kaspersky Security Center 管理コンソールウィンドウを閉じます。
2. %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ にある Kaspersky Security Center 15.1 のファイルを削除します。
3. Kaspersky Security Center 管理コンソールを実行します。
   管理サーバーへの接続と既存の証明書の受け入れを要求するメッセージが表示されます。
4. 次のいずれかの手順を実行します：
   - ［**はい**］をクリックして、既存の証明書を受け入れます。
   - 保有している証明書を指定する場合は、［**いいえ**］をクリックして管理サーバーの認証に使用する証明書ファイルを参照先として選択します。

証明書に関する問題が解決します。管理コンソールを使用して管理サーバーに接続できます。

管理サーバーの設定の表示と変更

当該サーバーのプロパティウィンドウで管理サーバーの設定を指定できます。

［プロパティ：管理サーバー］ウィンドウを開くには：

コンソールツリーの管理サーバーフォルダーのコンテキストメニューで、［**プロパティ**］を選択します。

管理サーバーの全般設定の調整

管理サーバーの全般設定は、管理サーバーのプロパティウィンドウの［**全般**］、［**管理サーバー接続設定**］、［**イベントリポジトリ**］、および［**セキュリティ**］セクションで調整できます。

管理コンソールのインターフェイスで表示が無効化されていると、管理サーバーのプロパティウィンドウで［**セキュリティ**］セクションが表示されないことがあります。

*管理コンソールでの［**セキュリティ**］セクションの表示を有効にするには：*

1. コンソールツリーで、目的の管理サーバーを選択します。
2. メインウィンドウの［**表示**］メニューで、［**インターフェイスの設定**］を選択します。
3. ［**インターフェイスの設定**］ウィンドウが開いたら、［**セキュリティ設定タブの表示**］をオンにして、［**OK**］をクリックします。
4. アプリケーションメッセージが表示されたウィンドウで、［**OK**］をクリックします。

［**セキュリティ**］セクションが管理サーバーのプロパティウィンドウに表示されます。

管理コンソールのインターフェイスの設定

管理コンソールのインターフェイスの設定を編集して、次の機能に関するユーザーインターフェイスメニューの表示と非表示を切り替えることができます。

- 脆弱性とパッチ管理
- データ暗号化と保護機能
- エンドポイントコントロール設定
- モバイルデバイス管理
- セカンダリ管理サーバー
- セキュリティ設定タブ

管理コンソールのインターフェイスの設定を編集するには：

1. コンソールツリーで、目的の管理サーバーを選択します。
2. メインウィンドウの［**表示**］メニューで、［**インターフェイスの設定**］を選択します。
3. 表示される［**インターフェイスの設定**］ウィンドウで、表示する機能の隣にあるチェックボックスをオンにし、［OK］をクリックします。
4. アプリケーションメッセージが表示されたウィンドウで、［OK］をクリックします。

管理コンソールのインターフェイスで、選択した機能が表示されるようになります。

管理サーバーでのイベントの処理と保管

アプリケーションの動作および管理対象デバイスでのイベントに関する情報は、管理サーバーデータベースに保存されます。イベントにはそれぞれ種別と重要度（*緊急イベント*、*機能エラー*、*警告*、*情報*）という属性があります。イベントが発生した条件に応じて、同じ種別のイベントに異なる重要度を割り当てることができます。

イベントに割り当てられた種別および重要度は、管理サーバーのプロパティウィンドウの［**イベントの設定**］セクションに表示されます。［**イベントの設定**］セクションでは、管理サーバーによる各イベントの処理を設定することもできます。

- 管理サーバーにおけるイベントの登録、およびデバイスと管理サーバーのオペレーティングシステムのイベントログにおけるイベントの登録
- 管理者へのイベントの通知方法（例：SMS、メール）

管理サーバーのプロパティウィンドウ内にある［**イベントリポジトリ**］セクションで、管理サーバーデータベース内で保管するイベントの設定を編集できます。編集可能な設定項目は、イベントのレコード数上限やレコードの保管期間があります。保管するイベント数の上限を指定すると、指定した数に応じて必要なディスク容量の概算値が算出されます。データベースのオーバーフローを避けるために十分な空き容量があるかどうかのこの概算値を使用できます。既定の設定では、管理サーバーデータベース内に保管できるイベント数は 400,000 件までとなっています。データベースで推奨される範囲でのイベント数の上限は、45,000,000 件です。

アプリケーションは 10 分ごとにデータベースをチェックします。イベント数が指定された最大値に 10,000 を加えた値に達すると、アプリケーションは最も古いイベントを削除し、指定された最大数のイベントのみが残ります。

管理サーバーが古いイベントを削除する際に、新しいイベントのデータベースへの保存は行えません。この期間、拒否したイベントの情報は Kaspersky イベントログに書き込まれます。新しいイベントはキューに追加され、削除操作が完了した後にデータベースに保存されます。

任意のタスクの設定を変更して、タスクの進行状況に関連するイベントを保存したり、タスクの実行結果のみを保存したりできます。それにより、データベース内のイベントの数を削減することで、データベース内のイベントの分析を伴う操作の実行速度を向上し、多数のイベントによって重要なイベントが上書きされる可能性を低下させることができます。

管理サーバーへの接続のログの表示

動作中の管理サーバーへの接続と接続試行の履歴がログファイルに保存されます。ログファイル内の情報により、ネットワークインフラストラクチャにおける接続だけでなく、管理サーバーに対する不正アクセスの試行についても追跡できます。

管理サーバーへの接続イベントのログを記録するには：

1. コンソールツリーで、接続イベントのログ記録を有効にする管理サーバーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. プロパティウィンドウが開いたら、［**管理サーバー接続設定**］セクションで［**接続ポート**］サブセクションを選択します。
4. ［**管理サーバーへの接続イベントを記録する**］をオンにします。
5. ［**OK**］をクリックして、管理サーバーのプロパティウィンドウを閉じます。

管理サーバーの受信接続イベント、認証の結果、SSL エラーが「%ProgramData%\KasperskyLab\adminkit\logs\sc.syslog」ファイルに記録されます。

ウイルスアウトブレイクの制御

Kaspersky Security Center では、ウイルスアウトブレイクの脅威に迅速に対応できます。ウイルスアウトブレイクの危険度は、デバイスにおけるウイルスアクティビティを監視することで評価されます。

ウイルスアウトブレイクの脅威の評価ルールおよび発生時の処理を設定するには、管理サーバーのプロパティウィンドウにある［**ウイルスアウトブレイク**］セクションを使用します。

［*ウイルスアウトブレイク*］イベント発生時の通知手順は、管理サーバーのプロパティウィンドウの［**イベントの設定**］セクションから、［*ウイルスアウトブレイク*］イベントのプロパティウィンドウで設定できます。

［*ウイルスアウトブレイク*］イベントが作成されるのは、セキュリティ製品の動作中に*感染したオブジェクトの検知*イベントが検知された場合です。そのため、ウイルスアウトブレイクを認識できるようにするには、*感染したオブジェクトの検知*イベントに関する情報を管理サーバーに保存する必要があります。

*感染したオブジェクトの検知*イベントに関する情報を保存する設定は、セキュリティ製品のポリシーで指定します。

*悪意のあるオブジェクトの検知*イベントの数をカウントする場合、プライマリ管理サーバーのデバイスからの情報のみが考慮されます。セカンダリ管理サーバーからの情報は考慮されません。各セカンダリ管理サーバーで、［*ウイルスアウトブレイク*］イベントを個別に設定します。

トラフィック制限

ネットワーク内のトラフィック量を軽減するために、このアプリケーションには、指定の IP アドレス範囲および IP サブネットから管理サーバーへのデータ転送速度を制限するオプションが用意されています。

トラフィック制限ルールは、管理サーバーのプロパティウィンドウの［**トラフィック**］セクションで作成、設定できます。

トラフィック制限ルールを作成するには：

1. コンソールツリーで、トラフィック制限ルールを作成する必要がある管理サーバーの名前が付けられたフォルダーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウで、［**トラフィック**］セクションを選択します。
4. ［**追加**］をクリックします。
5. ［**新規ルール**］ウィンドウで、次の設定を指定します：

   ［**トラフィックを制限する IP アドレス範囲**］セクションで、データ送信速度が制限されるサブネットまたは範囲の定義に使用される方法を選択し、選択した方法に対応するパラメータの値を入力します。次のいずれかの方法を選択します：

   - **アドレスとネットワークマスクで範囲を指定する**

     トラフィックはサブネットの設定に基づいて制限されます。トラフィックが制限される範囲を決めるサブネットアドレスとサブネットマスクを指定します。

     ［**参照**］をクリックして、サブネットのグローバルリストからサブネットを追加することもできます。

   - **開始アドレスと終了アドレスで範囲を指定する**

     トラフィックは IP アドレスの範囲に基づいて制限されます。［**開始**］と［**終了**］に IP アドレスを入力して範囲を指定します。

     既定ではこのオプションが選択されます。

   ［**トラフィック制限**］セクションでは、次のデータ送信速度の制限設定を調整できます：

   - **時間**

     トラフィック制限を実施する時間。この入力フィールドで時間間隔を指定できます。

   - **制限（KB/秒）**

     管理サーバーの着信データと発信データの最大送信速度。トラフィック制限は、［**時間**］で指定した時間内でのみ有効になります。

   - **上記以外の時間もトラフィックを制限する（KB/秒）**

トラフィックは、このチェックボックスをオンにすると、［**時間**］で指定した期間内だけでなく、それ以外の時間も制限されます。

既定では、このチェックボックスはオフです。このフィールドの値は、［**制限（KB/秒）**］の値と一致しない場合があります。

トラフィック制限は基本的にファイルの転送に適用されます。これらのルールは、管理サーバーとネットワークエージェントの同期またはプライマリ管理サーバーとセカンダリ管理サーバーの同期によって生成されるトラフィックには適用されません。

Web サーバーの設定

Web サーバーは、スタンドアロンインストールパッケージ、iOS MDM プロファイル、および共有フォルダーのファイルを公開することを目的に設計されています。

管理サーバーのプロパティウィンドウの［**Web サーバー**］セクションで、Web サーバーと管理サーバー間の接続設定を定義し、Web サーバー証明書を設定できます。

内部ユーザーによる操作

*内部ユーザー*のアカウントは、仮想管理サーバーを操作するために使用します。Kaspersky Security Center によって、実際のユーザーの権限がアプリケーションの内部ユーザーに付与されます。

内部ユーザーのアカウントは、Kaspersky Security Center 内でのみ作成および使用されます。内部ユーザーに関するデータは、オペレーティングシステムには送信されません。Kaspersky Security Center が内部ユーザーを認証します。

コンソールツリーの［**ユーザーアカウント**］フォルダーで、内部ユーザーのアカウントを設定できます。

管理サーバーの設定のバックアップと復元

管理サーバーとそのデータベースの設定のバックアップは、バックアップタスクと klbackup ユーティリティを使用して実行されます。バックアップコピーには、証明書、管理対象デバイスのドライブ暗号化用のプライマリキー、様々なライセンス情報、および内容、タスク、ポリシーのすべてを含む管理グループ構造など、管理サーバーに関係するすべての主要な設定とオブジェクトが含まれています。バックアップコピーを使用すると、数十分から数時間で可能な限り迅速に管理サーバーの操作を復元できます。

バックアップコピーが使用できない場合は、障害が発生して証明書や管理サーバーの設定がすべて失われてしまうことがあります。この場合は、Kaspersky Security Center を最初から再設定し、組織ネットワークで再度ネットワークエージェントの初期導入を実行する必要があります。管理対象デバイスのドライブ暗号化用のプライマリキーもすべて失われ、Kaspersky Endpoint Security がインストールされたデバイスの暗号化されたデータも失われてしまう危険性があります。そのため、必ず標準的なバックアップタスクを実行し、管理サーバーを定期的にバックアップしてください。

クイックスタートウィザードは、管理サーバー設定のバックアップタスクを作成し、このタスクが毎日午前 4 時に実行されるように設定します。既定では、バックアップコピーはフォルダー %ALLUSERSPROFILE%\Application Data\KasperskySC に保存されます。

別のデバイスにインストールされている Microsoft SQL Server のインスタンスが DBMS として使用されている場合は、バックアップコピーを格納するフォルダーとして UNC パスを指定し、バックアップタスクを変更する必要があります。この場合、管理サーバーサービスと SQL Server サービスの両方による書き込みが使用できます。この要件は、Microsoft SQL Server DBMS のバックアップ特別機能から導かれます。

Microsoft SQL Server のローカルインスタンスが DBMS として使用されている場合は、専用メディアにバックアップコピーを保存して、管理サーバーとともに損傷から保護することを推奨します。

バックアップコピーには重要なデータが含まれているため、バックアップタスクと klbackup ユーティリティではバックアップコピーがパスワードにより保護されます。既定では、作成されるバックアップタスクのパスワードは空白です。このため、バックアップタスクのプロパティでパスワードを設定する必要があります。この要件を無視すると、管理サーバー証明書のすべての鍵、ライセンスの鍵、および管理対象デバイスのドライブ暗号化用のプライマリキーが暗号化されないままになります。

定期的なバックアップの他に、管理サーバーのアップグレードのインストールやパッチ適用などの重要な変更を加える前にも、必ずバックアップコピーを作成する必要があります。

Microsoft SQL Server を DBMS として使用すると、バックアップコピーのサイズを最小限に抑えることができます。これを行うには、SQL Server 設定で［**バックアップを圧縮する**］をオンにします。

バックアップコピーからの復元を実行するには、インストール済みで、バックアップコピーを作成したのと同じバージョン（またはそれ以降）の管理サーバーの操作可能なインスタンスでユーティリティ klbackup を使用します。

復元を実行する対象の管理サーバーのインスタンスでは、同じ種別（たとえば、同じ SQL Server または MariaDB）で同じかそれ以降のバージョンの DBMS を使用する必要があります。管理サーバーのバージョンは、同じ（同一またはそれ以降のパッチを適用）またはそれ以降にする必要があります。

このセクションでは、管理サーバーの設定とオブジェクトを復元する標準的な方法について説明します。

ファイルシステムのスナップショットを使用しバックアップの所要時間を短縮

Kaspersky Security Center 15.1 では、バックアップ時の管理サーバーの非稼働時間が、以前のバージョンと比較して短縮されました。加えて、**データのバックアップにファイルシステムスナップショットを使用する**機能が、タスクの設定に追加されました。この機能を使用すると、ツール klbackup の使用により、非稼働時間がさらに短縮されます。このツールは、バックアップ中にディスクのシャドウコピーを作成し（数秒かかります）、同時にデータベースをコピーします（最大で数分かかります）。klbackup がディスクのシャドウコピーとデータベースのコピーを作成すると、管理サーバーへの接続が再び可能になります。

ファイルシステムスナップショット機能は、以下の 2 つの条件を満たした時のみに使用可能です：

- 管理サーバーの共有サーバーと、フォルダー %ALLUSERSPROFILE%\KasperskyLab が同一の論理ディスク内に配置され、管理サーバーからローカルで参照可能である。
- フォルダー %ALLUSERSPROFILE%\KasperskyLab 内に、手動で作成されたシンボリックリンクがない。

いずれかの条件を満たさない場合は、この機能を使用しないでください。使用した場合、ファイルシステムスナップショットを使用する試行に対して、エラーメッセージが返されます。

この機能を使用するには、フォルダー %ALLUSERSPROFILE% が存在する論理ディスク上でスナップショットを作成する権限が付与されているアカウントが必要です。管理サーバーサービスのアカウントには、この権限が付与されていません。

ファイルシステムスナップショット機能を使用して、バックアップの時間を短縮するには：

1. ［**タスク**］セクションで、バックアップタスクを選択します。
2. コンテキストメニューから［**プロパティ**］を選択します。
3. タスクのプロパティウィンドウが開いたら、［**設定**］セクションを選択します。
4. ［**データのバックアップにファイルシステムスナップショットを使用する**］をオンにします。
5. ［**ユーザー名**］と［**パスワード**］のフィールドに、フォルダー %ALLUSERSPROFILE% が存在する論理ディスク上でスナップショットを作成する権限が付与されているアカウントの名前とパスワードを入力します。
6. ［**適用**］をクリックします。

その後、バックアップタスクの起動時に、klbackup ツールはファイルシステムスナップショットを常に作成し、タスク実行時の管理サーバーの非稼働時間を短縮します。

管理サーバーがインストールされているデバイスを操作できない

障害が発生しているため、管理サーバーをインストールしたデバイスが操作できない場合は、次の操作を実行してください：

- 新しい管理サーバーを同じアドレスで割り当てる：NetBIOS 名、FQDN、または固定 IP（ネットワークエージェント導入時の設定に応じて）。
- 同じ種別、同じ（またはそれ以降の）バージョンの DBMS を使用して、管理サーバーをインストールする。同じ（またはそれ以降の）パッチが適用された、同じバージョンまたはそれ以降のバージョンのサーバーをインストールする必要があります。インストール後は、ウィザードによる初期セットアップを実行しないでください。
- ［**スタート**］メニューで、klbackup ユーティリティによる復元を実行する。

管理サーバーまたはデータベースの設定が破損している

設定またはデータベースが破損しているため（たとえば、電力サージが原因）、管理サーバーが操作できない場合は、次の復元方法を使用してください：

1. 損傷を受けたデバイスでファイルシステムをスキャンする。
2. 操作できないバージョンの管理サーバーをアンインストールする。
3. 同じ種別、同じ（またはそれ以降の）バージョンの DBMS を使用して、管理サーバーを再インストールする。同じ（またはそれ以降の）パッチが適用された、同じバージョンまたはそれ以降のバージョンのサーバーをインストールする必要があります。インストール後は、ウィザードによる初期セットアップを実行しないでください。
4. ［**スタート**］メニューで、ユーティリティ klbackup による復元を実行する。

klbackup ユーティリティ以外の方法で管理サーバーを復元することは禁止されています。

サードパーティ製のソフトウェアを使用して管理サーバーの復元を試行した場合は、配信アプリケーション Kaspersky Security Center のノード上のデータが同期化されなくなり、その結果、本製品が正常に動作しなくなります。

管理サーバーデータのバックアップと復元

データバックアップにより、データを失わずに、管理サーバーをデバイス間で移動できます。バックアップを使用すると、管理サーバーのデータベースを別のデバイスに移動した時や、新しいバージョンの Kaspersky Security Center にアップグレードした時に、データを復元できます。

インストールされている管理プラグインはバックアップされないこと留意してください。管理サーバーのデータをバックアップコピーから復元した後で、管理対象アプリケーション用のプラグインをダウンロードして再インストールする必要があります。

管理サーバーのデータをバックアップする前に、仮想管理サーバーが管理グループに追加されているかどうかを確認してください。仮想管理サーバーを追加する場合は、バックアップ前にこの仮想管理サーバーに管理者が割り当てられていることを確認してください。バックアップ後は、仮想管理サーバーへの管理者アクセス権を付与できません。管理者アカウントの資格情報が失われると、仮想管理サーバーに新しい管理者を割り当てることができなくなることに注意してください。

次の方法のいずれかを使用して、管理サーバーデータのバックアップコピーを作成できます。

- 管理コンソールで、データバックアップタスクを作成して実行します。
- 管理サーバーがインストールされているデバイスで klbackup ユーティリティを実行する。このユーティリティは、Kaspersky Security Center の配布キットに含まれています。管理サーバーをインストールすると、このユーティリティは、アプリケーションのインストール時に指定したインストール先フォルダーのルートに格納されます。

次のデータが管理サーバーのバックアップコピー内に保存されます：

- 管理サーバーのデータベース（管理サーバーに保存されているポリシー、タスク、アプリケーション設定、イベント）
- 管理グループとクライアントデバイスの構造についての設定情報
- リモートインストール用アプリケーション配布パッケージのリポジトリ
- 管理サーバー証明書
- ［アップデート］フォルダーの内容。

  既定では、フォルダーのパスは C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\ です。

管理サーバーデータを復元するには、klbackup ユーティリティを使用する必要があります。

管理サーバーデータのバックアップタスク

管理サーバーデータのバックアップタスクの作成

バックアップタスクは管理サーバーのタスクであり、クイックスタートウィザードを通じて作成されます。クイックスタートウィザードで作成されたバックアップタスクが削除された場合、手動で作成することができます。

管理サーバーデータのバックアップタスクを作成するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. 次のいずれかの方法で、タスクの作成を開始します：
   - コンソールツリーの［**タスク**］フォルダーのコンテキストメニューで、［**新規**］→［**タスク**］の順に選択する。
   - 作業領域で［**タスクの作成**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。ウィザードの［**タスク種別の選択**］ウィンドウでは［**管理サーバーデータのバックアップ**］タスク種別を選択します。

［**管理サーバーデータのバックアップ**］タスクは1つのみ作成できます。管理サーバーの管理サーバーデータのバックアップタスクが既に作成されている場合は、管理サーバーのバックアップタスク作成ウィザードのタスク種別選択ウィンドウには表示されません。

管理サーバーデータのバックアップタスクの設定

バックアップタスクの作成後に、タスク設定を構成できます。

管理サーバーデータのバックアップタスクを設定するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. **管理サーバーデータのバックアップ**のコンテキストメニューから［**プロパティ**］を選択します。

   *管理サーバーデータのバックアップタスク*のプロパティウィンドウが開きます。次の機能を使用できます：

- **全般**

  ［**全般**］セクションでは、タスク名を指定し、タスクの作成日、最後のコマンドの日付、タスクの起動のステータス、およびタスクの結果を表示できます。

- **通知**

  ［**通知**］セクションでは、タスクを保存するための設定を指定したり、タスクの実行結果に関する通知を設定したりできます。

- **スケジュール**

  ［**スケジュール**］セクションでは、タスク開始のスケジュールを指定できます。

- **保存先**

  ［**保存先**］セクションでは、管理サーバーデータのバックアップコピーを保存するフォルダーへのパスを指定できます。

- **設定**

  ［**設定**］セクションでは、必要に応じて、バックアップ保護パスワードとバックアップコピーの数を設定できます。

  %ALLUSERSPROFILE% フォルダを保存している論理ディスクのシャドウコピーを作成し、管理サーバー定義データベースをコピーすることもできます。これを行うには、［**データのバックアップにファイルシステムスナップショットを使用する**］をオンにし、スナップショットを作成する権限を持つアカウントの名前とパスワードを指定する必要があります。

- **セキュリティ**

  ［**セキュリティ**］セクションでは、管理サーバー上で操作を実行する権限をユーザーとグループに付与できます。［**管理サーバーから設定を継承する**］がオンになっている場合、タスクのセキュリティ設定は管理サーバーから継承されます。

  このオプションがオフの場合、タスクのセキュリティ設定を編集できます。タスクへの適用と同様に、ロールをユーザーまたはユーザーのグループに割り当てたり、権限をユーザーまたはユーザーのグループに割り当てることができます。

  既定では、［**管理サーバーから設定を継承する**］がオンになっています。

- **変更履歴**

  ［**変更履歴**］セクションでは、タスクの変更を追跡できます。オブジェクトに変更を加えるたびに、リビジョンが作成されます。

データバックアップおよび復元ユーティリティ（klbackup）

バックアップと将来の復元に備えて、Kaspersky Security Center 配布キットに含まれている klbackup ユーティリティを使用して、管理サーバーのデータをコピーできます。

klbackup ユーティリティは、次の 2 つのモードのいずれかで実行できます：

- 対話モード
- サイレント

対話モードによるデータのバックアップと復元

対話モードで管理サーバーデータのバックアップを作成するには：

1. Kaspersky Security Center のインストールフォルダーにある klbackup ユーティリティを実行します。

   バックアップと復元ウィザードが起動します。

2. ウィザードの最初のウィンドウで、［**管理サーバーデータのバックアップを実行**］を選択します。

   ［**管理サーバーの証明書のみを復元またはバックアップする**］をオンにすると、管理サーバーの証明書のバックアップコピーと秘密鍵のみが保存されます。管理サーバー証明書と秘密鍵をバックアップしておくと、Kaspersky Security Center Windows の管理サーバーから Kaspersky Security Center Linux の管理サーバーへの移行を実行する時に役立ちます。また、管理対象デバイスを Kaspersky Security Center Linux 管理サーバー間、および Kaspersky Security Center Windows 管理サーバー間で移行することもできます。詳細については、「klbackup ユーティリティを使用して、別の管理サーバーの管理下にある管理対象デバイスを切り替える」を参照してください。

   ［**次へ**］をクリックします。

3. ウィザードの次のウィンドウで、次のオプションを指定します：

- **バックアップの保存先フォルダー**
- **MySQL/MariaDB 形式へ移行**

  SQL Server を管理サーバーの DBMS として使用中で、データを MySQL または MariaDB DBMS へ移行する場合に、このオプションをオンにします。MySQL および MariaDB と互換性があるバックアップが作成されます。その後、データをバックアップから MySQL または MariaDB へ復元することができます。

- **Azure 形式へ移行**

  SQL Server を管理サーバーの DBMS として使用中で、データを SQL Server から Azure SQL DBMS へ移行する場合に、このオプションをオンにします。Azure SQL と互換性があるバックアップが作成されます。その後、データをバックアップから Azure SQL へ復元することができます。

- **現在の日時をバックアップ先のフォルダー名に含めます**
- **バックアップのパスワード**

4. ［**次へ**］をクリックし、バックアップを開始します。
5. Amazon Web Services（AWS）または Microsoft Azure のクラウド環境のデータベースを使用している場合、［**オンラインストレージへサインイン**］ウィンドウで、次のフィールドに情報を入力してください。
   - AWS の場合：
     - **S3 バケット名**

       バックアップ用に作成した S3 バケットの名前です。

     - **アクセスキーの ID**

       S3 バケットストレージインスタンスを使用するために IAM ユーザーアカウントを作成した時に受け取ったキーの ID（英数字の並び）です。

       このフィールドは、S3 バケット上の RDS データベースを選択した場合に使用可能になります。

     - **秘密鍵**

       IAM ユーザーアカウント作成時にアクセスキーの ID と一緒に受け取った秘密鍵です。

       秘密鍵の文字はアスタリスクで表示されます。秘密鍵を入力し始めると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを必要な間だけ押し続けます。

       このフィールドは、IAM ロールではなく AWS IAM アクセスキーを認証のために選択した場合に使用できます。

   - Microsoft Azure の場合：
     - **Azure ストレージアカウント名**

       Kaspersky Security Center で使用するために作成した Azure ストレージアカウントの名前です。

- **Azure サブスクリプション ID**

  Azure ポータルで作成したサブスクリプションです。

- **Azure パスワード**

  アプリケーション ID の作成時に取得したアプリケーション ID のパスワードです。

  パスワードの文字はアスタリスクで表示されます。パスワードの入力を開始すると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを押し続けます。

- **Azure アプリケーション ID**

  Azure ポータルで作成したアプリケーション ID です。

  ポーリングやその他の目的で使用する Azure アプリケーション ID を 1 つだけ指定できます。別の Azure セグメントでポーリングを実行する場合は、既存の Azure 接続を事前に削除する必要があります。

- **Azure SQL サーバー名**

  この名前とリソースグループは Azure SQL サーバーのプロパティで確認できます。

- **Azure SQL サーバーリソースグループ**

  この名前とリソースグループは Azure SQL サーバーのプロパティで確認できます。

- **Azure ストレージのアクセスキー**

  情報はストレージアカウントのプロパティの［アクセスキー］セクションで確認できます。いずれのキー（key1 または key2）も使用できます。

管理サーバーデータを対話モードで復元するには：

1. Kaspersky Security Center のインストールフォルダーにある klbackup ユーティリティを実行します。
   klbackup ユーティリティは、管理サーバーをインストールした時と同じアカウントで起動する必要があります。新しくインストールした管理サーバーでユーティリティを実行することを推奨します。

   バックアップと復元ウィザードが起動します。

2. ウィザードの最初のウィンドウで、［**管理サーバーデータを復元**］を選択し、その後［**次へ**］をクリックします。

   ［**管理サーバーの証明書のみを復元またはバックアップする**］をオンにすると、管理サーバー証明書と秘密鍵のみが復元されます。

   非アクティブなフェールオーバークラスターノードで klbackup ユーティリティを実行すると、管理サーバー証明書を指定するか、管理サーバーからデータを自動的に取得するかのいずれかのオプションを選択するように要求されます。

3. ウィザードの［**設定の復元**］ウィンドウで、次の操作を実行します：

   - 管理サーバーデータのバックアップコピーがあるフォルダーを指定します。

AWS または Azure のクラウド環境を使用している場合、ストレージのアドレスを指定してください。ファイルが backup.zip という名前になっていることを確認してください。

- データのバックアップ時に入力したパスワードを指定します。

  データを復元する時は、バックアップ時に入力したパスワードを指定します。共有フォルダーへのパスがバックアップ後に変更された場合は、復元されたデータを使用するタスクの操作（復元タスクとリモートインストールタスク）を確認します。必要に応じて、これらのタスクの設定を編集します。バックアップファイルからのデータの復元中は、共有フォルダーまたは管理サーバーにアクセスしないでください。klbackup ユーティリティを開始するアカウントは、共有フォルダーへのフルアクセスの権限を持っている必要があります。

4. ［**次へ**］をクリックし、データを復元します。

サイレントモードでのデータのバックアップと復元

サイレントモードでバックアップコピーを作成または管理サーバーデータを復元するには：

管理サーバーがインストールされているデバイスのコマンドラインで、必要なキーを指定して klbackup を実行します。

ユーティリティのコマンドライン構文は次の通りです：

```
klbackup -path BACKUP_PATH [-linux_path LINUX_PATH][-node_cert CERT_PATH] [-logfile
LOGFILE] [-use_ts]|[-restore] [-password PASSWORD] [-cert_only] [-online]
```

klbackup ユーティリティのコマンドラインでパスワードを指定しないと、対話形式でパスワードを入力するように指示されます。

キーの説明：

- `-path` <バックアップパス> – <バックアップパス> で指定したフォルダーに情報を保存します。または、<バックアップパス> で指定したフォルダーのデータを使用して復元を実行します（必須パラメータ）。

  データベースサーバーのアカウントと klbackup ユーティリティには、<バックアップパス> で指定したフォルダーのデータを変更するアクセス権を付与する必要があります。

- `-linux_path <LINUX` パス> — Linux 上の SQL サーバーのバックアップデータが含まれるフォルダーへのローカルパス。

  データベースサーバーのアカウントと klbackup ユーティリティには、フォルダー LINUX_PATH のデータを変更するアクセス権を付与する必要があります。

- `-node_cert` <証明書のパス> — 回復後に非アクティブなフェールオーバークラスターノードを設定するためのサーバー証明書ファイル。設定されていない場合は、サーバーから自動的に取得されます。

  非アクティブなフェールオーバークラスターノードで klbackup ユーティリティを実行する場合は、このライセンスを使用してサーバー証明書へのパスを指定します。

- `-logfile` <ログファイル名> – 管理サーバーデータのバックアップと復元に関するレポートを保存します。

- `-use_ts` – データを保存する時に、<バックアップパス> で指定したフォルダーの、現在のシステム日付と処理時刻が付いたサブフォルダー（`klbackup YYYY-MM-DD # HH-MM-SS` 形式）に情報をコピーします。キーを指定しない場合は、<バックアップパス> で指定したフォルダーのルートに保存されます。

既にバックアップコピーがあるフォルダーに情報を保存しようとすると、エラーメッセージが表示されます。情報は更新されません。

`-use_ts` キーを使用することで、管理サーバーデータのアーカイブを保持することができます。たとえば、`-path` キーにフォルダー `C:\KLBackups` を指定した場合、フォルダー `klbackup 2022/6/19 # 11-30-18` には、2022 年 6 月 19 日午前 11 時 30 分 18 秒時点の管理サーバーのステータス情報が保存されます。

- `-restore` – 管理サーバーデータを復元します。データ復元は <バックアップパス> で指定したフォルダーの情報に基づいて実行されます。このキーを指定しない場合、データは <バックアップパス> で指定したフォルダーにバックアップされます。

- `-password <パスワード>` – 機密データを保護するためのパスワード。

  パスワードを忘れた場合、復元できません。パスワードに条件はありません。パスワードの長さは無制限です。また、0 文字（パスワードを設定しない）も可能です。

  データを復元する時は、バックアップ時に入力したパスワードを指定します。共有フォルダーへのパスがバックアップ後に変更された場合は、復元されたデータを使用するタスクの操作（復元タスクとリモートインストールタスク）を確認します。必要に応じて、これらのタスクの設定を編集します。バックアップファイルからのデータの復元中は、共有フォルダーまたは管理サーバーにアクセスしないでください。klbackup ユーティリティを開始するアカウントは、共有フォルダーへのフルアクセスの権限を持っている必要があります。新しくインストールした管理サーバーでユーティリティを実行することを推奨します。

- `-cert_only` – 管理サーバーの証明書と秘密鍵のみを保存または回復します。

  このフラグは、Kaspersky Security Center Windows の管理サーバーから Kaspersky Security Center Linux の管理サーバーへの移行を実行する時に役立ちます。また、管理対象デバイスを Kaspersky Security Center Linux 管理サーバー間および Kaspersky Security Center Windows 管理サーバー間で移行することもできます。

- `-online` – 不具合などによる管理サーバーのオフライン時間を最小限にするために、ボリュームスナップショットを作成して管理サーバーのデータをバックアップします。データを復元するためにこの機能を使用する場合は、このオプションは必要ありません。

klbackup ユーティリティを使用して、別の管理サーバーの管理下にある管理対象デバイスを切り替える

klbackup ユーティリティを使用すると、別の管理サーバーの管理下にある管理対象デバイスを切り替えることができます。移行を実行する時に、klbackup ユーティリティを使用して、Kaspersky Security Center Windows 管理サーバーを Kaspersky Security Center Linux 管理サーバーに変更できます。また、管理対象デバイスを Kaspersky Security Center Linux 管理サーバー間、および Kaspersky Security Center Windows 管理サーバー間で移行することもできます。

klbackup ユーティリティを使用して、別の管理サーバーの管理下にある管理対象デバイスを切り替えるには、次の手順を実行します：

1. 以前のデバイスで、管理サーバー証明書と秘密鍵のバックアップコピーを作成します。

   次のいずれかの方法でバックアップコピーを作成できます：

   - klbackup ユーティリティインターフェイスを使用する（Kaspersky Security Center Windows 管理サーバーのみ）

     Kaspersky Security Center インストールフォルダーにある klbackup ユーティリティを実行し、［**管理サーバーの証明書のみを復元またはバックアップする**］を使用してバックアップを作成します。

- コマンドプロンプトを使用する（Kaspersky Security Center Windows および Kaspersky Security Center Linux 管理サーバーバージョン 15.1 以降）

  管理サーバー証明書と秘密鍵のバックアップコピーを作成するには、コマンドラインから `-cert_only` キーを指定して klbackup ユーティリティを実行します。

  ```
  klbackup -path <管理サーバー証明書のバックアップコピーへのパス> -cert_only
  ```

2. 前のデバイスで、管理サーバーをネットワークから切断します。

3. 別の管理サーバーを使用してデバイスに同じアドレスを割り当てます。

   新しい管理サーバーに NetBIOS 名、FQDN、および固定 IP アドレスを割り当てることができます。これは、ネットワークエージェントが導入された時にネットワークエージェントのインストールパッケージで設定された管理サーバーのアドレスによって異なります。あるいは、ネットワークエージェントが接続する管理サーバーを決定する接続アドレスを使用することもできます（管理対象デバイスでこのアドレスを取得するには、klnagchk ユーティリティを使用します）。

4. 別の管理サーバーがあるデバイスで、バックアップコピーから管理サーバー証明書と秘密鍵を復元します。

   次のいずれかの方法でバックアップコピーを復元できます：

   - klbackup ユーティリティインターフェイスを使用する（Kaspersky Security Center Windows 管理サーバーのみ）

     klbackup ユーティリティを実行し、［**管理サーバーの証明書のみを復元またはバックアップする**］を使用してバックアップを復元します。

   - コマンドプロンプトを使用する（Kaspersky Security Center Windows および Kaspersky Security Center Linux 管理サーバーバージョン 15.1 以降）

     管理サーバー証明書と秘密鍵のバックアップコピーを復元するには、コマンドラインから `-cert_only` キーを指定して klbackup ユーティリティを実行します：

     ```
     klbackup -path <管理サーバー証明書のバックアップコピーへのパス> -restore -cert_only
     ```

管理対象デバイスは別の管理サーバーの管理下に置かれます。この管理サーバーにアクセスし、管理対象デバイスがネットワークで表示されていること、ネットワークエージェントがインストールされ、実行されていることを確認できます（［**可視**］、［**ネットワークエージェントがインストール済み**］、［**ネットワークエージェントが実行中**］列の［*はい*］の値）。

管理サーバーの別のデバイスへの移動

新しいデバイスで管理サーバーを使用する必要がある場合は、次のいずれかの方法で移動できます：

- 管理サーバーおよび定義データベースサーバーを新しいデバイスに移動します（定義データベースサーバーは、管理サーバーと一緒に新しいデバイスにインストールすることも、別のデバイスにインストールすることもできます）。

- データベースサーバーを以前のデバイスに保持し、管理サーバーのみを新しいデバイスに移動する。

管理サーバーを新しいデバイスへ移動するには：

1. 以前のデバイスで、管理サーバーデータのバックアップを作成します。

   このためには、管理コンソールからデータバックアップタスクを実行するか、klbackup ユーティリティを実行します。

SQL Server を管理サーバーの DBMS として使用している場合、SQL Server から MySQL または MariaDB DBMS へデータを移行できます。これを行うには、klbackup ユーティリティを対話モードで実行して、データバックアップを作成します。バックアップと復元ウィザードの［**バックアップ設定**］ウィンドウで［**MySQL/MariaDB 形式へ移行**］をオンにします。MySQL および MariaDB と互換性があるバックアップが作成されます。その後、データをバックアップから MySQL または MariaDB へ復元することができます。

SQL Server から Azure SQL DBMS にデータを移行する場合は、［**Azure 形式へ移行**］オプションをオンにすることもできます。

2. 前のデバイスで、管理サーバーをネットワークから切断します。

3. 管理サーバーをインストールする新しいデバイスを選択します。選択したデバイスのハードウェアとソフトウェアが、管理サーバー、管理コンソール、およびネットワークエージェントの要件を満たしていることを確認してください。また、管理サーバーで使用されるポートが使用可能であることを確認してください。

4. 新しいデバイスに同じアドレスを割り当てます。

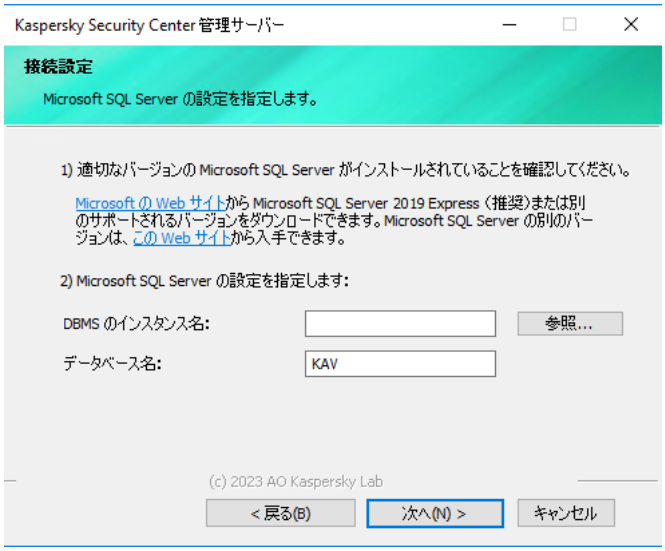
   新しい管理サーバーに NetBIOS 名、FQDN、および固定 IP アドレスを割り当てることができます。これは、ネットワークエージェントが導入された時にネットワークエージェントのインストールパッケージで設定された管理サーバーのアドレスによって異なります。あるいは、ネットワークエージェントが接続する管理サーバーを決定する接続アドレスを使用することもできます（管理対象デバイスでこのアドレスを取得するには、klnagchk ユーティリティを使用します）。

5. 必要に応じて、別のデバイスに管理サーバーが使用するデータベース管理システム（DBMS）をインストールします。

   定義データベースは、管理サーバーと一緒に新しいデバイスにインストールすることも、別のデバイスにインストールすることもできます。このデバイスがハードウェアおよびソフトウェアの要件を満たしていることを確認してください。DBMS を選択する際は、管理サーバーが対応するデバイスの数を考慮してください。

6. 新しいデバイスで管理サーバーのインストールを実行します。

7. 管理サーバーのインストール中に、定義データベースサーバーの接続設定を構成します。



Microsoft SQL Server の［接続設定］ウィンドウの例

データベースサーバーを配置する必要がある場所に応じて、次のいずれかを実行します：

- **データベースサーバーを以前のデバイスに保持する**

  1. ［**DBMS のインスタンス名**］の横にある［**参照**］をクリックし、表示されるリストで以前のデバイスの名前を選択します。

     新しい管理サーバーに接続するためには、以前のデバイスを使用できる必要があります。

  2. ［**データベース名**］に以前のデータベース名を入力します。

- **定義データベースサーバーを新しいデバイスに移動する**

  1. ［**DBMS のインスタンス名**］の横にある［**参照**］をクリックし、表示されるリストで新しいデバイス名を選択します。

  2. ［**データベース名**］に新しいデータベース名を入力します。

     なお、新しいデータベース名は、以前のデバイスのデータベース名と一致している必要があります。管理サーバーのバックアップを使用できるように、データベースの名前は同一である必要があります。既定のデータベース名は *KAV* です。

8. インストールが完了したら、klbackup ユーティリティを使用して、新しいデバイスで管理サーバーのデータを復元します。

   以前のデバイスと新しいデバイスで SQL Server を DBMS として使用する場合、新しいデバイスにインストールされている SQL Server のバージョンは、以前のデバイスにインストールされている SQL Server のバージョンと同じかそれ以降である必要があります。それ以外のバージョンの場合、新しいデバイスで管理サーバーのデータを復元できません。

9. 管理コンソールを開き、管理サーバーに接続します。

10. すべての管理対象デバイスが管理サーバーに接続されていることを確認します。

11. 以前のデバイスから管理サーバーとデータベースサーバーをアンインストールします。

Kaspersky Security Center Web コンソールを使用して、管理サーバーとデータベースサーバーを別のデバイスに移動することもできます。

複数の管理サーバー間での競合の回避

ネットワーク上に複数の管理サーバーがある場合、これらの管理サーバー上で同じクライアントデバイスが可視になる可能性があります。これにより、たとえば同じデバイスへの同じアプリケーションのリモートインストールが複数の管理サーバーから実行されるなどの競合が発生する場合があります。こうした状況を回避するため、Kaspersky Security Center 15.1 では別の管理サーバーの管理対象デバイスへのアプリケーションのインストールを防ぐように設定できます。

また、［**別の管理サーバーの管理対象**］属性は、次の用途の識別条件としても使用できます：

- デバイスの検索

- デバイスの抽出
- デバイス移動ルール
- 自動タグルール

Kaspersky Security Center 15.1 は、ヒューリスティックスを使用して、クライアントデバイスが現在操作中の管理サーバーの管理対象か、それとも別の管理サーバーの管理対象かを判定します。

二段階認証

このセクションでは、管理サーバーまたは Kaspersky Security Center Web コンソールへの不正なアクセスのリスクを軽減するために二段階認証を使用する方法と、Kaspersky Security Center のセキュリティ設定について説明します。

シナリオ：すべてのユーザーに対して二段階認証を設定する

このシナリオでは、すべてのユーザーに対して二段階認証を有効にする方法と、二段階認証からユーザーアカウントを除外する方法について説明します。別のユーザーに対する二段階認証を有効にする前に自分のアカウントの二段階認証を有効にしなかった場合、本製品は最初にお使いのアカウントの二段階認証を有効にするウィンドウを開きます。このシナリオでは、自分のアカウントに対して二段階認証を有効にする方法についても説明します。

自分のアカウントの二段階認証を有効にした後、すべてのユーザーに対して二段階認証を有効にする手順に進んでください。

必須条件

開始する前に：

- ご自分のアカウントに、別のユーザーのアカウントのセキュリティ設定を変更するための［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限があることを確認してください。
- 管理サーバーの他のユーザーがデバイス上に認証アプリをインストール済みであることを確認してください。

実行するステップ

すべてのユーザーに対して二段階認証を段階的に有効にするには：

1. **認証アプリをデバイスにインストールする**

   時間ベースのワンタイムパスワードのアルゴリズム（TOTP）をサポートする任意のアプリケーションをインストールできます。たとえば：

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP

- Yandex Key
- Avanpost Authenticator
- Aladdin 2FA

Kaspersky Security Center が使用する認証アプリをサポートしているかどうかを確認するには、すべてのユーザーまたは特定のユーザーに対して二段階認証を有効にします。

手順の1つでは、認証アプリによって生成されたセキュリティコードを指定することを推奨しています。成功すると、Kaspersky Security Center は選択した認証システムをサポートします。

> 管理サーバーへの接続が確立されているデバイスと同じデバイスに認証アプリをインストールすることは強く推奨しません。

2. **管理サーバーがインストールされているデバイスの時刻と、認証アプリの時刻を同期する**

   外部時刻ソースを使用して、認証アプリを備えたデバイスの時刻と、管理サーバーを備えたデバイスの時刻が UTC に同期されていることを確認します。そうしないと、認証および二段階認証のアクティブ化中に失敗が発生する可能性があります。

3. **自分のアカウントの二段階認証を有効にし、アカウントの秘密鍵を受け取る**

   実行手順の説明：

   - MMC ベースの管理コンソール：自分のアカウントの二段階認証を有効にする
   - Kaspersky Security Center Web コンソール：自分のアカウントの二段階認証を有効にする

   自分のアカウントの二段階認証を有効にした後、すべてのユーザーに対して二段階認証を有効にできるようになります。

4. **すべてのユーザーに対して二段階認証を有効にする**

   二段階認証を有効にしたユーザーは、管理サーバーにログインする際に二段階認証を使用する必要があります。

   実行手順の説明：

   - MMC ベースの管理コンソール：すべてのユーザーに対して二段階認証を有効にする
   - Kaspersky Security Center Web コンソール：すべてのユーザーに対して二段階認証を有効にする

5. **セキュリティコードの発行元の名前を変更する**

   同じ名前の管理サーバーがある場合は、異なる管理サーバーとして認識できるように、セキュリティコードの発行元の名前を別のものに変更する必要があります。

   実行手順の説明：

   - MMC ベースの管理コンソール：セキュリティコードの発行元の名前を変更する
   - Kaspersky Security Center Web コンソール：セキュリティコードの発行元の名前を変更する

6. **二段階認証を有効にする必要のないユーザーアカウントを除外する**

   必要に応じて、二段階認証からユーザーを除外することができます。アカウントが除外されたユーザーは管理サーバーへのログインの際に二段階認証が不要となります。

   実行手順の説明：

- MMC ベースの管理コンソール：二段階認証からアカウントを除外する
- Kaspersky Security Center Web コンソール：二段階認証からアカウントを除外する

7. **自分のアカウントの二段階認証を設定します**

   ユーザーが二段階認証から除外されておらず、アカウントに二段階認証がまだ設定されていない場合は、Kaspersky Security Center にサインインする時に開くウィンドウで設定する必要があります。そうしないと、権限に従って管理サーバーにアクセスできなくなります。

   実行手順の説明：

   - MMC ベースの管理コンソール：自分のアカウントの二段階認証を設定します
   - Kaspersky Security Center Web コンソール：自分のアカウントの二段階認証を設定します

結果

このシナリオの完了時には：

- 自分のアカウントの二段階認証が有効になります。
- 除外したユーザーアカウント以外の管理サーバーのすべてのユーザーアカウントに対して、二段階認証が有効になります。

二段階認証の概要

アカウントの二段階認証が有効になっている場合、管理コンソールまたは Kaspersky Security Center Web コンソールにログインするには、ユーザー名とパスワードに加えて、1回のみ使用するセキュリティコードが必要です。ドメイン認証を有効にすると、ユーザーは1回のみ使用するセキュリティコードを入力するだけで済みます。

二段階認証を使用するには、1回のみ使用するセキュリティコードを生成する認証アプリをモバイルデバイスまたはコンピュータにインストールする必要があります。時間ベースのワンタイムパスワードのアルゴリズム（TOTP）をサポートする任意のアプリケーションを使用できます。たとえば：

- Google Authenticator
- Microsoft Authenticator
- Bitrix24 OTP
- Yandex Key
- Avanpost Authenticator
- Aladdin 2FA

Kaspersky Security Center が使用する認証アプリをサポートしているかどうかを確認するには、すべてのユーザーまたは特定のユーザーに対して二段階認証を有効にします。

手順の1つでは、認証アプリによって生成されたセキュリティコードを指定することを推奨しています。成功すると、Kaspersky Security Center は選択した認証システムをサポートします。

秘密鍵または QR コードを保存し、安全な場所に保管することを強く推奨します。これにより、モバイルデバイスにアクセスできなかった際に Kaspersky Security Center Web コンソールへのアクセスを復元することができます。

Kaspersky Security Center を安全に使用するため、自分のアカウントに対して二段階認証を設定し、すべてのユーザーに対して二段階認証を有効にできます。

二段階認証からアカウントを除外することができます。これは認証のためのセキュリティコードを受信できないサービスアカウントで必要となる場合があります。

ルールと制限事項

すべてのユーザーに対して二段階認証を有効にし、特定のユーザーに対して二段階認証を無効にするには：

- アカウントが［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限を持っていることを確認します。
- アカウントの二段階認証を有効にする。

すべてのユーザーの二段階認証を無効にするには：

- アカウントが［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限を持っていることを確認します。
- 二段階認証を使用して Kaspersky Security Center Web コンソールにログインします。

Kaspersky Security Center 管理サーバーのバージョン 13 以降でユーザーアカウントに二段階認証が有効になっている場合、Kaspersky Security Center Web コンソールのバージョン 12、12.1 または 12.2 にユーザーはログインできません。

秘密鍵の再発行

二段階認証に使用する秘密鍵は、どのユーザーでも再発行できます。ユーザーが再発行された秘密鍵を使用して管理サーバーにログインすると、新しい秘密鍵がユーザーアカウントに保存されます。ユーザーが新しい秘密鍵を誤って入力した場合、新しい秘密鍵は保存されず、現在の秘密鍵は有効なままになります。

セキュリティコードには、*発行元の名前*として参照される識別子があります。セキュリティコードの発行元の名前は、認証アプリの管理サーバーの識別子として使用されます。既定では、セキュリティコードの発行元の名前は管理サーバーの名前と同じです。セキュリティコードの発行元の名前を変更することができます。セキュリティコードの発行元の名前を変更した後は、新しい秘密鍵を発行して認証アプリに渡す必要があります。

自分のアカウントの二段階認証を有効にする

アカウントの二段階認証を有効にする前に、お使いのモバイルデバイスに認証アプリがインストールされていることを確認してください。認証アプリケーションと管理サーバーの時刻が同期されていることを確認します。

アカウントの二段階認証を有効にするには：

1. Kaspersky Security Center のコンソールツリーで、［**管理サーバー**］フォルダーのコンテキストメニューを開いて、［**プロパティ**］を選択します。
2. 管理サーバーのプロパティウィンドウで［**セクション**］ペインに移動し、［**詳細**］→［**二段階認証**］の順に選択します。
3. ［**二段階認証**］セクションで、［**設定**］をクリックします。

   > アカウントで二段階認証が既に有効になっている場合は、［**設定**］をクリックすると秘密鍵がリセットされ、二段階認証を再設定できるようになります。

   表示される二段階認証のプロパティウィンドウに秘密鍵が表示されます。
4. 認証アプリに秘密鍵を入力して、ワンタイムセキュリティコードを受け取ります。この秘密鍵を認証アプリで手動で指定するか、お使いのモバイルデバイスの認証アプリで QR コードをスキャンします。
5. 認証アプリによって生成されたセキュリティコードを指定して、［**OK**］をクリックして二段階認証のプロパティウィンドウを終了します。
6. ［**適用**］をクリックします。
7. ［**OK**］をクリックします。

アカウントの二段階認証が有効になります。

すべてのユーザーに対して二段階認証を有効にする

お客様自身のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限があり、二段階認証を使用して認証済みである場合、管理サーバーのすべてのユーザーに対して二段階認証を有効にすることができます。

すべてのユーザーに対して二段階認証を有効にするには：

1. Kaspersky Security Center のコンソールツリーで、［**管理サーバー**］フォルダーのコンテキストメニューを開いて、［**プロパティ**］を選択します。
2. 管理サーバーのプロパティウィンドウにある［**セクション**］ペインで、［**詳細**］→［**二段階認証**］の順に選択します。
3. ［**必須に設定**］をクリックして、すべてのユーザーに対して二段階認証を有効にします。
4. 自分のアカウントの二段階認証を有効にしなかった場合、本製品は最初に自分のアカウントの二段階認証を有効にするウィンドウを開きます。

   a. 認証アプリに秘密鍵を入力して、ワンタイムセキュリティコードを受け取ります。この秘密鍵を認証アプリで手動で指定するか、お使いのモバイルデバイスの認証アプリで QR コードをスキャンすることによって、ワンタイムセキュリティコードを受け取ることができます。

   b. 認証アプリによって生成されたセキュリティコードを指定して、［**OK**］をクリックして二段階認証のプロパティウィンドウを終了します。

5. ［**二段階認証**］セクションで、［**適用**］をクリックし、［**OK**］をクリックします。

すべてのユーザーに対して二段階認証が有効になります。以降、このオプションを有効にする前に追加されたユーザーを含む管理サーバーのすべてのユーザーは、アカウントが二段階認証の対象から除外されたユーザー以外全員、アカウントに二段階認証を設定する必要があります。

ユーザーアカウントの二段階認証を無効にする

自分のアカウントの二段階認証を無効にするには：

1. Kaspersky Security Center のコンソールツリーで、［**管理サーバー**］フォルダーのコンテキストメニューを開いて、［**プロパティ**］を選択します。
2. 管理サーバーのプロパティウィンドウにある［**セクション**］ペインで、［**詳細**］→［**二段階認証**］の順に選択します。
3. ［**二段階認証**］セクションで、［**無効にする**］をクリックします。
4. ［**適用**］をクリックします。
5. ［**OK**］をクリックします。

自分のアカウントの二段階認証が無効になります。

他のユーザーのアカウントの二段階認証を無効にすることができます。ユーザーがデバイスを紛失したり破損したりした場合に、アカウントを保護します。

> 他のユーザーアカウントの二段階認証を無効にできるのは、お客様が**一般的な機能：ユーザー権限**のオブジェクト ACL の変更権限があり、二段階認証を使用して認証済みである場合のみです。また、次の手順で自分のアカウントに対する二段階認証も無効にすることができます。

ユーザーアカウントの二段階認証を無効にするには：

1. コンソールツリーで、［**ユーザーアカウント**］フォルダーを開きます。
   既定では、［**ユーザーアカウント**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。
2. ワークスペースで、二段階認証を無効にするユーザーアカウントをダブルクリックします。
   二段階認証が有効になっているすべてのユーザーアカウントでは、［**2FA が必要**］列が［**はい**］に設定されています。
3. 表示された［**プロパティ：<ユーザー名>**］ウィンドウで、［**二段階認証**］セクションを選択します。
4. ［**二段階認証**］セクションで、次のオプションを選択します：
   - ユーザーアカウントに対して二段階認証を無効にするには、［**無効にする**］をクリックします。
   - 二段階認証からユーザーアカウントを除外するには［**ユーザー名とパスワードの入力のみでユーザー認証を可能にする**］を選択します。
5. ［**適用**］をクリックします。
6. ［**OK**］をクリックします。

ユーザーアカウントに対する二段階認証が無効になります。

二段階認証を使用して管理コンソールにログインできないユーザーのアクセスを復元する場合は、このユーザーアカウントの二段階認証を無効にし、上記の説明に従って**二段階認証**で［**ユーザー名とパスワードの入力のみでユーザー認証を可能にする**］をオンにします。その後、二段階認証を無効にしたユーザーアカウントで管理コンソールにログインし、再度認証を有効にします。

全ユーザーに対して二段階認証の無効化

お客様自身のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限があり、二段階認証を使用して認証済みである場合、管理サーバーのすべてのユーザーに対して必要な二段階認証を無効にすることができます。

すべてのユーザーに対して二段階認証を無効にするには：

1. Kaspersky Security Center のコンソールツリーで、［**管理サーバー**］フォルダーのコンテキストメニューを開いて、［**プロパティ**］を選択します。
2. 管理サーバーのプロパティウィンドウにある［**セクション**］ペインで、［**詳細**］→［**二段階認証**］の順に選択します。
3. ［**任意に設定**］をクリックして、すべてのユーザーに対して二段階認証を無効にします。
4. ［**二段階認証**］セクションで、［**適用**］をクリックします。
5. ［**二段階認証**］セクションで、［**OK**］をクリックします。

すべてのユーザーに対して二段階認証が無効になります。全ユーザーに対して二段階認証を無効にしても、以前に二段階認証が個別に有効になっていた特定のアカウントには適用されません。

二段階認証からアカウントを除外する

使用中のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限がある場合は、二段階認証からアカウントを除外することができます。

ユーザーアカウントが二段階認証から除外された場合、そのユーザーは二段階認証を使用せずに管理コンソールまたは Kaspersky Security Center Web コンソールにログインできます。

認証中にセキュリティコードをパスできないサービスアカウントの場合、二段階認証からアカウントを除外する必要がある場合があります。

二段階認証からユーザーアカウントを除外するには：

1. 管理サーバーのユーザーのリストを更新するため、Active Directory のアカウントを除外する場合は、最初に Active Directory のポーリングを実行する必要があります。
2. コンソールツリーで、［**ユーザーアカウント**］フォルダーを開きます。

既定では、［**ユーザーアカウント**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。

3. ワークスペースで、二段階認証から除外するユーザーアカウントをダブルクリックします。

4. 表示された［**プロパティ：<ユーザー名>**］ウィンドウで、［**二段階認証**］セクションを選択します。

5. 表示されたセクションで、［**ユーザー名とパスワードの入力のみでユーザー認証を可能にする**］を選択します。

6. ［**二段階認証**］セクションで、［**適用**］をクリックし、［**OK**］をクリックします。

ユーザーアカウントが二段階認証から除外されます。除外されたアカウントはユーザーアカウントのリストで確認できます。

セキュリティコードの発行元の名前を変更する

異なる管理サーバーに対して、複数の識別子（発行元）を設定することができます。別の管理サーバーに同じようなセキュリティコードの発行元の名前が使用されている場合などに、別のセキュリティコードの発行元の名前に変更することができます。既定では、セキュリティコードの発行元の名前は管理サーバーの名前と同じです。

セキュリティコードの発行元の名前を変更した後は、新しい秘密鍵を発行して認証アプリに渡す必要があります。

セキュリティコードの発行元の名前を指定するには：

1. Kaspersky Security Center のコンソールツリーで、［**管理サーバー**］フォルダーのコンテキストメニューを開いて、［**プロパティ**］を選択します。

2. 管理サーバーのプロパティウィンドウにある［**セクション**］ペインで、［**詳細**］→［**二段階認証**］の順に選択します。

3. ［**セキュリティコードの発行者**］フィールドに、新しいセキュリティコードの発行元の名前を入力します。

4. ［**二段階認証**］セクションで、［**適用**］をクリックします。

5. ［**二段階認証**］セクションで、［**OK**］をクリックします。

管理サーバーに新しいセキュリティコードの発行元の名前が設定されます。

自分のアカウントの二段階認証を設定します

二段階認証を有効にした後、初めて Kaspersky Security Center にサインインすると、自分のアカウントの二段階認証を設定するためのウィンドウが開きます。

アカウントの二段階認証を設定する前に、使用中のモバイルデバイスに認証アプリがインストールされていることを確認してください。外部時刻ソースを使用して、認証アプリを備えたデバイスの時刻と、管理サーバーを備えたデバイスの時刻が UTC に同期されていることを確認します。

アカウントの二段階認証を設定するには：

1. モバイルデバイスの認証アプリを使用して、ワンタイムセキュリティコードを生成します。開くには、次のいずれかの操作を行います：

   - 認証アプリに秘密鍵を手動で入力します。
   - 認証アプリを使用して QR コードをスキャンします。

   モバイルデバイスにセキュリティコードが表示されます。

2. ［**二段階認証を設定**］ウィンドウで、認証アプリが生成したセキュリティコードを入力し、［**OK**］をクリックします。

アカウントには二段階認証が設定されています。自分の権利に従って管理サーバーにアクセスできます。

管理グループの管理

このセクションでは、管理グループの管理方法について説明します。

管理グループには次の処理を行うことができます：

- 任意の階層レベルのネストされたグループを管理グループに追加する
- デバイスを管理グループに追加する
- 個々のデバイスとグループ全体を別のグループに移動して、管理グループの階層を変更する
- ネストされたグループとデバイスを管理グループから削除する
- セカンダリ管理サーバーおよび仮想管理サーバーを管理グループに追加する
- 任意の管理サーバーの管理グループから別の管理サーバーの管理グループにデバイスを移動する
- グループに含まれているデバイスに自動的にインストールされるカスペルスキー製品を定義する

管理する管理グループ（またはその管理グループが属する管理サーバー）の［**管理グループの管理**］領域で［**変更**］権限を付与されている場合にのみ、これらの処理を実行できます。

管理グループの作成

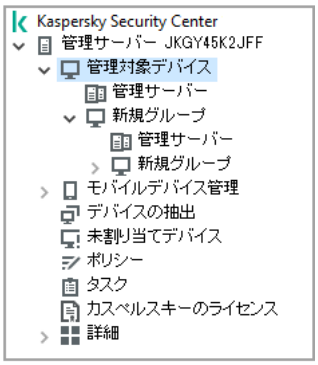
選択した管理グループの階層は、Kaspersky Security Center のメインウィンドウの［**管理対象デバイス**］フォルダー内に作成されます。管理グループはコンソールツリーにフォルダーとして表示されます（次の図を参照）。

Kaspersky Security Center のインストール直後は、［**管理対象デバイス**］フォルダーには空の［**管理サーバー**］フォルダーのみ含まれています。

ユーザーインターフェイス設定で、［**管理サーバー**］フォルダーをコンソールツリーに表示するかどうかを指定します。このフォルダーを表示するには、メニューバーで［**表示**］→［**インターフェイスの設定**］の順に選択し、開かれる［**インターフェイスの設定**］ウィンドウで［**セカンダリ管理サーバーの表示**］をオンにします。

管理グループの階層の作成時に、デバイスと仮想マシンを［**管理対象デバイス**］フォルダーに追加したり、ネストされたグループを追加したりできます。セカンダリ管理サーバーおよび仮想管理サーバーを［**管理サーバー**］フォルダーに追加できます。

［**管理対象デバイス**］フォルダーとまったく同様に、作成された各グループには、最初は空の［**管理サーバー**］フォルダーしか作成されていません。このフォルダーから同じグループのセカンダリ管理サーバーおよび仮想管理サーバーを操作します。このグループのポリシーとタスクに関する情報、およびこのグループに含まれるデバイスに関する情報は、このグループのワークスペース内の対応する名前のタブに表示されます。



管理グループ階層の表示

管理グループを作成するには：

1. コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。
2. 既存の管理グループのサブグループを作成するには、［**管理対象デバイス**］フォルダーで、新しい管理グループを含めるグループに対応するサブフォルダーを選択します。

   新しい最上位の管理グループを作成する場合は、このステップをスキップできます。
3. 次のいずれかの方法で管理グループの作成を開始します：
   - コンテキストメニューで、［**新規**］→［**グループ**］の順に選択します。
   - メインウィンドウの作業領域の［**デバイス**］タブにある［**新規グループ**］をクリックします。
4. ［**グループ名**］ウィンドウが表示されたら、グループの名前を入力し、［OK］をクリックします。

   指定した名前の新しい管理グループフォルダーがコンソールツリーに表示されます。

Active Directory またはドメインネットワークの構成に基づいて管理グループの階層を作成することが可能です。テキストファイルからグループの構成を作成することも可能です。

管理グループの構造を作成するには：

1. コンソールツリーで、［**管理対象デバイス**］フォルダーを選択します。
2. ［**管理対象デバイス**］フォルダーのコンテキストメニューで、［**すべてのタスク**］→［**グループ構造の新規作成**］の順に選択します。

新規管理グループ構造作成ウィザードが開始します。ウィザードの指示に従ってください。

管理グループの移動

ネストされた管理グループは、グループ階層内で移動できます。

グループを移動すると、すべてのネストされたグループ、セカンダリ管理サーバー、デバイス、グループポリシー、およびタスクも一緒に移動します。移動したグループには、管理グループ階層内の新しい位置に対応するすべての設定が適用されます。

グループの名前は、階層の1レベル内で一意である必要があります。管理グループを移動するフォルダー内に同じ名前のグループが既にある場合は、後者の名前を変更してください。移動するグループの名前を変更しなかった場合は、移動すると、**(1)**、**(2)** のような **(<次の連番>)** 形式のインデックスが名前に自動的に追加されます。

［**管理対象デバイス**］フォルダーは管理コンソールの組み込み要素であるため、名前を変更できません。

グループをコンソールツリーの別のフォルダーに移動するには：

1. コンソールツリーで移動するグループを選択します。
2. 次のいずれかの手順を実行します：
   - コンテキストメニューを使用してグループを移動します：
     1. グループのコンテキストメニューから［**切り取り**］を選択します。
     2. 選択したグループの移動先となる管理グループのコンテキストメニューで、［**貼り付け**］を選択します。
   - アプリケーションのメインメニューを使用してグループを移動します：
     a. メインメニューで、［**操作**］→［**切り取り**］を選択します。
     b. 選択したグループの移動先にする必要がある管理グループをコンソールツリーから選択します。
     c. メインメニューで、［**操作**］→［**貼り付け**］を選択します。
   - マウスを使用して、グループをコンソールツリーの別のグループに移動します。

管理グループの削除

管理グループを削除できるのは、そのグループ内にセカンダリ管理サーバー、ネストされたグループ、クライアントデバイスが含まれておらず、そのグループ用にグループタスクやポリシーが作成されていない場合です。

管理グループを削除する前に、そのグループからセカンダリ管理サーバー、ネストされたグループ、クライアントデバイスをすべて削除する必要があります。

グループを削除するには：

1. コンソールツリーで管理グループを選択します。
2. 次のいずれかの手順を実行します：
   - グループのコンテキストメニューから［**削除**］を選択します。
   - メインメニューで、［**操作**］→［**削除**］を選択します。
   - **DELETE** キーを押します。

管理グループの構造の自動作成

Kaspersky Security Center では、グループ構造作成ウィザードを使用して管理グループの構造を作成できます。

このウィザードは、次のデータに基づいて管理グループの構造を作成します：

- Windows ドメインとワークグループの構造
- Active Directory グループの構造
- 管理者が手動で作成するテキストファイルの内容

テキストファイルを生成する際は、次の要件を満たす必要があります：

- 各新規グループの名前は、改行して行頭から指定します。区切り文字は改行文字で開始する必要があります。空白行は無視されます。

  例：
  Office 1
  Office 2
  Office 3
  第 1 階層レベルの 3 つのグループが対象グループに作成されます。

- ネストされたグループの名前はスラッシュ記号（/）を使用して入力します。

  例：
  Office 1/Division 1/Department 1/Group 1
  ネストされた 4 つのサブグループが対象グループに作成されます。

- 同じ階層レベルに複数のネストされたグループを作成するには、「グループの絶対パス」を指定する必要があります。

  例：
  Office 1/Division 1/Department 1
  Office 1/Division 2/Department 1
  Office 1/Division 3/Department 1
  Office 1/Division 4/Department 1
  第 1 階層レベルの 1 つのグループ Office 1 が指定のグループに作成されます。このグループには同じ階層レベルの 4 つのネストされたグループ「Division 1」「Division 2」「Division 3」「Division 4」が含まれます。これらの各グループには、「Department 1」グループが含まれます。

ウィザードを使用して管理グループの階層を作成する場合、ネットワークの整合性に影響はありません：既存のグループを置き換える代わりに、新しいグループが追加されます。クライアントデバイスを管理グループに移動すると、［**未割り当てデバイス**］グループから削除されるため、そのクライアントデバイスを再び管理グループに含めることはできません。

管理グループ構造の作成中、デバイスが何らかの理由（停止していた、またはネットワークに接続されていなかった）で［**未割り当てデバイス**］グループに含まれていなかった場合、そのデバイスが管理グループに自動で移動されることはありません。ウィザードが完了したら、デバイスを手動で管理グループに追加できます。

管理グループの構造の自動作成を開始するには：

1. コンソールツリーで［**管理対象デバイス**］フォルダーを選択します。
2. ［**管理対象デバイス**］フォルダーのコンテキストメニューで、［**すべてのタスク**］→［**グループ構造の新規作成**］の順に選択します。

   新規管理グループ構造作成ウィザードが開始します。ウィザードの指示に従ってください。

管理グループ内のデバイスでのアプリケーションの自動インストール

管理グループ内のクライアントデバイスにカスペルスキー製品を自動的にリモートインストールする際に、使用するインストールパッケージを指定できます。

管理グループ内のデバイスでのアプリケーションの自動インストールを設定するには：

1. コンソールツリーで、目的の管理グループを選択します。
2. その管理グループのプロパティウィンドウを開きます。
3. ［**セクション**］ペインで［**自動インストール**］を選択し、ワークスペースで、デバイスにインストールするアプリケーションのインストールパッケージを選択します。
4. ［**OK**］をクリックします。

   グループタスクが作成されます。管理グループにクライアントデバイスが追加されるとすぐにそのクライアントデバイスで実行されます。

1つのアプリケーションの複数のインストールパッケージを自動インストールとして選択した場合、インストールタスクは最新のバージョンに対してのみ作成されます。

クライアントデバイスの管理

このセクションでは、クライアントデバイスの操作について説明します。

クライアントデバイスの管理サーバーへの接続

クライアントデバイスから管理サーバーへの接続はクライアントデバイスにインストールされたネットワークエージェントによって確立されます。

クライアントデバイスが管理サーバーに接続すると、次の処理が実行されます。

- データの自動的な同期
  - クライアントデバイスにインストールされたアプリケーションのリストの同期
  - ポリシー、アプリケーション設定、タスク、およびタスク設定の同期
- アプリケーションのステータス、タスクの実行、アプリケーションの管理サーバー別の動作統計情報に関する最新情報の取得
- 処理するイベント情報の管理サーバーへの配信

自動同期は、ネットワークエージェント設定に合わせて定期的に（たとえば 15 分ごとに）実行されます。接続間隔は手動で指定できます。

イベント情報は、イベントが発生するとすぐに管理サーバーに配信されます。

管理サーバーがリモートであり、企業ネットワークの外にある場合、クライアントデバイスはインターネット経由で管理サーバーに接続できます。

デバイスがインターネット経由で管理サーバーに接続するには、次の条件を満たしている必要があります：

- リモート管理サーバーに外部 IP アドレスを設定し、受信ポート 13000 を開放しておく必要があります（ネットワークエージェントの接続用）。UDP ポート 13000 の開放も推奨します（デバイスのシャットダウン通知の受信用）。
- ネットワークエージェントをデバイスにインストールします。
- デバイスにネットワークエージェントをインストールする時に、リモート管理サーバーの外部 IP アドレスを指定します。インストールパッケージを使用してインストールする場合は、インストールパッケージのプロパティの［**設定**］セクションに、外部 IP アドレスを手動で指定します。
- リモート管理サーバーを使用してデバイスのアプリケーションとタスクを管理するには、デバイスのプロパティウィンドウの［**全般**］セクションで、［**管理サーバーから切断しない**］をオンにします。その後、管理サーバーがリモートデバイスと同期されるまで待ちます。管理サーバーと常時接続できるクライアントデバイスの数は最大 300 です。

リモート管理サーバーによって開始されるタスクのパフォーマンスを高めるには、デバイスのポート 15000 を開きます。この場合、管理サーバーは、タスクを実行する際、デバイスとの同期が完了するまで待つことなく、ポート 15000 経由でネットワークエージェントに特別なパケットを送信します。

Kaspersky Security Center は、クライアントデバイスと管理サーバーの接続を設定して、すべての処理の完了後も接続をアクティブな状態にします。アプリケーションのステータスをリアルタイムで監視する必要がある場合や、管理サーバーがクライアントとの接続を何らかの理由（接続がファイアウォールで保護されている、クライアントデバイスのポートを開けない、クライアントデバイスの IP アドレスが不明など）で確立できない場合は、切断されない接続が必要です。デバイスのプロパティウィンドウの［**全般**］セクションで、クライアントデバイスと管理サーバー間で切断されることのない接続を確立することができます。

最も重要なデバイスとの間では、切断されることのない接続を確立してください。管理サーバーでは、同時に 300 件の接続までしか維持できません。

手動で同期される場合、システムでは、管理サーバーが接続を開始することができる補助的な接続方法が使用されます。クライアントデバイス上で接続を確立する前には、UDP ポートを開く必要があります。クライアントデバイスの UDP ポートには管理サーバーから接続要求が送信されます。これに対して、管理サーバーの証明書が検証されます。管理サーバーの証明書がクライアントデバイスに保存されている証明書のコピーと一致すると、接続が確立されます。

同期の手動による起動を使用して、アプリケーションのステータス、タスクの実行、およびアプリケーションの動作統計情報に関する最新情報を取得することもできます。

クライアントデバイスから管理サーバーへの手動接続：Klmover ユーティリティ

クライアントデバイスを管理サーバーに手動で接続する場合は、クライアントデバイスで klmover ユーティリティを使用します。

クライアントデバイスにネットワークエージェントをインストールすると、このユーティリティは自動的にネットワークエージェントのインストールフォルダーにコピーされます。

klmover ユーティリティを使用してクライアントデバイスから管理サーバーに手動で接続するには：

デバイスのコマンドラインで klmover ユーティリティを起動します。

コマンドラインから起動された場合、klmover ユーティリティでは（使用するライセンスに応じて）次の処理を実行できます：

- 特定の設定でネットワークエージェントを管理サーバーに接続する
- 処理結果をイベントログファイルに記録するか、画面に表示する

ユーティリティのコマンドライン構文は次の通りです：

```
klmover [-logfile <ファイル名>] [-address <サーバーのアドレス>] [-pn <ポート番号>] [-ps
<SSL ポート番号>] [-nossl] [-cert <証明書ファイルのパス>] [-silent] [-dupfix] [-virtserv]
[-cloningmode]
```

ユーティリティを実行するには管理者権限が必要です。

キーの説明：

- `-logfile <ファイル名>` – ユーティリティ実行結果をログファイルに記録します。
  既定では、情報は標準出力ストリーム（stdout）に保存されます。このキーを使用しない場合、結果とエラーメッセージは画面に表示されます。
- `-address <サーバーのアドレス>` – 接続する管理サーバーのアドレス。
  デバイスの IP アドレス、NetBIOS 名、DNS 名をアドレスとして指定できます。
- `-pn <ポート番号>` – 管理サーバーへの暗号化されていない接続が確立されるポートの番号。
  既定のポート番号は 14000 です。
- `-ps <SSL ポート番号>` – SSL を使用した管理サーバーへの暗号化接続の確立に使用する SSL ポートの番号。

既定のポート番号は 13000 です。

- `-nossl` – 管理サーバーへの暗号化されていない接続を使用します。

  このキーを使用しない場合、ネットワークエージェントは暗号化された SSL プロトコルを使用して管理サーバーに接続されます。

- `-cert <証明書ファイルのパス>` – 管理サーバーへのアクセス認証で使用する証明書ファイル。

  このキーを使用しない場合、ネットワークエージェントは管理サーバーへの初回接続時に証明書を取得します。

- `-silent` – サイレントモードでユーティリティを実行します。

  たとえば、ユーティリティをユーザーの登録のログインスクリプトから起動する場合など、このキーを使用すると便利な場合があります。

- `-dupfix` – このキーは、たとえば ISO ディスクイメージから復元している場合など、ネットワークエージェントが通常（配布パッケージの使用）とは異なる方法でインストールされている場合に使用されます。

- `-virtserv`：仮想管理サーバー名の指定。

- `-cloningmode`：ネットワークエージェントのディスククローンモード。

  次のパラメーターのいずれかを使用して、ディスクのクローンモードを構成します。

  - `-cloningmode`：ディスククローンモードのステータスを要求します。
  - `-cloningmode 1`：ディスククローンモードをオンにします。
  - `-cloningmode 0`：ディスククローンモードをオフにします。

たとえば、ネットワークエージェントを管理サーバーに接続するには、次のコマンドを実行します。

```
klmover  -address kscserver.mycompany.com -logfile klmover.log
```

クライアントデバイスと管理サーバー間のトンネリング接続

Kaspersky Security Center では、管理コンソールから管理サーバーを経由し、次にネットワークエージェントを経由して、管理対象デバイスの指定されたポートに到達する TCP 接続のトンネリングが可能です。トンネリングは、管理コンソールと管理対象デバイスを直接接続できない場合に、管理コンソールがインストールされたデバイスのクライアントアプリケーションを、管理対象デバイスの TCP ポートに接続するように設計されています。

たとえばトンネリングは、リモートデスクトップへの接続に使用され、既存セッションへの接続と新しいリモートセッションの作成の双方に対応しています。

トンネリングは、外部ツールを使用して有効にすることもできます。たとえば、管理者はこの方法で PuTTY ユーティリティ、VNC クライアント、およびその他のツールを実行できます。

クライアントデバイスと管理サーバー間のトンネリング接続は、管理サーバーへの接続に使用するポートがデバイスで使用できない場合に必要です。デバイスのポートは、次の場合に利用できないことがあります：

- リモートデバイスが NAT を使用するローカルネットワークに接続されている。
- リモートデバイスが管理サーバーのローカルネットワークの一部であるが、ファイアウォールによりポートが閉じられている。

クライアントデバイスと管理サーバー間のトンネリング接続を設定するには：

1. コンソールツリーで、クライアントデバイスを含むグループのフォルダーを選択します。
2. ［**デバイス**］タブで、デバイスを選択します。
3. デバイスのコンテキストメニューから、［**すべてのタスク**］→［**トンネリング接続**］の順に選択します。
4. 表示される［**トンネリング接続**］ウィンドウでトンネルを作成します。

クライアントデバイスのデスクトップへのリモート接続

管理者は、デバイスにインストールされているネットワークエージェントを使用して、クライアントデバイスのデスクトップへのリモートアクセスを取得できます。

ネットワークエージェントを使用したデバイスへのリモート接続は、クライアントデバイスの TCP ポートと UDP ポートが閉じている場合でも可能です。デバイスとの接続を確立すると、管理者はそのデバイスに保存されている情報へのフルアクセス権を取得できます。そのため、そのデバイスにインストールされているアプリケーションを管理することが可能です。

このセクションでは、ネットワークエージェントを介して Windows クライアントデバイスおよび macOS クライアントデバイスへの接続を確立する方法について説明します。

Windows クライアントデバイスへの接続

デバイスとのリモート接続は、次のいずれかの方法で確立できます：

- リモートデスクトップ接続という名前の標準の Microsoft Windows コンポーネントを使用します。

  リモートデスクトップへの接続は、ユーティリティの設定に従い、Windows の標準のユーティリティ mstsc.exe を使用して確立されます。

- Windows デスクトップ共有テクノロジーを使用します。

リモートデスクトップ接続による Windows クライアントデバイスへの接続

ユーザーの現在のリモートデスクトップのセッションへの接続は、ユーザーが認識することなく確立されます。管理者がセッションに接続すると、デバイスのユーザーは、事前の通知なくセッションから切断されます。

リモートデスクトップ接続を使用してクライアントデバイスのデスクトップに接続するには：

1. 管理コンソールツリーで、アクセスを取得する必要があるデバイスを選択します。
2. デバイスのコンテキストメニューから、［**すべてのタスク**］→［**デバイスに接続**］→［**RDP セッションの新規作成**］の順に選択します。

   Windows の標準ユーティリティ mstsc.exe が起動し、リモートデスクトップに接続されます。
3. ユーティリティのダイアログボックスに表示される指示に従います。

デバイスへの接続が確立されると、Microsoft Windows のリモートデスクトップ接続ウィンドウにデスクトップが表示されます。

Windows デスクトップ共有による Windows クライアントデバイスへの接続

リモートデスクトップの既存のセッションに接続する場合、デバイスのセッションユーザーは管理者から接続要求を受信します。デバイスのリモートからの動作とその結果に関する情報は、Kaspersky Security Center により作成されるレポートに保存されません。

管理者は、このセッションのユーザーを切断することなく、クライアントデバイスでの既存のセッションに接続することができます。この場合、管理者とデバイスのセッションユーザーが、デスクトップのアクセスを共有します。

管理者はリモートクライアントデバイスでのユーザー操作の監査を設定できます。監査中に、管理者が開いている（または変更している）クライアントデバイスのファイルの情報が保存されます。

Windows デスクトップ共有を使用してクライアントデバイスのデスクトップに接続するには、次の条件を満たす必要があります：

- Microsoft Windows Vista 以降の Windows オペレーティングシステムが管理ステーションにインストールされている。管理サーバーをホストしているデバイスのオペレーティングシステムの種別により、Windows デスクトップ共有を使用した接続に制限が適用されることはありません。

  使用する Windows のエディションに Windows デスクトップ共有機能が含まれているかどうかを確認するには、Windows レジストリに CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} キーがあることを確認します。

- Microsoft Windows Vista 以降の Windows オペレーティングシステムがクライアントデバイスにインストールされている。

- Kaspersky Security Center が、脆弱性とパッチ管理ライセンスを使用している。

Windows デスクトップ共有を使用してクライアントデバイスのデスクトップに接続するには：

1. 管理コンソールツリーで、アクセスを取得する必要があるデバイスを選択します。
2. デバイスのコンテキストメニューから、［**すべてのタスク**］→［**デバイスに接続**］→［**Windows デスクトップ共有**］の順に選択します。
3. ［**リモートデスクトップ接続を選択**］ウィンドウが表示されるので、接続する必要があるデバイスのセッションを選択します。

   デバイスへの接続が正常に確立すると、［**Kaspersky リモートデスクトップ接続ビューア**］ウィンドウにデバイスのデスクトップが表示されて使用可能になります。
4. デバイスとの対話を開始するには、［**Kaspersky リモートデスクトップ接続ビューア**］ウィンドウで、［**処理**］→［**対話モード**］の順に選択します。

［**Kaspersky リモートデスクトップ接続ビューア**］ユーティリティには商用ライセンスが必要です。

macOS クライアントデバイスへの接続

管理者は、Virtual Network Computing（VNC）システムを使用して macOS デバイスに接続できます。

リモートデスクトップへの接続は、管理サーバーデバイスにインストールされた VNC クライアントを介して確立されます。VNC クライアントは、キーボードとマウスの制御をクライアントデバイスから管理者に切り替えます。

管理者がリモートデスクトップに接続する際に、ユーザーは管理者からの通知や接続要求を受け取りません。管理者は、このセッションからユーザーを切断することなく、クライアントデバイスでの既存のセッションに接続します。

VNC クライアントを使用してクライアント macOS デバイスのデスクトップに接続するには、次の条件を満たす必要があります：

- VNC クライアントは、管理サーバーデバイスにインストールされます。
- クライアントデバイスでは、リモートログインとリモート管理が許可されます。
- ユーザーは、macOS オペレーティングシステムの**共有**設定で、クライアントデバイスへの管理者アクセスを許可します。

Virtual Network Computing システムを使用してクライアントデバイスのデスクトップに接続するには：

1. 管理コンソールツリーで、アクセスを取得する必要があるデバイスを選択します。
2. デバイスのコンテキストメニューから、［**すべてのタスク**］→［**トンネリング接続**］の順に選択します。
3. 表示される［**トンネリング接続**］ウィンドウで、次の操作を実行します：
   a. ［**1. ネットワークポート**］セクションで、接続する必要があるデバイスのネットワークポート番号を指定します。
      既定では、ポート 5900 が使用されます。
   b. ［**2. トンネリング**］セクションで、［**Create tunnel**］をクリックします。
   c. ［**3. ネットワーク設定**］セクションで、［**Copy**］をクリックします。
4. VNC クライアントを開き、コピーしたネットワーク属性をテキストフィールドに貼り付けます。**Enter** を押します。
5. 表示されたウィンドウで、証明書の詳細情報を表示します。証明書の使用に同意する場合は、［**Yes**］をクリックします。
6. ［**Authentication**］ウィンドウで、クライアントデバイスの資格情報を指定し、［**OK**］をクリックします。

Windows デスクトップ共有によるデバイスへの接続

Windows デスクトップ共有でデバイスに接続するには：

1. コンソールツリーで［**管理対象デバイス**］フォルダーの［**デバイス**］タブを選択します。
   このフォルダーの作業領域には、デバイスのリストが表示されます。
2. 接続するデバイスのコンテキストメニューで、［**デバイスに接続**］→［**Windows デスクトップ共有**］の順に選択します。
   ［**リモートデスクトップ接続を選択**］ウィンドウが表示されます。

3. ［**リモートデスクトップ接続を選択**］ウィンドウで、デバイスへの接続に使用するデスクトップセッションを選択します。

4. ［**OK**］をクリックします。

デバイスが接続されます。

クライアントデバイスの再起動の設定

Kaspersky Security Center を使用、インストール、または削除する場合には、デバイスを再起動する必要があります。再起動設定は、Windows が実行されているデバイスの場合にのみ設定できます。

クライアントデバイスの再起動を設定するには：

1. コンソールツリーで、再起動を設定する必要がある管理グループを選択します。

2. グループの作業領域で、［**ポリシー**］タブを選択します。

3. 作業領域で、ポリシーのリストにある Kaspersky Security Center ネットワークエージェントのポリシーを選択してから、ポリシーのコンテキストメニューで［**プロパティ**］を選択します。

4. ポリシーのプロパティウィンドウで［**再起動の設定**］セクションを選択します。

5. デバイスの再起動が必要な場合に実行すべき処理を選択します：

   - ［**OS を再起動しない**］を選択して、自動的な再起動をブロックする。
   - ［**必要に応じて自動的に OS を再起動する**］を選択して、自動的な再起動を許可する。
   - ［**ユーザーに処理を確認する**］を選択して、ユーザーが再起動できるようにする。

   再起動の処理を確認する間隔を指定するとともに、対応するチェックボックスをオンにすることにより、デバイスでセッションがブロックされたアプリケーションを強制的に再起動したり強制終了したりすることができます。

6. ［**OK**］をクリックして、変更内容を保存し、ポリシーのプロパティウィンドウを閉じます。

ここで、デバイスの再起動が設定されます。

リモートクライアントデバイスでの動作の監査

本製品では、Windows を実行しているリモートクライアントデバイスでの管理者の操作を監査することができます。監査中、管理者によって開かれたか変更されたファイルに関する情報がデバイスに保存されます。管理者の処理の監査が使用可能である条件は次の通りです：

- 脆弱性とパッチ管理のライセンスが使用されている
- 管理者がリモートデバイスのデスクトップに対する共有アクセスを開始する権限を持っている

リモートクライアントデバイスでの動作の監査を有効にするには：

1. コンソールツリーで、管理者の動作の監査を設定する必要がある管理グループを選択します。

2. グループの作業領域で、［**ポリシー**］タブを選択します。

3. Kaspersky Security Center ネットワークエージェントのポリシーを選択し、ポリシーのコンテキストメニューで［**プロパティ**］を選択します。

4. ポリシーのプロパティウィンドウで［**Windows デスクトップ共有**］セクションを選択します。

5. ［**監査を有効にする**］をオンにします。

6. ［**読み取り時に監視する必要のあるファイルのマスク**］および［**変更時に監視する必要のあるファイルのマスク**］リストで、監査中に動作を監視する必要のあるファイルマスクを追加します。

   既定では、拡張子が txt、rtf、doc、xls、docx、xlsx、odt、pdf のファイルの動作が監視されます。

7. ［**OK**］をクリックして、変更内容を保存し、ポリシーのプロパティウィンドウを閉じます。

これにより、デスクトップアクセスを共有しているユーザーのリモートデバイスでの管理者による操作の監査が設定されます。

リモートデバイスにおける管理者の処理の記録は次に保存されます：

- リモートデバイスのイベントログ
- リモートデバイスのネットワークエージェントフォルダーにある拡張子 syslog のファイル（C:\ProgramData\KasperskyLab\adminkit\1103\logs など）
- Kaspersky Security Center のイベントデータベース

クライアントデバイスと管理サーバー間の接続の確認

Kaspersky Security Center では、クライアントデバイスと管理サーバー間の接続を自動または手動で確認できます。

接続の自動確認は管理サーバーで実行されます。接続の手動確認はデバイスで実行されます。

クライアントデバイスと管理サーバー間の接続の自動確認

クライアントデバイスと管理サーバー間の接続の自動確認を開始するには：

1. コンソールツリーで、デバイスを含む管理グループを選択します。

2. 管理グループの作業領域の［**デバイス**］タブで、デバイスを選択します。

3. デバイスのコンテキストメニューで［**デバイスのアクセス可否の確認**］を選択します。

ウィンドウが開き、デバイスにアクセス可能かどうかに関する情報が表示されます。

クライアントデバイスと管理サーバー間の接続の手動確認：Klnagchk ユーティリティ

klnagchk ユーティリティを使用すると、クライアントデバイスと管理サーバー間の接続を確認し、接続設定に関する詳細情報を取得できます。klnagchk ユーティリティはネットワークエージェントのインストールフォルダーにあります。

klnagchk ユーティリティは、コマンドラインから起動すると、次の処理を実行します（使用するキーによって異なります）：

- デバイスにインストールされたネットワークエージェントから管理サーバーへの接続に使用される設定値を画面に表示するかログに記録する
- ネットワークエージェントの統計情報（前回の起動以降）とユーティリティ処理結果をイベントログファイルに記録するか画面に表示する
- ネットワークエージェントと管理サーバー間の接続の確立を試行する

  接続の試行に失敗した場合、ICMP パケットを送信して、管理サーバーがインストールされているデバイスの状態を確認します。

klnagchk ユーティリティを使用して、クライアントデバイスと管理サーバー間の接続を確認するには、

ネットワークエージェントがインストールされているデバイスで、ローカル管理者アカウントのコマンドラインから klnagchk ユーティリティを起動します。

ユーティリティのコマンドライン構文は次の通りです：

```
klnagchk [-logfile <ファイル名>] [-sp] [-savecert <証明書ファイルのパス>] [-restart][-sendhb]
```

キーの説明：

- `-logfile <ファイル名>`ーネットワークエージェントと管理サーバー間の接続設定値とユーティリティの処理結果をログファイルに記録します。

  既定では、情報は標準出力ストリーム（stdout）に保存されます。このキーを使用しない場合、設定、結果、エラーメッセージは画面に表示されます。
- `-sp`ープロキシサーバー上のユーザー認証パスワードを表示します。

  このライセンスは、プロキシサーバー経由で管理サーバーへの接続が確立される場合に使用されます。
- `-savecert <ファイル名>`ー管理サーバーへのアクセス認証用の証明書を指定したファイルに保存します。
- `-restart`ーユーティリティの処理完了後にネットワークエージェントを再起動します。
- `-sendhb`ーネットワークエージェントと管理サーバーの同期を開始します。

起動後、klnagchk ユーティリティはネットワークエージェントの設定情報ファイルにアクセスし、接続パラメータを表示します。これらのパラメータは、ネットワークエージェントのインストール時およびネットワークエージェントのポリシー設定で指定されます：

- `Current device`ークライアントデバイスの Windows ネットワークでの名前。
- `Network Agent version`ーデバイスにインストールされているネットワークエージェントのバージョンの（パッチまで含む）完全な数字。
- `Administration Server address`ー管理サーバーのアドレス。

- Use SSL－管理サーバーに接続する時にセキュアな接続が使用されるかどうかを示すパラメータ。
  指定可能な値：
  - 0－セキュアな接続は使用されません。
  - 1－セキュアな接続が使用されます。
- Compress traffic－クライアントデバイスと管理サーバー間のトラフィックが圧縮されるかどうかを示すパラメータ。
- Numbers of the Administration Server SSL ports－セキュアな接続を使用する場合の管理サーバーとの通信に有効なポート番号。
- Numbers of the Administration Server ports－通常の接続を使用する場合に管理サーバーと通信するために有効なポート番号。
- Use proxy server－プロキシサーバーが使用されるかどうかを示すパラメータ。
  指定可能な値：
  - 0－プロキシサーバーは使用されません。
  - 1－プロキシサーバーが使用されます。
- Address－プロキシサーバーのアドレスとポート（コロンで区切られます）。このパラメータは、プロキシサーバーが使用されている場合にのみ表示されます。
- User name－プロキシサーバーにアクセスするためのユーザー名。このパラメータは、プロキシサーバーが使用されている場合にのみ表示されます。
- Password－プロキシサーバーにアクセスするためのパスワード。このパラメータは、プロキシサーバーが使用されている場合にのみ表示されます。プロキシサーバーのパスワードを表示するには、コマンドで sp キーを使用する必要があります。
- Administration Server certificate－クライアントデバイスに管理サーバー証明書があるかどうかを示すパラメータ。たとえば、ネットワークエージェントが管理サーバーに一度も正常に接続したことがない場合は、証明書が存在しない可能性があります。
  指定可能な値：
  - not installed－クライアントデバイスに管理サーバー証明書がありません。
  - available－クライアントデバイスに管理サーバー証明書があります。
- Open UDP port－ネットワークエージェントが管理サーバーからの同期要求を受信するために UDP ポートを使用するかどうかを示すパラメータ。
  指定可能な値：
  - 0－管理サーバーからの同期要求を受信するための UDP ポートが閉じられています。
  - 1－管理サーバーからの同期要求を受信するために UDP ポートが開かれています。
- Numbers of UDP ports－ネットワークエージェントで使用できる UDP ポートの数。
- Location name－デバイスのネットワーク上の場所。

- State of network location－クライアントデバイスを1つの管理サーバー接続プロファイルから別の接続プロファイルに切り替えることができるかどうかを示すパラメータ。

  指定可能な値：

  - Enabled－クライアントデバイスの管理サーバー接続プロファイルを切り替えることができます。
  - Disabled－クライアントデバイスの管理サーバー接続プロファイルを切り替えることはできません。

- Profile to use－管理サーバーの接続プロファイル。
- Condition－クライアントデバイスが接続されているネットワークのIPアドレスとサブネットマスク。
- Synchronization interval (min)－同期の標準間隔。
- Connection timeout (in seconds)－接続タイムアウト。
- Send / receive timeout (in seconds)－読み取り/書き込み操作の接続タイムアウト。
- Device ID－ネットワーク内のデバイス識別子。Device IDは、特定の管理サーバーによって管理されるクライアントデバイス間で一意です。
- Locations of connection gateways－接続ゲートウェイを介してクライアントデバイスを管理サーバーに接続するためのパラメータ。
- Location of distribution points－ディストリビューションポイントを介してクライアントデバイスを管理サーバーに接続するためのパラメータ。
- Connection with server－接続ゲートウェイが管理サーバーに継続的に接続されているかどうかを示すパラメータ。このパラメータは、クライアントデバイスが接続ゲートウェイとして機能する場合にのみ表示されます。

  指定可能な値：

  - active－接続ゲートウェイは管理サーバーに継続的に接続されています。
  - inactive－接続ゲートウェイは管理サーバーに継続的に接続されていません。

- Connection with server through connection gateway－接続ゲートウェイを介した管理サーバーへの接続が正しく確立されているかどうかを示すパラメータ。このパラメータは、クライアントデバイスが接続ゲートウェイとして機能する場合にのみ表示されます。

  指定可能な値：

  - active－接続ゲートウェイを介した管理サーバーへの接続が正しく確立されています。
  - inactive－接続ゲートウェイを介した管理サーバーへの接続が正しく確立されていません。

また、klnagchkユーティリティの出力には、次のいずれかの行が含まれる場合があります：

- Administration Server is installed on this device－klnagchkユーティリティは管理サーバーデバイスで実行されます。
- This device has been assigned a connection gateway but is not yet registered on Administration Server－klnagchkユーティリティは、ネットワークエージェントがインストールされているデバイス上で、接続ゲートウェイモードで実行されます。設定された接続ゲートウェイは管理サーバーからの接続を待機していますが、管理サーバーが管理対象デバイス中のデバイスをリストしません。管理サーバーが接続ゲートウェイへの接続を開始するようにする必要があります。

- `This device is a connection gateway`－klnagchk ユーティリティは、接続ゲートウェイとして機能するデバイス上で実行されます。
- `Acts as a distribution point`－klnagchk ユーティリティは、ディストリビューションポイントとして機能するデバイス上で実行されます。

klnagchk ユーティリティは、ネットワークエージェントサービスのステータスをチェックします。サービスが実行されていない場合、ユーティリティは停止します。サービスが実行中の場合、ユーティリティは次の接続統計を表示します：

- `Total number of synchronization requests`－クライアントデバイスから管理サーバーへの接続試行回数。
- `The number of successful synchronization request`－クライアントデバイスから管理サーバーへの接続試行が成功した回数。
- `Total number of synchronizations`－クライアントデバイス設定と管理サーバー設定の同期試行回数。
- `The number of successful synchronizations`－クライアントデバイス設定と管理サーバーの同期試行が成功した回数。
- `Date/time of the last request for synchronization`－最後の接続の日時。

管理サーバーとネットワークエージェント間の接続を分析する時は、`Total number of synchronization requests`と`The number of successful synchronization request`パラメータを使用する必要があります。クライアントデバイスの設定は、管理サーバーの設定が変更された場合（たとえば、新しいタスクが追加された場合やポリシー設定が変更された場合）のみ、管理サーバーの設定と同期されます。それ以外の場合、`Total number of synchronizations`と`The number of successful synchronizations`のパラメータ値は変更されません。

ネットワークエージェントを管理サーバーに接続する際に発生する問題のトラブルシューティング方法の詳細については、Kaspersky Security Center の FAQ を参照してください。

デバイスと管理サーバー間の接続時間の確認について

デバイスのシャットダウン時に、ネットワークエージェントは管理サーバーにシャットダウンを通知します。管理コンソールでは、そのデバイスはシャットダウンと表示されます。ただし、ネットワークエージェントがすべてのシャットダウンを管理サーバーに通知できるわけではありません。そのため、管理サーバーは、各デバイスの［**管理サーバーへの接続**］属性（この属性の値は、管理コンソールのデバイスプロパティの［**全般**］セクションに表示されます）を定期的に分析し、ネットワークエージェントの現在の設定の同期間隔と比較します。あるデバイスが連続した同期間隔に 3 回を超えて応答していない場合、そのデバイスはシャットダウンとマーク付けされます。

管理サーバーでのクライアントデバイスの識別

クライアントデバイスは、名前に基づいて識別されます。デバイスの名前は、管理サーバーに接続しているすべてのデバイス名の中で一意です。

デバイスの名前は、Windows ネットワークでポーリングが実行されて新規デバイスが検出された時、またはデバイスにインストールされたネットワークエージェントが最初に管理サーバーに接続した時に、管理サーバーに送信されます。既定では、この名前は Windows ネットワーク上のデバイス名（NetBIOS 名）と一致します。この名前のデバイスが既に管理サーバーに登録されている場合、**<名前>-1**、**<名前>-2** のように連番が接尾辞として新規デバイスの名前に追加されます。デバイスは、この名前で管理グループに追加されます。

管理グループへのデバイスの移動

移動元と移動先の両方の管理グループ（またはこれらの管理グループが属する管理サーバー）の［**管理グループの管理**］の［**変更**］権限を付与されている場合のみ、デバイスを管理グループから別の管理グループに移動できます。

特定の管理グループに1台以上のデバイスを含めるには：

1. コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。
2. ［**管理対象デバイス**］フォルダーで、クライアントデバイスを含めるグループに対応するサブフォルダーを選択します。

   デバイスを［**管理対象デバイス**］グループに含める場合は、この手順を省略できます。
3. 選択した管理グループの作業領域の［**デバイス**］タブで、次のいずれかの方法により、デバイスをグループに含めるプロセスを実行します：

   - デバイスのリストの情報ボックスの［**デバイスをグループに移動**］をクリックして、デバイスをグループに追加する
   - デバイスリストのコンテキストメニューから［**作成**］→［**デバイス**］の順に選択する

   デバイス移動ウィザードが起動します。指示に従って、デバイスをグループに移動する方法を選択し、グループに含めるデバイスのリストを作成します。

   デバイスのリストを手動で作成する場合、デバイスのアドレスとしてIPアドレス（またはIPアドレスの範囲）、NetBIOS名、またはDNS名を使用できます。リストに手動で移動できるのは、デバイスへの接続時に、またはデバイスの検出後に、管理サーバーのデータベースに既に情報が追加されているデバイスのみです。

   ファイルからデバイスのリストをインポートするには、追加するデバイスのアドレスのリストが含まれるTXTファイルを指定します。各アドレスをそれぞれの行に指定する必要があります。

ウィザードが完了すると、選択したデバイスが管理グループに追加され、管理サーバーによって作成された名前でデバイスのリストに表示されます。

［**未割り当てデバイス**］フォルダーから管理グループフォルダーにデバイスをドラッグすることで、選択した管理グループにデバイスを移動できます。

クライアントデバイスの管理サーバーの変更

［*管理サーバーの変更*］タスクを使用して、クライアントデバイスを管理する管理サーバーを別のサーバーに変更できます。

クライアントデバイスを管理する管理サーバーを別のサーバーに変更するには：

1. デバイスを管理する管理サーバーに接続します。

2. 次のいずれかの方法で、管理サーバー変更タスクを作成します：

   - 選択した管理グループに含まれるデバイスの管理サーバーを変更する場合は、選択したグループに対するタスクを作成します。
   - いくつかの管理グループにまたがるデバイスまたは既存の管理グループに含まれていないデバイスの管理サーバーを変更するには、特定のデバイスに対するタスクを作成します。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。新規タスクウィザードの［**タスク種別の選択**］ウィンドウでは、［**Kaspersky Security Center**］ノードを選択し、［**詳細**］フォルダーを開いて*管理サーバーの変更*タスクを選択します。

3. 作成したタスクを実行します。

   タスクが完了すると、タスクの対象となったクライアントデバイスは、タスク設定で指定した管理サーバーの管理下に置かれます。

管理サーバーで暗号化とデータ保護をサポートしている場合、［*管理サーバーの変更*］タスクを作成しようとすると、警告が表示されます。その警告には、デバイスに暗号化されたデータが保存される場合、新しいサーバーがデバイスの管理を開始すると、ユーザーは以前に処理したことがある暗号化データにしかアクセスできなくなることが示されます。それ以外の暗号化されたデータにはアクセスできなくなります。暗号化されたデータにアクセスできなくなるケースの詳細な説明については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

管理サーバーに接続されたデバイスを接続ゲートウェイ経由で別の管理サーバーに移動する

管理サーバーに接続されているデバイスを、接続ゲートウェイを介して別の管理サーバーに移動できます。たとえば、別のバージョンの管理サーバーをインストールし、時間がかかる可能性があるためデバイスにネットワークエージェントを再インストールしたくない場合に、これが必要になることがあります。

手順に記載されているコマンドは、管理者権限を持つアカウントでクライアントデバイス上で実行する必要があります。

接続ゲートウェイを介して接続されたデバイスを別の管理サーバーに移動するには：

1. klmover ユーティリティを実行し、`-address<server address>` パラメータを使用して、新しい管理サーバーに切り替えます。
2. `klnagchk -nagwait -tl 4` コマンドを実行します。
3. 新しい接続ゲートウェイを設定するには、次のコマンドを実行します：

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "gateway_ip_or_name" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `"gateway_ip_or_name"` は、インターネットからアクセス可能な接続ゲートウェイのアドレスです。

- `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

  `1300` は、接続ゲートウェイがリッスンしている TCP ポートの番号です。

4. `klnagchk -restart -tl 4` コマンドを実行して、ネットワークエージェントサービスを開始します。

デバイスは新しい管理サーバーに移動され、新しく接続されたゲートウェイを介して接続されます。

クラスターとサーバーアレイ

Kaspersky Security Center はクラスターテクノロジーをサポートします。クライアントデバイスにインストールされたアプリケーションがサーバーアレイの一部であることを確認する情報が、ネットワークエージェントから管理サーバーに送信されると、このクライアントデバイスはクラスターノードになります。このクラスターは、［**管理対象デバイス**］フォルダーの独立したオブジェクトとしてコンソールツリーに追加され、サーバーアイコン（  ）で表示されます。

クラスターの一般的な特徴は次の通りです：

- クラスターとそのすべてのノードは常に同じ管理グループに属します。
- クラスターのノードを移動しようとすると、そのノードは元の位置に戻ります。
- クラスターを別のグループに移動すると、そのクラスターのすべてのノードが一緒に移動します。

クライアントデバイスのリモートでの起動、停止、再起動

Kaspersky Security Center では、クライアントデバイスをリモートで管理できます（起動、停止、再起動）。

クライアントデバイスをリモートで管理するには：

1. デバイスを管理する管理サーバーに接続します。
2. 次のいずれかの方法で、デバイス管理タスクを作成します：
   - 選択した管理グループに含まれるデバイスの管理サーバーの起動、停止、または再起動が必要な場合は、選択したグループに対するタスクを作成します。
   - いくつかの管理グループにまたがるデバイスまたはどのグループにも属していないデバイスを起動、停止、あるいは再起動するには、特定のデバイスに対するタスクを作成します。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。新規タスクウィザードの［**タスク種別の選択**］ウィンドウで、［**Kaspersky Security Center**］ノードを選択し、［**詳細**］フォルダーを開いて**デバイスの管理**タスクを選択します。
3. 作成したタスクを実行します。

タスクの完了後、選択したデバイスでコマンド（起動、停止、再起動）が実行されます。

管理対象デバイスと管理サーバーの継続した接続の使用について

既定では、Kaspersky Security Center は、管理対象デバイスと管理サーバーを継続して接続しません。管理対象デバイスのネットワークエージェントが、定期的に接続を確立し、管理サーバーと同期させます。これらの同期セッションの間隔はネットワークエージェントによって定義されており、既定では 15 分間隔になっています。同期が必要な場合（たとえば、アプリケーションのポリシーを強制的に適用するなど）、管理サーバーは署名されたネットワークパケットをネットワークエージェントの UDP ポート 15000 へ送付します（管理サーバーは、IPv4 または IPv6 ネットワークでこのパケットを送信できます）。管理サーバーと対象デバイス間の UDP 接続が何らかの理由で不可能である場合、ネットワークエージェントと管理サーバーの次回の接続時の同期間隔時間内に同期が実行されます。

一部の操作は、ネットワークエージェントと管理サーバー間を早期に接続せずに実行することはできません。この操作には、ローカルタスクの実行や停止、管理対象製品の統計の受信、トンネリングといった操作が含まれます。これらの操作を可能にするには、［**管理サーバーから切断しない**］を管理対象デバイスでオンにする必要があります。

強制同期について

Kaspersky Security Center では、管理対象デバイスのステータス、設定、タスク、ポリシーは自動的に同期されますが、場合によっては、現時点において指定されたデバイスで同期が実行されているかどうかを管理者が正確に知る必要があります。

管理コンソールにおける管理対象デバイスのコンテキストメニューでは、［**すべてのタスク**］メニューに［**強制同期**］コマンドが含まれます。Kaspersky Security Center 15.1 がこのコマンドを実行すると、管理サーバーはデバイスへの接続を試みます。この試行が成功すると、強制同期が実行されます。試行が失敗した場合は、ネットワークエージェントと管理サーバー間の次の定期接続まで待機してから同期が強制的に実行されます。

接続スケジュールの概要

ネットワークエージェントのプロパティウィンドウにある［**接続**］セクションの［**接続スケジュール**］サブセクションで、ネットワークエージェントが管理サーバーにデータを送信する時間間隔を指定できます。

要求時に接続：このオプションをオンにすると、ネットワークエージェントが管理サーバーへのデータ送信を要求された時に、接続が確立されます。

指定の時間帯に接続：このオプションをオンにすると、ネットワークエージェントは指定した時間に管理サーバーへ接続します。複数の接続時間帯を追加できます。

デバイスのユーザーへのメッセージの送信

メッセージをデバイスのユーザーに送るには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. 次の方法のいずれかを使用して、デバイスのユーザーにメッセージを送信するタスクを作成します：
   - 選択した管理グループに属するデバイスのユーザーにメッセージを送信するには、選択したグループに対するタスクを作成します。
   - いくつかの管理グループにまたがるデバイスのユーザーまたは管理グループに属していないデバイスのユーザーにメッセージを送信するには、特定のデバイスに対するタスクを作成します。

新規タスクウィザードが起動します。ウィザードの指示に従ってください。

3. 新規タスクウィザードの［タスク種別の選択］ウィンドウで、［**Kaspersky Security Center 管理サーバー**］ノードを選択し、［**詳細**］フォルダーを開いて**ユーザーにメッセージを送信**タスクを選択します。ユーザーにメッセージを送信するタスクは、Windows を実行しているデバイスでのみ使用できます。［**ユーザーアカウント**］フォルダーからユーザーのコンテキストメニューを使用してメッセージを送信することもできます。

4. 作成したタスクを実行します。

タスクの完了後、作成したメッセージが、選択したデバイスのユーザーに送信されます。ユーザーにメッセージを送信するタスクは、Windows を実行しているデバイスでのみ利用できます。［**ユーザーアカウント**］フォルダーからユーザーのコンテキストメニューを使用してメッセージを送信することもできます。

Kaspersky Security for Virtualization の管理

Kaspersky Security Center は、仮想マシンと管理サーバーの接続機能をサポートしています。仮想マシンは、Kaspersky Security for Virtualization によって保護されます。詳細については、該当する各製品のドキュメントを参照してください。

デバイスのステータスの切り替えの設定

デバイスに「*緊急*」または「*警告*」ステータスを割り当てる条件を変更できます。

デバイスのステータスの「緊急」への切り替えを有効にするには：

1. 次のいずれかの方法で、プロパティウィンドウを開きます：

   - ［**ポリシー**］フォルダーの管理サーバーポリシーのコンテキストメニューで［**プロパティ**］を選択します。
   - 管理グループのコンテキストメニューで［**プロパティ**］を選択します。

2. **プロパティ**ウィンドウが表示されたら、［**セクション**］ペインで［**デバイスのステータス**］を選択します。

3. 右側の［**ステータスを「緊急」にする条件**］セクションで、リスト内の各条件に隣接するチェックボックスをオンにします。

   親ポリシーでロック状態になっていない設定のみ変更できます。

4. 選択した条件に対して適切な値を設定します。
   一部の条件では値を指定できますが、値を指定できない条件もあります。

5. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*緊急*」ステータスが割り当てられます。

デバイスのステータスの「警告」への切り替えを有効にするには：

1. 次のいずれかの方法で、プロパティウィンドウを開きます：

- ［**ポリシー**］フォルダーの管理サーバーポリシーのコンテキストメニューで［**プロパティ**］を選択します。
- 管理グループのコンテキストメニューで［**プロパティ**］を選択します。

2. **プロパティ**ウィンドウが表示されたら、［**セクション**］ペインで［**デバイスのステータス**］を選択します。
3. 右側の［**ステータスを「警告」にする条件**］セクションで、リスト内の各条件に隣接するチェックボックスをオンにします。

   親ポリシーでロック状態になっていない設定のみ変更できます。

4. 選択した条件に対して適切な値を設定します。

   一部の条件では値を指定できますが、値を指定できない条件もあります。
5. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*警告*」ステータスが割り当てられます。

デバイスのタグ付けおよび割り当てられたタグの表示

Kaspersky Security Center では、デバイスにタグ付けできます。*タグ*は、デバイスのグループ化、説明、または検索に使用できるデバイスの ID です。デバイスに割り当てられたタグは、抽出の作成、デバイスの検索、および各管理グループへのデバイスの割り当てに使用できます。

デバイスには、手動または自動でタグ付けできます。デバイスのプロパティで手動でデバイスにタグ付けします。個々のデバイスにタグ付けする必要がある場合は、手動のタグ付けを使用できます。自動タグ付けは、指定したタグ付けルールに従い、管理サーバーによって実行されます。

管理サーバーのプロパティで、この管理サーバーによって管理されるデバイスの自動タグ付けを設定できます。デバイスには、指定されたルールが適合する場合に自動的にタグ付けされます。個々のルールは各タグに対応します。ルールは、デバイス、オペレーティングシステム、デバイスにインストールされたアプリケーションのネットワークプロパティ、およびその他のデバイスのプロパティに適用されます。たとえば、Windows が実行されているすべてのデバイスに *Win* タグを割り当てるルールを設定できます。その後、デバイスの抽出を作成する場合にこのタグを使用できます。これにより、Windows が実行されているすべてのデバイスを分類することができます。

また、特定のポリシープロファイルが特定のタグが付いたデバイスにのみ適用されるようにするため、管理対象デバイスでのポリシープロファイルの有効化条件としてタグを使用することもできます。たとえば、［*配達担当者*］としてタグ付けされたデバイスが［*ユーザー*］管理グループに表示され、［*配達担当者*］タグによる対応するポリシープロファイルの有効化がオンになっている場合、［*ユーザー*］グループを対象に作成されたポリシーはこのデバイスに適用されませんが、ポリシープロファイルのプロファイルが適用されます。ポリシープロファイルにより、このデバイスでは、そのポリシーによって実行をブロックされている一部のアプリケーションを起動することができます。

複数のタグ付けルールを作成できます。複数のタグ付けルールを作成しており、それらのルールのそれぞれの条件が同時に満たされる場合は、1つのデバイスに複数のタグを割り当てることができます。すべての割り当てられたタグのリストは、デバイスのプロパティで確認できます。それぞれのタグ付けルールは、有効または無効にすることができます。ルールは、有効な場合、管理サーバーの管理対象デバイスに適用されます。ルールは、現時点では使用しないものの将来的に必要になる可能性がある場合、削除する必要はありません。代わりに、［**ルールを有効にする**］をオフにすることができます。この場合、ルールは無効になっており、［**ルールを有効にする**］を再びオンにするまで実行されません。タグ付けルールのリストからルールを一時的に除外し、その後再び含める必要がある場合は、ルールを削除せずに無効にする必要があります。

自動でのデバイスのタグ付け

管理サーバーのプロパティウィンドウで、自動タグルールを作成、編集することができます。

デバイスを自動的にタグ付けするには：

1. コンソールツリーで、タグルールを指定する管理サーバーの名前のノードを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウで［**タグルール**］セクションを選択します。
4. ［**タグルール**］セクションで、［**追加**］をクリックします。
   ［**新規ルール**］ウィンドウが表示されます。
5. ［**新規ルール**］ウィンドウで、ルールのプロパティ全般を設定します：
   - ルール名を指定します。
     ルール名は 255 文字以下で、特殊文字（**"*<>?\:|**）を含めることはできません。
   - ［**ルールを有効にする**］を使用して、ルールを有効または無効にします。
     既定では、［**ルールを有効にする**］はオンになっています。
   - ［**タグ**］にタグ名を入力します。
     タグ名は 255 文字以下で、特殊文字（**"*<>?\:|**）を含めることはできません。
6. ［**条件**］セクションで、［**追加**］をクリックして新しい条件を追加するか、［**プロパティ**］をクリックして既存の条件を編集します。
   ［新規自動タグルール条件ウィザード］ウィンドウが表示されます。
7. ［**タグの割り当て条件**］ウィンドウで、タグ付けに作用する条件のチェックボックスをオンにします。複数の条件を選択できます。
8. 選択したタグ付け条件に応じて、対応する条件を設定するためのウィンドウがウィザードに表示されます。次の条件によりルールのトリガーを設定します：
   - **デバイスの使用状況または特定のネットワークとの関連付け** - デバイスのネットワークプロパティ（Windows ネットワーク上のデバイス名、デバイスがドメインまたは IP サブネットに含まれるかなど）

     Kaspersky Security Center で使用するデータベースに大文字と小文字を区別する照合が設定されている場合は、デバイスの DNS 名の指定時に大文字と小文字を区別してください。そうしないと、自動タグ付けルールが機能しません。

- **Active Directory の使用** - Active Directory 組織単位内のデバイスの存在および Active Directory グループ内のデバイスの所属。
- **特定のアプリケーション** - デバイス上のネットワークエージェントの存在、オペレーティングシステムの種別、バージョン、アーキテクチャ。
- **仮想マシン** - デバイスが仮想マシンの特定の種別に属しているかどうか
- **アプリケーションレジストリのアプリケーションがインストール済み** - デバイス上の異なる製造元によるアプリケーションの存在。

9. 条件を設定した後、その名前を入力し、ウィザードを閉じます。

   必要に応じて、1つのルールに対して複数の条件を設定できます。この場合、タグは少なくとも1つの条件を満たすデバイスに割り当てられます。追加した条件は、ルールのプロパティウィンドウに表示されます。

10. ［**新規ルール**］ウィンドウの［**OK**］をクリックして、管理サーバーのプロパティウィンドウの［**OK**］をクリックします。

新しく作成されたルールは、選択した管理サーバーによって管理されているデバイスに適用されます。デバイスの設定がルールの条件を満たす場合、そのデバイスにタグが割り当てられます。

デバイスに割り当てられているタグの表示および設定

デバイスに割り当てられたすべてのタグのリストを表示できます。また、デバイスのプロパティウィンドウに移動して自動タグルールを設定できます。

デバイスに割り当てられているタグを表示、および設定するには：

1. コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。
2. ［**管理対象デバイス**］フォルダーの作業領域で、割り当てられたタグを表示するデバイスを選択します。
3. モバイルデバイスのコンテキストメニューから、［**プロパティ**］を選択します。
4. デバイスのプロパティウィンドウで［**タグ**］セクションを選択します。

   選択されたデバイスに割り当てられているタグのリストが表示されます。また、それぞれのタグが割り当てられた方法（手動か、ルールによるものか）も表示されます。

5. 必要に応じて、次のいずれかの操作を実行します：
   - タグルールの設定に進む場合は、［**自動タグルールの設定**］をクリックします（Windows のみ）。
   - タグの名前を変更するには、タグを選択して［**名前の変更**］をクリックします。
   - タグを削除するには、タグを選択して［**削除**］をクリックします。
   - タグを手動で追加する場合は、［**タグ**］セクションの下部にあるフィールドにタグを入力して、［**追加**］をクリックします。
6. ［**タグ**］セクションに対して変更を行った場合、変更を有効にするには、［**適用**］をクリックします。
7. ［**OK**］をクリックします。

デバイスのプロパティでタグを削除または名前を変更した場合、この変更は管理サーバーのプロパティに設定されているタグルールには影響しません。変更は、プロパティの変更が行われたデバイスに対してのみ適用されます。

クライアントデバイスのリモート診断：Kaspersky Security Center リモート診断ユーティリティ

Kaspersky Security Center リモート診断ユーティリティ（「リモート診断ユーティリティ」とも表記）は、クライアントデバイスへの次の処理のリモート実行を目的として設計されています：

- トレースの有効化と無効化、トレースレベルの変更、トレースファイルのダウンロード
- システム情報とアプリケーション設定のダウンロード
- イベントログのダウンロード
- アプリケーションのダンプファイルの生成
- 診断の開始および診断レポートのダウンロード
- アプリケーションの起動および停止

クライアントデバイスからダウンロードしたイベントログと診断レポートを、管理者自身による問題のトラブルシューティングに活用できます。また、テクニカルサポートの担当者がより詳細な分析を行うために、トレースファイル、ダンプファイル、イベントログ、診断レポートをクライアントデバイスからダウンロードするように求められる場合もあります。

リモート診断ユーティリティは管理コンソールと併せて自動的にインストールされます。

リモート診断ユーティリティのクライアントデバイスへの接続

リモート診断ユーティリティをクライアントデバイスに接続するには：

1. コンソールツリーで任意の管理グループを選択します。
2. 作業領域の［**デバイス**］タブで、任意のデバイスのコンテキストメニューから、［**カスタムツール**］→［**リモート診断**］の順に選択します。

   リモート診断ユーティリティのメインウィンドウが開きます。
3. リモート診断ユーティリティのメインウィンドウの最初のフィールドでは、デバイスへの接続時に使用するツールを次から指定します：
   - **Microsoft Windows ネットワークを使用してアクセスする**：
   - **管理サーバーを使用してアクセスする**：
4. ユーティリティのメインウィンドウの最初のフィールドで［**Microsoft Windows ネットワークを使用してアクセスする**］を選択した場合は、次の操作を実行します：
   - ［**デバイス**］で、接続するデバイスのアドレスを指定します。

     デバイスのアドレスとして、IP アドレス、NetBIOS 名または DNS 名を使用できます。

既定値は、コンテキストメニューからユーティリティを実行したデバイスのアドレスです。

- デバイスに接続するアカウントを指定します：

  - **既に接続しているユーザーとして接続する**（既定では、この項目が選択されます）。現在のユーザーアカウントで接続します。

  - **ユーザー名とパスワードを使用して接続する**：指定されたユーザーアカウントで接続します。目的のアカウントの［**ユーザー名**］と［**パスワード**］を指定します。

  > デバイスのローカル管理者アカウントで接続した場合にのみ、デバイスに接続できます。

5. ユーティリティのメインウィンドウの最初のフィールドで［**管理サーバーを使用してアクセスする**］を選択した場合は、次の操作を実行します：

   - ［**管理サーバー**］で、デバイスに接続しようとする管理サーバーのアドレスを指定します。

     管理サーバーのアドレスとして、IP アドレス、NetBIOS 名または DNS 名を使用できます。

     既定値は、ユーティリティを実行した管理サーバーのアドレスです。

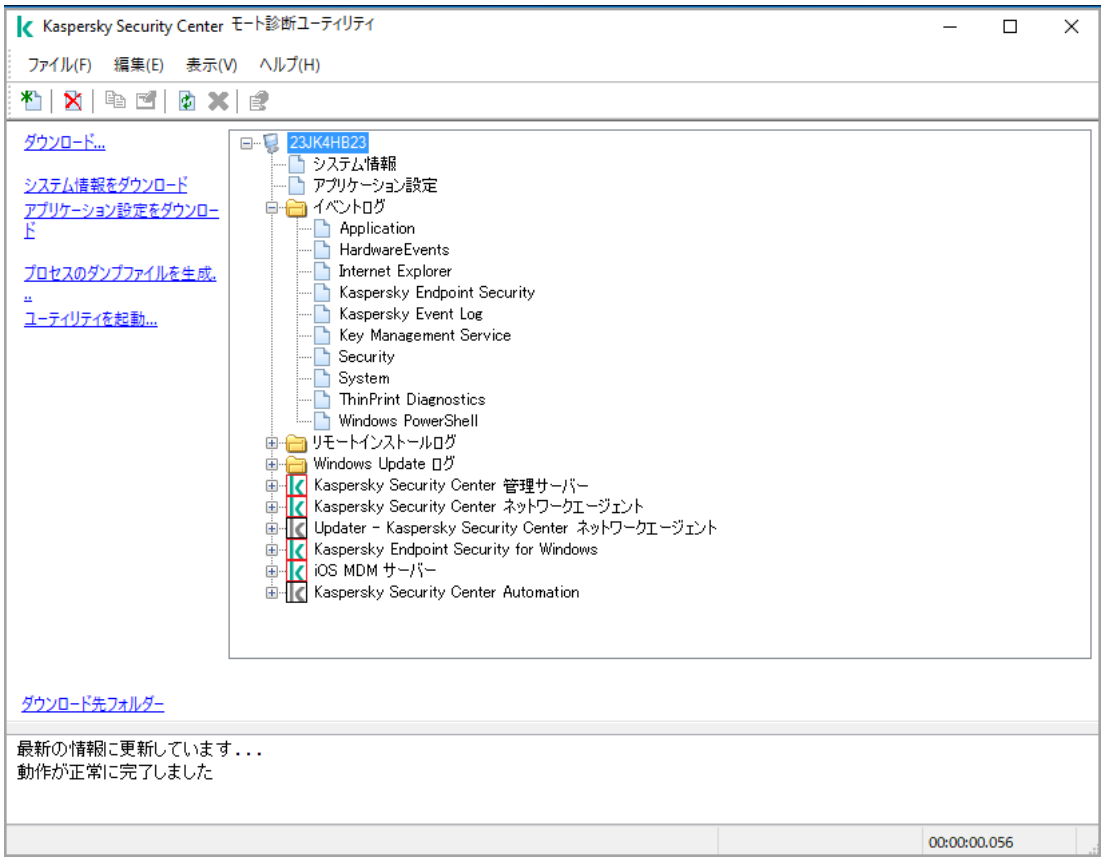
   - 必要に応じて、［**SSL を使用する**］、［**トラフィックを圧縮する**］、［**セカンダリ管理サーバーに属するデバイス**］をオンにします。

     ［**セカンダリ管理サーバーに属するデバイス**］をオンにした場合は、［**参照**］をクリックして、デバイスを管理するセカンダリ管理サーバーの名前を［**セカンダリ管理サーバーに属するデバイス**］に入力します。

6. デバイスに接続するには、［**サインイン**］をクリックします。

> 二段階認証を自分のアカウントで有効にする場合は、二段階認証を使用して認証する必要があります。

これにより、デバイスのリモート診断用ウィンドウが開きます（次の図を参照）。ウィンドウの左側には、デバイス診断処理へのリンクが表示されます。ウィンドウの右側には、デバイスのオブジェクトツリーが表示され、ユーティリティを操作できます。ウィンドウの下部には、ユーティリティ処理の進行状況が表示されます。



リモート診断ユーティリティ：リモートデバイス診断ウィンドウ

リモート診断ユーティリティはデバイスからダウンロードしたファイルを実行元のデバイスのデスクトップに保存します。

アプリケーションのダンプファイルの生成

アプリケーションダンプファイルを使用すると、ある時点でクライアントデバイスで実行されているアプリケーションのパラメータを表示できます。このファイルには、アプリケーション用にロードされたモジュールに関する情報も含まれています。

Linux ベースのデバイスからのダンプ取得はサポートされていません。

リモート診断を通じてダンプを取得するには、kldumper ユーティリティを使用します。このユーティリティは、テクニカルサポートの専門家の要求に応じて、カスペルスキー製品のプロセスのダンプを取得するように設計されています。kldumper ユーティリティの使用要件に関する詳細情報は、Kaspersky Security Center ナレッジベースに記載されています。

アプリケーションのダンプファイルを生成するには：

1. ［**管理対象デバイス**］フォルダーのワークスペースの［**デバイス**］タブで、必要なデバイスのコンテキストメニューを開き、［**カスタムツール**］→［**リモート診断**］を選択します。

   ［**Kaspersky Security Center リモート診断ユーティリティ**］ウィンドウが開きます。

2. リモート診断ユーティリティをクライアントデバイスに接続します。

   これにより、デバイスのリモート診断用ウィンドウが開きます。

3. ウィンドウの左側にある［**プロセスのダンプファイルを生成**］をクリックします。

4. ［**ダンプファイルを生成中**］ウィンドウが開くので、ダンプファイルを生成するアプリケーションの実行ファイルを指定します。

5. ［**OK**］をクリックします。

指定されたアプリケーションのダンプファイルを含むアーカイブがダウンロードされます。

指定されたアプリケーションがクライアントデバイス上で実行されていない場合、ダウンロードされたアーカイブに含まれる［結果］フォルダーは空になります。

指定されたアプリケーションが実行中であるにもかかわらず、ダウンロードがエラーで失敗したり、ダウンロードしたアーカイブに含まれる［結果］フォルダーが空の場合は、Kaspersky Security Center ナレッジベースを参照してください。

トレースの有効化と無効化、トレースファイルのダウンロード

リモートデバイスでのトレースを有効にするには：

1. リモート診断ユーティリティを実行して、目的のデバイスに接続します。

2. デバイスのオブジェクトツリーで、トレースを有効にするアプリケーションを選択します。

> デバイスが管理サーバーのツールを使用して接続している場合にだけ、セルフディフェンス機能があるアプリケーションのトレースを有効または無効にすることができます。

ネットワークエージェントのトレースの有効化は、アップデートのインストールと脆弱性の修正タスクの作成時に行うこともできます。この場合、リモート診断ユーティリティでネットワークエージェントのトレースが無効になっていても、ネットワークエージェントはトレース情報を書き込みます。

3. トレースを有効にするには：

   a. リモート診断ユーティリティウィンドウの左側で、［**トレースを有効化**］をクリックします。

   b. ［**トレースレベルの選択**］ウィンドウで表示される設定の既定値は変更しないことを推奨します。設定値の編集が必要な場合は、テクニカルサポート担当者が必要な変更をご案内します。次の設定を使用できます：

   - **トレースレベル**

     > トレースレベルでは、トレースファイルに含める情報の詳細度を指定できます。

   - **ローテーションありトレース**（Kaspersky Endpoint Security でのみ使用可能）

     > トレース情報を上書きし、トレースファイルのサイズが過剰に大きくなるの防止します。トレース情報を保存するために使用できるファイルの最大数と、各ファイルの最大サイズを指定します。トレースファイルの数が指定した最大数と同じになり、書き込み中のファイルのサイズが指定した最大サイズに達すると、新しいトレースファイルを作成できるように最も古いトレースファイルが削除されます。

   c. ［**OK**］をクリックします。

4. Kaspersky Endpoint Security では、テクニカルサポート担当者がシステムのパフォーマンス情報の Xperf トレースを有効にするようにお願いする場合があります。

   Xperf トレースを有効にするには：

   a. リモート診断ユーティリティウィンドウの左側で、［**Xperf トレースを有効化**］をクリックします。

   b. ［**トレースレベルの選択**］ウィンドウが開くので、テクニカルサポート担当者からの依頼内容に応じて、いずれかのトレースレベルを選択してください。

   - **低レベル**

     この種別のトレースファイルには、システムに関する最小限の量の情報が含まれています。
     既定では、このオプションがオンです。

   - **高レベル**

     この種別のトレースファイルには*低レベル*のトレースファイルより詳細な情報が含まれています。*低レベル*のトレースファイルではパフォーマンスを十分に評価できない場合などに、テクニカルサポートの担当者から提出を求められることがあります。*高レベル*のトレースファイルには、ハードウェア、オペレーティングシステム、プロセスとアプリケーションの開始と終了のリスト、パフォーマンスの評価に使用されたイベント、Windows システム評価ツールからのイベントなどに関する情報を含む技術情報が含まれます。

   c. 次のいずれかのトレース種別を選択します：

   - **基本**

     Kaspersky Endpoint Security の動作中にトレース情報が取得されます。
     既定では、このオプションがオンです。

   - **再起動時**

     管理対象デバイスでのオペレーティングシステムの起動時にトレース情報を受信します。このトレース種別は、デバイスが起動してから Kaspersky Endpoint Security が起動するまでの間にシステムパフォーマンスに影響を与える問題が発生している場合に使用すると効果的です。

   d. ［**ローテーションありトレース**］を有効にし、トレースファイルのサイズが過剰に大きくなるのを防止するように依頼される場合もあります。続いて、トレースファイルの最大サイズを設定します。ファイルが指定した最大サイズに達すると、最も古いトレース情報が削除され、新しい情報が上書きされます。

   e. ［**OK**］をクリックします。

   場合によっては、トレースを有効にするには、セキュリティ製品とタスクを再起動しなければならないことがあります。

リモート診断ユーティリティで、選択したアプリケーションのトレースが有効になります。

アプリケーションのトレースファイルをダウンロードするには：

1. 「リモート診断ユーティリティのクライアントデバイスへの接続」の説明に従って、リモート診断ユーティリティを実行し、目的のデバイスに接続します。

2. アプリケーションのフォルダーの［**トレースファイル**］フォルダーで、目的のファイルを選択します。

3. リモート診断ユーティリティウィンドウの左側で、［**ファイル全体をダウンロード**］をクリックします。

   ファイルのサイズが大きい場合、最も新しいトレースの部分をダウンロードできます。

   ハイライトされたトレースファイルを削除できます。ファイルを削除するには、トレースを無効にする必要があります。

選択したファイルが、ウィンドウ下部に表示されるパスにダウンロードされます。

リモートデバイスでのトレースを無効にするには：

1. 「リモート診断ユーティリティのクライアントデバイスへの接続」の説明に従って、リモート診断ユーティリティを実行し、目的のデバイスに接続します。

2. デバイスのオブジェクトツリーで、トレースを無効にするアプリケーションを選択します。

   デバイスが管理サーバーのツールを使用して接続している場合にだけ、セルフディフェンス機能があるアプリケーションのトレースを有効または無効にすることができます。

3. リモート診断ユーティリティウィンドウの左側で、［**トレースを無効化**］をクリックします。

リモート診断ユーティリティで、選択したアプリケーションのトレースが無効になります。

アプリケーション設定のダウンロード

リモートデバイスからアプリケーション設定をダウンロードするには：

1. 「リモート診断ユーティリティのクライアントデバイスへの接続」の説明に従って、リモート診断ユーティリティを実行し、目的のデバイスに接続します。

2. リモート診断ユーティリティウィンドウのオブジェクトツリーで、デバイス名のフォルダーを選択します。

3. リモート診断ユーティリティウィンドウの左側で、次のオプションから必要な処理を選択します：

   - **システム情報をダウンロード**
   - **アプリケーション設定をダウンロード**
   - **プロセスのダンプファイルを生成**

     このリンクをクリックして表示されるウィンドウでは、ダンプファイルを生成するアプリケーションの実行ファイルを指定します。

   - **ユーティリティを起動**

     このリンクをクリックして表示されるウィンドウでは、起動するユーティリティの実行ファイルと実行設定を指定します。

選択したユーティリティがダウンロードされて、デバイスで起動します。

イベントログのダウンロード

リモートデバイスからイベントログをダウンロードするには：

1. 「リモート診断ユーティリティのクライアントデバイスへの接続」の説明に従って、リモート診断ユーティリティを実行し、目的のデバイスに接続します。
2. デバイスオブジェクトツリーの［**システムイベントログ**］フォルダーで該当するログを選択します。
3. リモート診断ユーティリティウィンドウの左にある［**<イベントログ名> イベントログをダウンロード**］をクリックして、選択したログをダウンロードします。

選択したイベントログが、ペイン下部に表示されるパスにダウンロードされます。

複数個の診断情報項目のダウンロード

Kaspersky Security Center リモート診断ユーティリティを使用して、イベントログ、システム情報、トレースファイル、ダンプファイルなどを含む複数の診断情報項目をダウンロードできます。

リモートデバイスから診断情報をダウンロードするには：

1. 「リモート診断ユーティリティのクライアントデバイスへの接続」の説明に従って、リモート診断ユーティリティを実行し、目的のデバイスに接続します。
2. リモート診断ユーティリティウィンドウの左側で、［**ダウンロード**］をクリックします。
3. ダウンロードする項目の隣にあるチェックボックスをオンにします。
4. ［**開始**］をクリックします。

選択したすべての項目が、ペイン下部に表示されるパスにダウンロードされます。

診断の開始および結果のダウンロード

リモートデバイスでアプリケーションの診断を開始して、結果をダウンロードするには：

1. 「リモート診断ユーティリティのクライアントデバイスへの接続」の説明に従って、リモート診断ユーティリティを実行し、目的のデバイスに接続します。
2. デバイスのオブジェクトツリーで、目的のアプリケーションを選択します。
3. リモート診断ユーティリティウィンドウの左にある［**診断を実行**］をクリックして、診断を開始します。
   オブジェクトツリーで選択したアプリケーションのフォルダーに診断レポートが表示されます。
4. オブジェクトツリーで新しく生成された診断レポートを選択し、［**ダウンロード先フォルダー**］をクリックしてダウンロードします。

選択したレポートが、ペイン下部に表示されるパスにダウンロードされます。

アプリケーションの起動、停止、再起動

管理サーバーのツールを使用してデバイスに接続している場合にのみ、アプリケーションの起動、停止、再起動ができます。

アプリケーションを起動、停止、再起動するには：

1. 「リモート診断ユーティリティのクライアントデバイスへの接続」の説明に従って、リモート診断ユーティリティを実行し、目的のデバイスに接続します。
2. デバイスのオブジェクトツリーで、目的のアプリケーションを選択します。
3. リモート診断ユーティリティウィンドウの左側で処理を選択します：
   - **アプリケーションの停止**
   - **アプリケーションの再開**
   - **アプリケーションの開始**

   選択した処理に応じて、アプリケーションが起動、停止、再起動します。

UEFI 保護デバイス

*UEFI 保護デバイス*とは、BIOS レベルで統合された UEFI 用のカスペルスキーソリューションまたはアプリケーションを備えたデバイスです。統合された保護により、システムが起動した瞬間からデバイスのセキュリティを確保し、同時に、ソフトウェアが統合されていないデバイスでの保護が、セキュリティ製品の起動後にのみ機能し始めるようにします。Kaspersky Security Center はこれらのデバイスをサポートしています。

UEFI 保護デバイスの接続設定を編集するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウで、［**サーバー接続設定**］→［**追加のポート**］の順に選択します。
4. ［**追加のポート**］セクションで、関連する設定を変更します：
   - **UEFI 保護デバイスおよび KasperskyOS デバイス用のポートを開く**

     UEFI 保護デバイスを管理サーバーに接続できます。
   - **UEFI 保護デバイスおよび KasperskyOS デバイス用のポート**

     ［**UEFI 保護デバイスおよび KasperskyOS デバイス用のポートを開く**］がオンの場合、ポート番号を変更できます。既定のポート番号は 13294 です。

5. ［**OK**］をクリックします。

管理対象デバイスの設定

管理対象デバイスの設定を表示するには：

1. コンソールツリーで、［**管理対象デバイス**］フォルダーを選択します。
2. フォルダーの作業領域で、デバイスを選択します。
3. デバイスのコンテキストメニューで［**プロパティ**］を選択します。

選択したデバイスのプロパティウィンドウの［**全般**］セクションが表示されます。

全般

［**全般**］セクションには、クライアントデバイスに関する全般的な情報が表示されます。情報は、クライアントデバイスと管理サーバーとの前回の同期中に受信されたデータに基づいて提供されます：

- **名前**

  このフィールドでは、管理グループ内のクライアントデバイスの名前を表示したり変更したりできます。

- **説明**

  このフィールドでは、クライアントデバイスの補足的な説明を入力できます。

- **Windows ドメイン**

  このデバイスを含む Windows ドメインまたはワークグループ。

- **NetBIOS 名**

  クライアントデバイスの Windows ネットワークでの名前。

- **DNS 名**

  クライアントデバイスの DNS ドメイン名。

- **IP アドレス**

  デバイスの IP アドレス。

- **グループ**

クライアントデバイスが属する管理グループ。

- **前回のアップデート**

  定義データベースまたはアプリケーションをデバイス上で前回アップデートした日付。

- **前回の可視**

  デバイスが前回ネットワークで検出された日時。

- **管理サーバーへの接続**

  クライアントデバイスにインストールされたネットワークエージェントが管理サーバーに最後に接続した日時。

- **管理サーバーから切断しない**

  このオプションをオンにすると、管理対象デバイスと管理サーバー間の継続的な接続が維持されます。このオプションは、継続的な接続を提供するプッシュサーバーを使用していない場合に使用することがあります。

  このオプションがオフで、プッシュサーバーが使用されていない場合、管理対象デバイスは、データの同期または情報の送信のためにのみ管理サーバーに接続します。

  ［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

  このオプションは、管理対象デバイスでは既定でオフになっています。このオプションは、管理サーバーがインストールされているデバイスでは既定でオンになっており、オフにしようとしてもオンのままになります。

プロテクション

［**プロテクション**］セクションには、クライアントデバイスにおけるアンチウイルスによる保護に関する現在のステータスが表示されます：

- **デバイスのステータス**

  管理者によって定義された基準に基づいて、デバイス上のアンチウイルスによる保護のステータスとデバイスのネットワーク動作に対して割り当てられたクライアントデバイスのステータス。

- **すべての問題**

  この表には、クライアントデバイスにインストールされた管理対象アプリケーションで検知されたすべての問題のリストが表示されます。問題ごとに、アプリケーションがデバイスへの割り当てを推奨するステータスも表示されます。

- **リアルタイム保護**

クライアントデバイスのリアルタイム保護に関する現在のステータスが表示されます。

デバイスのステータスに変更があると、新しいステータスは、クライアントデバイスと管理サーバーが同期された後にのみデバイスのプロパティウィンドウに表示されます。

- **前回のオンデマンドスキャン**

  クライアントデバイスで前回のマルウェアスキャンが実行された日時。

- **検知した脅威の数**

  セキュリティ製品のインストール後（最初のスキャンの場合）またはウイルスカウンターを前回リセットした後に、クライアントデバイスで検知された脅威の合計数。

- **アクティブな脅威**

  クライアントデバイスにおける未処理ファイルの数。

  このフィールドは、モバイルデバイス上の未処理ファイルの数をスキップします。

- **ディスク暗号化ステータス**

  デバイスのローカルドライブでのファイル暗号化の現在のステータス。ステータスの説明は、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

アプリケーション

［**アプリケーション**］セクションには、クライアントデバイスにインストールされているすべてのカスペルスキー製品のリストが表示されます。このセクションには開始ボタン（▶）と停止ボタン（■）を使用すると、選択したカスペルスキー製品（ネットワークエージェントを除く）を起動および停止できます。管理対象デバイスで管理サーバーからの受信プッシュ通知用にポート 15000 UDP が使用可能な場合は、これらのボタンを使用できます。管理対象デバイスがプッシュ通知に使用できないが、管理サーバーへの継続的な接続モードが有効になっている場合（［**全般**］セクションの［**管理サーバーから切断しない**］がオンになっている場合）、［開始］と［停止］も使用できます。また、［**アプリケーション**］セクションには次のボタンが含まれています：

- **イベント**

  このボタンをクリックすると、アプリケーションの実行時にクライアントデバイスに起こったイベントのリストと、このアプリケーションのタスク結果が表示されます。

- **統計**

  このボタンをクリックすると、アプリケーションに関する現在の統計情報が表示されます。

- **プロパティ**

このボタンをクリックすると、アプリケーションに関する情報を受信し、アプリケーションを設定できます。

タスク

［**タスク**］タブでは、既存タスクのリストの表示、新規タスクの作成、タスクの削除、タスクの開始と停止、タスク設定の変更、実行結果の表示など、クライアントデバイスのタスクを管理できます。タスクのリストは、管理サーバーとの前回のクライアント同期セッション中に受信されたデータに基づいて提供されます。管理サーバーは、タスクステータスに関する情報をクライアントデバイスに要求します。

管理サーバーからのプッシュ通知を受信するために、管理対象デバイスでポート 15000 UDPが利用可能な場合、［開始］（  ）、［停止］（  ）、［削除］（  ）ボタンが有効になります。管理対象デバイスがプッシュ通知に使用できないが、管理サーバーへの継続的な接続モードが有効になっている場合（［**全般**］セクションの［**管理サーバーから切断しない**］がオンになっている場合）、［開始］、［停止］と［削除］も使用できます。

接続に失敗すると、ステータスは表示されず、ボタンは無効になります。

イベント

［**イベント**］タブでは、選択したクライアントデバイスについて管理サーバーに記録されたイベントが表示されます。

タグ

［**タグ**］タブでは、クライアントデバイスの検索に使用されるキーワードのリストを管理できます。また、既存のタグのリストの表示、リストからのタグの割り当て、自動タグ付けルールの設定、新規タグの追加、既存のタグの名称変更、タグの削除なども可能です。

システム情報

［**システム全般情報**］セクションには、クライアントデバイスにインストールされているアプリケーションに関する情報が表示されます。

アプリケーションレジストリ

［**アプリケーションレジストリ**］セクションでは、クライアントデバイス上にインストールされたアプリケーションのレジストリとそのアップデートを表示し、アプリケーションレジストリの表示を設定することができます。

インストール済みアプリケーションの情報は、クライアントデバイスにインストールされているネットワークエージェントから必要な情報が管理サーバーに送信されている場合に供給されます。管理サーバーへの情報の送信は、ネットワークエージェントまたはそのポリシーのプロパティウィンドウにある［**リポジトリ**］セクションで設定できます。

- **競合するセキュリティ製品のみ表示**

このオプションをオンにすると、カスペルスキー製品と互換性がないセキュリティ製品のみがアプリケーションのリストに表示されます。

既定では、このオプションはオフです。

- **アップデートの表示**

  このオプションをオンにすると、アプリケーションリストには、アプリケーションだけでなくアプリケーションにインストールされたアップデートパッケージも含まれます。

  アップデートのリストを表示するには、100 KB のトラフィックが必要になります。リストを閉じて再度開く場合は、再度 100 KB のトラフィックを使用する必要があります。

  既定では、このオプションはオフです。

- **ファイルへのエクスポート**

  このボタンをクリックすると、デバイスにインストールされているアプリケーションのリストを CSV ファイルまたは TXT ファイルにエクスポートできます。

- **履歴**

  このボタンをクリックすると、デバイスへのアプリケーションのインストールに関するイベントが表示されます。次の情報が表示されます：

  - アプリケーションがデバイスにインストールされた日時
  - アプリケーション名
  - アプリケーションのバージョン

- **プロパティ**

  このボタンをクリックすると、デバイスにインストールされているアプリケーションのリストで選択したデバイスのプロパティが表示されます。次の情報が表示されます：

  - アプリケーション名
  - アプリケーションのバージョン
  - アプリケーションの開発元

実行ファイル

［**実行ファイル**］セクションには、クライアントデバイスにある実行ファイルが表示されます。

ハードウェアレジストリ

［**ハードウェアレジストリ**］セクションでは、クライアントデバイスで使用されているハードウェアに関する情報を表示できます。Windows デバイスおよび Linux デバイスのこの情報を表示できます。

ハードウェアの詳細を取得する Linux デバイスに lshw ユーティリティがインストールされていることを確認してください。使用されているハイパーバイザーによっては、仮想マシンから取得されたハードウェアの詳細が不完全である場合があります。

セッション

［**セッション**］セクションは Windows デバイスに対してのみ表示され、クライアントデバイスの所有者および選択されたクライアントデバイスで作業を行ったユーザーのアカウントに関する情報が表示されます。

ドメインユーザー情報は、Active Directory データに基づいて生成されます。ローカルユーザーの詳細情報は、クライアントデバイスにインストールされている Windows セキュリティアカウントマネージャーから供給されます。

- **デバイスの所有者**

  ［**デバイスの所有者**］には、クライアントデバイスで特定の操作が必要になった際に管理者が連絡できるユーザーが表示されます。

  ［**割り当て**］および［**プロパティ**］を使用して、デバイスの所有者を選択したり、デバイスの所有者として指定されたユーザーの情報を表示したりすることができます。

  赤い×のマークが付いたボタンをクリックすると、現在のデバイスの所有者が削除されます。

リストには、クライアントデバイスを使用するユーザーのアカウントが表示されます。

- **名前**

  デバイスの Windows ネットワークでの名前。

- **参加者名**

  デバイス上のシステムにログオンしているユーザーの名前（ドメイン名またはローカル名）

- **アカウント**

  デバイスにログオンしているユーザーのアカウント

- **メール**

  ユーザーのメールアドレス

- **電話番号**

  ユーザーの電話番号

セキュリティ問題

［**セキュリティ問題**］タブでは、クライアントデバイスでのセキュリティ問題を表示、編集、作成できます。セキュリティ問題は、クライアントデバイスにインストールしたカスペルスキー製品によって自動で作成されるか、管理者が手動で作成します。たとえば、定期的にマルウェアを自分のリムーバブルドライブからデバイスに移しているユーザーがいた場合、管理者はこの件のセキュリティ問題を作成できます。管理者はセキュリティ問題のテキストに、概要説明と推奨される処分（ユーザーに下す懲戒処分など）を記載したり、ユーザーへのリンクを追加することもできます。

必要な処分がすべて行われたセキュリティ問題は、*処理済み*と呼ばれます。未処理のセキュリティ問題がある場合、デバイスのステータスを*緊急*または*警告*に変更する条件として選択できます。

このセクションには、デバイス用に作成したセキュリティ問題のリストがあります。セキュリティ問題は、重要度と種別で分類されます。セキュリティ問題のタイプは、セキュリティ問題を作成するカスペルスキー製品によって定義されます。［**処理済み**］列のチェックボックスをオンにすると、リストにある処理済みのセキュリティ問題を強調表示できます。

ソフトウェアの脆弱性

［**ソフトウェアの脆弱性**］セクションには、クライアントデバイスにインストールされているサードパーティのソフトウェアの脆弱性に関する情報が表示されます。リストの上にある検索フィールドを使用して、脆弱性を名前で検索することができます。

- **ファイルへのエクスポート**

  ［**ファイルへのエクスポート**］をクリックすると、脆弱性のリストがファイルに保存されます。既定では、脆弱性のリストは CSV ファイルにエクスポートされます。

- **修正可能な脆弱性のみ表示**

  このオプションを有効にすると、パッチを使用して修正できる脆弱性が表示されます。

  このオプションをオフにすると、パッチを使用して修正できる脆弱性と、パッチがリリースされていない脆弱性の両方が表示されます。

  既定では、このオプションはオンです。

- **プロパティ**

  リストからをふとウェアの脆弱性を選択し［**プロパティ**］をクリックすると、選択したソフトウェアの脆弱性が別ウィンドウで表示されます。ウィンドウで次の操作を実行できます：

  - 対象の管理対象デバイスではこのソフトウェア脆弱性を無視するようにする（管理コンソールまたは Kaspersky Security Center Web コンソールで操作）。
  - 脆弱性に対して推奨される修正のリストを表示する。
  - 脆弱性を修正するソフトウェアアップデートを手動で指定する（管理コンソールまたは Kaspersky Security Center Web コンソール）。
  - 脆弱性の該当数を表示する。
  - 脆弱性を修正するための既存のタスクのリストを表示したり、脆弱性を修正するためのタスクを新規作成する。

適用可能なアップデート

このセクションには、デバイスで検出されたがインストールされていないソフトウェアアップデートのリストが表示されます。

- **インストールされたアップデートの表示**

  このオプションをオンにすると、クライアントデバイスにインストールされたアップデートとインストールされていないアップデートの両方がリストに表示されます。

  既定では、このオプションはオフです。

アクティブポリシー

このセクションには、このデバイスに現在割り当てられているカスペルスキー製品のポリシーのリストが表示されます。

- **ファイルへのエクスポート**

  ［**ファイルへのエクスポート**］をクリックすると、アクティブなポリシーのリストがファイルに保存されます。既定では、ポリシーのリストは CSV ファイルにエクスポートされます。

アクティブなポリシーのプロファイル

- **アクティブなポリシーのプロファイル**

  クライアントデバイスでアクティブな既存のポリシーのプロファイルに関する情報がリスト表示されます。リストの上にある検索バーにポリシー名またはポリシープロファイル名を入力して、アクティブなポリシーのプロファイルを検索できます。

- **ファイルへのエクスポート**

  ［**ファイルへのエクスポート**］をクリックすると、アクティブなポリシーのプロファイルのリストがファイルに保存されます。既定では、ポリシーのプロファイルのリストは CSV ファイルにエクスポートされます。

ディストリビューションポイント

このセクションでは、デバイスがインタラクトするディストリビューションポイントのリストについて説明します。

- **ファイルへのエクスポート**

  ［**ファイルへのエクスポート**］をクリックすると、デバイスがインタラクトするディストリビューションポイントのリストがファイルに保存されます。既定では、デバイスのリストは CSV ファイルにエクスポートされます。

- **プロパティ**

［**プロパティ**］をクリックすると、デバイスがインタラクトするディストリビューションポイントが表示および設定されます。

ポリシーの全般的な設定

全般

［**全般**］セクションでは、ポリシーステータスの変更や、継承するポリシー設定の指定が可能です：

- ［**ポリシーのステータス**］セクションで、ポリシーのステータスを選択します：
  - **アクティブポリシー**

    このオプションをオンにすると、ポリシーがアクティブになります。

    既定では、このオプションがオンです。

  - **モバイルユーザーポリシー**

    このオプションをオンにすると、デバイスが企業ネットワークから離れるとポリシーがアクティブになります。

  - **非アクティブポリシー**

    このオプションをオンにすると、ポリシーは非アクティブになりますが［**ポリシー**］フォルダーに保持されます。必要に応じて、ポリシーをアクティブにすることができます。

- ［**設定の継承**］セクションでは、ポリシーの継承を設定できます。
  - **親ポリシーから設定を継承する**

    このオプションをオンにすると、ポリシーの設定値は上位レベルグループのポリシーから継承されるため、ロックされます。

    既定では、このオプションはオンです。

  - **設定を子ポリシーへ強制的に継承させる**

    このオプションをオンにすると、ポリシーの変更を適用した後に次の処理が実行されます：
    - 管理サブグループのポリシー（子ポリシー）に、ポリシーの設定値が継承されます。
    - 各子ポリシーのプロパティウィンドウの［**全般**］セクションにある［**設定の継承**］ブロックで、［**親ポリシーから設定を継承する**］が自動的にオンになります。

    このオプションをオンにすると、子ポリシーの設定はロックされます。

    既定では、このオプションはオフです。

イベントの設定

［**イベントの設定**］セクションでは、イベントの記録と通知を設定できます。イベントは、重要度に応じて次のタブに分類されます：

- **緊急**
  ［**緊急**］タブは、ネットワークエージェントのポリシーのプロパティに表示されません。
- **機能エラー**
- **警告**
- **情報**

それぞれのタブのリストには、イベントの種別と、管理サーバーでイベントが保存される既定の日数が表示されます。［**プロパティ**］をクリックすると、リストで選択したイベントについてのイベントログとイベント通知を設定できます。既定では、すべてのイベントで、管理サーバー全体を対象に指定された共通の通知設定が使用されます。しかしながら、目的のイベント種別の特定の設定を変更できます。

たとえば、［**警告**］タブで、イベント種別［**セキュリティ問題が発生しました**］を設定できます。このようなイベントは、たとえばディストリビューションポイントのディスク空き容量が 2 GB 未満の場合などに発生します（アプリケーションのインストール、アップデートのダウンロードをリモートで実行するには、少なくとも 4 GB が必要となります）。［**セキュリティ問題が発生しました**］イベントを設定するには、イベントを選択して［**プロパティ**］をクリックします。その後、発生したイベントの保存場所とその通知方法を指定できます。

ネットワークエージェントがセキュリティ問題を検知した場合は、管理対象デバイスの設定を使用してこの問題を管理できます。

複数のイベント種別を選択するには、**SHIFT** キーか **CTRL** キーを使用します。すべての種別を選択するには、［**すべて選択**］を使用します。

ネットワークエージェントのポリシー設定

ネットワークエージェントのポリシーを設定するには：

1. コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. フォルダーの作業領域で、ネットワークエージェントのポリシーを選択します。
3. ポリシーのコンテキストメニューで［**プロパティ**］を選択します。

   ネットワークエージェントポリシーのプロパティウィンドウが表示されます。

全般

［**全般**］セクションでは、ポリシーステータスの変更や、継承するポリシー設定の指定が可能です：

- ［**ポリシーのステータス**］セクションで、ポリシーのステータスを選択します：
  - **アクティブポリシー**

このオプションをオンにすると、ポリシーがアクティブになります。
既定では、このオプションがオン です。

- **モバイルユーザーポリシー**

  このオプションをオンにすると、デバイスが企業ネットワークから離れるとポリシーがアクティブになります。

- **非アクティブポリシー**

  このオプションをオンにすると、ポリシーは非アクティブになりますが［**ポリシー**］フォルダーに保持されます。必要に応じて、ポリシーをアクティブにすることができます。

- ［**設定の継承**］セクションでは、ポリシーの継承を設定できます。

  - **親ポリシーから設定を継承する**

    このオプションをオンにすると、ポリシーの設定値は上位レベルグループのポリシーから継承されるため、ロックされます。
    既定では、このオプションはオンです。

  - **設定を子ポリシーへ強制的に継承させる**

    このオプションをオンにすると、ポリシーの変更を適用した後に次の処理が実行されます：
    - 管理サブグループのポリシー（子ポリシー）に、ポリシーの設定値が継承されます。
    - 各子ポリシーのプロパティウィンドウの［**全般**］セクションにある［**設定の継承**］ブロックで、［**親ポリシーから設定を継承する**］が自動的にオンになります。

    このオプションをオンにすると、子ポリシーの設定はロックされます。
    既定では、このオプションはオフです。

イベントの設定

［**イベントの設定**］セクションでは、イベントの記録と通知を設定できます。イベントは、重要度に応じて次のタブに分類されます：

- **緊急**
  ［**緊急**］タブは、ネットワークエージェントのポリシーのプロパティに表示されません。
- **機能エラー**
- **警告**
- **情報**

それぞれのタブのリストには、イベントの種別と、管理サーバーでイベントが保存される既定の日数が表示されます。［**プロパティ**］をクリックすると、リストで選択したイベントについてのイベントログとイベント通知を設定できます。既定では、すべてのイベントで、管理サーバー全体を対象に指定された共通の通知設定が使用されます。しかしながら、目的のイベント種別の特定の設定を変更できます。

たとえば、［**警告**］タブで、イベント種別［**セキュリティ問題が発生しました**］を設定できます。このようなイベントは、たとえばディストリビューションポイントのディスク空き容量が 2 GB 未満の場合などに発生します（アプリケーションのインストール、アップデートのダウンロードをリモートで実行するには、少なくとも 4 GB が必要となります）。［**セキュリティ問題が発生しました**］イベントを設定するには、イベントを選択して［**プロパティ**］をクリックします。その後、発生したイベントの保存場所とその通知方法を指定できます。

ネットワークエージェントがセキュリティ問題を検知した場合は、管理対象デバイスの設定を使用してこの問題を管理できます。

複数のイベント種別を選択するには、**SHIFT** キーか **CTRL** キーを使用します。すべての種別を選択するには、［**すべて選択**］を使用します。

設定

［**設定**］セクションでは、ネットワークエージェントのポリシーを設定できます。

- **ディストリビューションポイント経由でのみファイルを配信する**

  このオプションをオンにすると、管理対象デバイスのネットワークエージェントはディストリビューションポイントからのみアップデートを取得します。

  このオプションをオフにすると、管理対象デバイス上のネットワークエージェント ディストリビューションポイントまたは管理サーバーからアップデートを取得します。

  > 管理対象デバイスのセキュリティ製品は、各セキュリティ製品のアップデートタスクで設定されたアップデート元からアップデートを取得することに注意してください。［**ディストリビューションポイント経由でのみファイルを配信する**］を有効にする場合、Kaspersky Security Center がアップデートタスクのアップデート元に設定されていることを確認してください。

  既定では、このオプションはオフです。

- **イベントキューの最大サイズ（MB）**

  このフィールドでは、イベントキューが使用できるドライブの最大サイズを指定できます。

  既定値は 2 メガバイト（MB）です。

- **アプリケーションがポリシーの拡張データをデバイスから取得可能である**

管理対象デバイスにインストールされたネットワークエージェントは、適用されたセキュリティ製品のポリシーに関する情報をセキュリティ製品（たとえば、Kaspersky Endpoint Security for Windows）に転送します。転送された情報は、セキュリティ製品のインターフェイスで表示できます。

ネットワークエージェントは次の情報を転送します：

- 管理対象デバイスへのポリシー導入の時間
- 管理対象デバイスへポリシー導入の時点でのアクティブポリシーまたはモバイルユーザーポリシーの名前
- 管理対象デバイスへポリシー導入の時点で管理対象デバイスが含まれていた管理グループの名前とフルパス
- アクティブポリシーのプロファイルのリスト

  情報を使用して、デバイスに正しいポリシーが適用されていることを確認し、トラブルシューティングを行うことができます。既定では、このオプションはオフです。

- **ネットワークエージェントを不正な削除・停止から保護し、設定の変更を防止する**

  このオプションをオンにすると、管理対象デバイスにネットワークエージェントのインストールされた後、必要な権限がない場合はコンポーネントの削除や再設定が行えなくなります。また、ネットワークエージェントサービスを停止できなくなります。このオプションはドメインコントローラーに影響しません。

  ローカル管理者権限で操作されているワークステーション上のネットワークエージェントを保護するには、このオプションをオンにします。

  既定では、このオプションはオフです。

- **アンインストール用パスワードを使用する**

  このオプションをオンにすると、［**変更**］をクリックして、klmover ユーティリティおよびネットワークエージェントのリモートアンインストール時に使用するパスワードを指定できます。

  既定では、このオプションはオフです。

リポジトリ

［**リポジトリ**］セクションでは、情報ネットワークエージェントから管理サーバーに詳細が送信されるオブジェクトの種別を選択できます。このセクションの設定の一部を変更することがネットワークエージェントのポリシーで禁止されている場合、それらの設定を変更することはできません。［**リポジトリ**］セクションの設定は、Windows を実行しているデバイスでのみ使用できます：

- **Windows Update 更新プログラムの詳細**

  このオプションをオンにすると、クライアントデバイスにインストールする必要のある Microsoft Windows 更新プログラムに関する情報が管理サーバーに送信されます。

  このオプションをオフにしても、［**適用なアップデート**］セクションのデバイスのプロパティに更新プログラムが表示されることがあります。たとえば、組織のデバイスにこれらの更新プログラムによって修正できる脆弱性がある場合などに、こうしたことが起こる可能性があります。

  既定では、このオプションはオンです。Windows でのみ使用できます。

- **ソフトウェアの脆弱性と対応するアップデートの詳細**

  このオプションをオンにすると、管理対象デバイスで検出されたサードパーティソフトウェア（Microsoft ソフトウェアを含む）の脆弱性に関する情報、およびサードパーティの脆弱性（Microsoft ソフトウェアを含まない）を修正するソフトウェアアップデートに関する情報が、管理サーバーに送信されます。

  このオプション（**ソフトウェアの脆弱性と対応するアップデートの詳細**）を選択すると、ネットワーク負荷、管理サーバーのディスク負荷、およびネットワークエージェントのリソース消費が増加します。

  既定では、このオプションはオンです。Windows でのみ使用できます。

  Microsoft ソフトウェアのソフトウェアアップデートを管理するには、［**Windows Update 更新プログラムの詳細**］を使用します。

- **ハードウェアレジストリの詳細**

  デバイスにインストールされたネットワークエージェントから、そのデバイスのハードウェアに関する情報が管理サーバーに送信されます。ハードウェアの詳細は、デバイスのプロパティで確認できます。

  ハードウェアの詳細を取得する Linux デバイスに lshw ユーティリティがインストールされていることを確認してください。使用されているハイパーバイザーによっては、仮想マシンから取得されたハードウェアの詳細が不完全である場合があります。

- **インストール済みアプリケーションの詳細**

  このオプションをオンにすると、クライアントデバイスにインストールされたアプリケーションに関する情報が管理サーバーに送信されます。

  既定では、このオプションはオンです。

- **パッチの情報を含める**

  クライアントデバイスにインストールされたアプリケーションのパッチに関する情報が管理サーバーに送信されます。このオプションをオンにすると、データベースに保存されるデータの容量が増えるとともに管理サーバーと DBMS での負荷が増大します。

  既定では、このオプションはオンです。Windows でのみ使用できます。

ソフトウェアのアップデートと脆弱性

この［**ソフトウェアのアップデートと脆弱性**］セクションでは、Windows アップデートの検索と配信を設定し、実行ファイルの脆弱性のスキャンを有効化できます。［**ソフトウェアのアップデートと脆弱性**］セクションの設定は、Windows を実行しているデバイスでのみ使用できます：

- **管理サーバーを WSUS サーバーとして使用する**

このオプションをオンにすると、Windows 更新プログラムが管理サーバーにダウンロードされます。管理サーバーは、ダウンロードしたアップデートを、ネットワークエージェントを利用してクライアントデバイスの Windows Update に一括配信します。

このオプションをオフにすると、Windows 更新プログラムのダウンロードに管理サーバーを使用しません。この場合、それぞれのクライアントデバイスが Windows アップデートを受信します。

既定では、このオプションはオフです。

- ［**Kaspersky Security Center 11 がインストールされた管理サーバーデバイスが WSUS サーバーとして使用されている場合に、バージョン 11 以降のネットワークエージェントがインストールされたデバイス上で、Windows Update 更新プログラムのインストールをユーザーが管理することを許可する**］の設定で、Windows Update を使用してデバイスに手動でインストールできる Windows 更新プログラムを制限できます。

  Windows 10 を実行しているデバイスで、デバイスに適用可能な更新プログラムが Windows Update 内で既に検出されている場合、［**Kaspersky Security Center 11 がインストールされた管理サーバーデバイスが WSUS サーバーとして使用されている場合に、バージョン 11 以降のネットワークエージェントがインストールされたデバイス上で、Windows Update 更新プログラムのインストールをユーザーが管理することを許可する**］は、検出された更新プログラムがインストールされた後に適用されます。

  ドロップダウンリストからオプションを選択します：

  - **Windows Update のすべての適用可能な更新プログラムのインストールをユーザーに許可する**

    ユーザーは、デバイスに適用可能な Microsoft Windows Update のすべての更新プログラムをインストールできます。

    アップデートのインストールをブロックしない場合は、このオプションを選択します。

    ユーザーが Microsoft Windows Update の更新プログラムを手動でインストールする時、更新プログラムを管理サーバーからではなく Microsoft サーバーからダウンロードする場合があります。これは、管理サーバーが対象の更新プログラムをまだダウンロードしていない場合に起こります。Microsoft サーバーから更新プログラムをダウンロードすると、トラフィック量が増加します。

  - **Windows Update の承認された更新プログラムのみのインストールをユーザーに許可する**

    ユーザーは、デバイスに適用可能で管理者に承認された Microsoft Windows Update のすべての更新プログラムをインストールできます。

    たとえば、最初にテスト環境にアップデートをインストールしてデバイスのオペレーティングシステムとの互換性の問題が生じないかを確認してから、クライアントデバイスへの承認されたアップデートのインストールを許可することができます。

    ユーザーが Microsoft Windows Update の更新プログラムを手動でインストールする時、更新プログラムを管理サーバーからではなく Microsoft サーバーからダウンロードする場合があります。これは、管理サーバーが対象の更新プログラムをまだダウンロードしていない場合に起こります。Microsoft サーバーから更新プログラムをダウンロードすると、トラフィック量が増加します。

  - **Windows Update 更新プログラムのインストールをユーザーに許可しない**

ユーザーは、デバイスに Microsoft Windows Update の更新プログラムを手動でインストールできません。すべての適用可能な更新プログラムは、管理者の設定に従ってインストールされます。

アップデートのインストールを一元的に管理する場合は、このオプションをオンにします。

たとえば、ネットワークの過負荷を避けるために、アップデートのスケジュールを最適化したい場合などです。ユーザーの業務に支障をきたさないように、業務時間外にアップデートをスケジュールすることができます。

- ［**Windows Update 検索モード**］で、更新プログラムの検索モードを選択できます：
  - **アクティブ**

    このオプションをオンにすると、管理サーバーがネットワークエージェントのサポートにより、クライアントデバイス上の Windows Update エージェントからアップデート元である Windows Update Server または WSUS への要求を開始します。次に、ネットワークエージェントが、Windows Update エージェントから受け取った情報を管理サーバーに渡します。

    このオプションは、*脆弱性とアプリケーションのアップデートの検索*タスクで［**アップデートサーバーに接続してアップデートを取得**］が選択されている場合にのみ有効になります。

    既定では、このオプションがオンです。

  - **パッシブ**

    このオプションをオンにすると、ネットワークエージェントは、Windows Update エージェントとアップデート元との前回の同期で取得した更新プログラムの情報を定期的に管理サーバーに渡します。Windows Update エージェントとアップデート元が同期されない場合、管理サーバー上のアップデートの情報が最新ではなくなります。

    アップデート元のメモリキャッシュからアップデートを取得する場合は、このオプションを選択します。

  - **無効**

    このオプションをオンにすると、管理サーバーは更新プログラムに関する情報を要求しません。

    このオプションは、たとえば手元のローカルデバイスで最初にアップデートをテストしたい場合などに選択します。

- **実行ファイルの開始時に脆弱性をスキャンする**

  このオプションをオンにすると、実行ファイルが実行時にスキャンされ、脆弱性がないかチェックされます。

  既定では、このオプションはオンです。

再起動の設定

［**再起動の設定**］セクションでは、アプリケーションの正しい使用、インストール、またはアンインストールのために管理対象デバイスのオペレーティングシステムの再起動が必要な場合に行う動作を指定できます。
［**再起動の設定**］セクションの設定は、Windows を実行しているデバイスでのみ使用できます：

- **OS を再起動しない**

オペレーティングシステムは再起動されません。

- **必要に応じて自動的に OS を再起動する**

  必要に応じて、オペレーティングシステムは自動的に再起動されます。

- **ユーザーに処理を確認する**

  オペレーティングシステムの再起動を許可するよう要求されます。
  既定では、このオプションがオンです。

  - **通知の繰り返し間隔（分）**

    このオプションをオンにすると、チェックボックスに隣接するフィールドに指定された頻度で、オペレーティングシステムの再起動を許可するよう要求されます。既定では、要求される頻度は 5 分です。
    このオプションをオフにすると、再起動の許可を繰り返し要求されることはありません。
    既定では、このオプションはオンです。

  - **次の時間経過後に強制的に再起動する（分）**

    このオプションをオンにすると、ユーザーへの通知後、チェックボックスに隣接するフィールドで指定した時間の経過後に、オペレーティングシステムが強制的に再起動します。
    このオプションをオフにすると、アプリケーションは強制的に再起動しません。
    既定では、このオプションはオンです。

  - **セッションがブロックされたアプリケーションを強制終了するまで待機する時間（分）**

    ユーザーのデバイスがロックされた場合にアプリケーションが強制終了されます（指定した非アクティブの時間が経過した後に自動で、または手動で）。
    このオプションを有効にすると、入力フィールドに指定した時間を過ぎた時に、ロックされたデバイスでアプリケーションが強制的に終了します。
    このオプションをオフにすると、ロックされたデバイスでアプリケーションは終了しません。
    既定では、このオプションはオフです。

Windows デスクトップ共有

［**Windows デスクトップ共有**］セクションでは、デスクトップアクセスの共有時にリモートデバイスで実行される管理者の処理の監査を有効にしたり、設定したりできます。［**Windows デスクトップ共有**］セクションの設定は、Windows を実行しているデバイスでのみ使用できます：

- **監査を有効にする**

このオプションをオンにすると、リモートデバイスにおける管理者の処理の監査が有効になります。リモートデバイスにおける管理者の処理の記録は次に保存されます：

- リモートデバイスのイベントログ
- リモートデバイス上のネットワークエージェントのインストールフォルダーにある、拡張子が syslog のファイル
- Kaspersky Security Center のイベントデータベース

管理者の処理の監査が使用可能である条件は次の通りです：

- 脆弱性とパッチ管理のライセンスが使用されている
- 管理者がリモートデバイスのデスクトップに対する共有アクセスを開始する権限を持っている

このオプションをオフにすると、リモートデバイスにおける管理者の処理の監査が無効になります。

既定では、このオプションはオフです。

- **読み取り時に監視する必要のあるファイルのマスク**

リストにはファイルマスクが含まれます。監査が有効になると、マスクと一致する管理者の読み取りファイルが監視され、ファイルの読み取りに関する情報が保存されます。リストは、［**監査を有効にする**］がオンの場合に使用できます。ファイルマスクを編集し、新しいマスクをリストに追加できます。新しいファイルマスクは、新しい行のリストに指定する必要があります。

既定では、*.txt、*.rtf、*.doc、*.xls、*.docx、*.xlsx、*.odt、*.pdf のファイルマスクが指定されます。

- **変更時に監視する必要のあるファイルのマスク**

リストには、リモートデバイス上のファイルのマスクが含まれます。監査が有効になると、マスクと一致するファイルで管理者によって行われた変更が監視され、その変更に関する情報が保存されます。リストは、［**監査を有効にする**］がオンの場合に使用できます。ファイルマスクを編集し、新しいマスクをリストに追加できます。新しいファイルマスクは、新しい行のリストに指定する必要があります。

既定では、*.txt、*.rtf、*.doc、*.xls、*.docx、*.xlsx、*.odt、*.pdf のファイルマスクが指定されます。

パッチとアップデートの管理

［**パッチとアップデートの管理**］セクションでは、アップデートのダウンロードを設定できます。また、管理対象デバイスへのパッチの配信とインストールについても設定できます：

- **コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**

このオプションをオンにすると、承認ステータスが「*未定義*」のカスペルスキー製品のパッチが、アップデートサーバーにダウンロードされるとすぐに、管理対象デバイスに自動インストールされます。

このオプションをオフにすると、ダウンロードされたパッチのうちステータスが「*未定義*」のものは、管理者がステータスを「*承認*」に変更しない限りインストールされません。

既定では、このオプションはオンです。

- **アップデートと定義データベースをあらかじめ管理サーバーからダウンロードする（推奨）**

このオプションをオンにすると、オフライン方式でのアップデートのダウンロードが使用されます。管理サーバーは、アップデートの受信時に、管理対象アプリケーションに必要なアップデートを、該当するアプリケーションがインストールされたデバイス上のネットワークエージェントに通知します。ネットワークエージェントは、アップデートに関する情報を受け取ると、適切なファイルを管理サーバーからあらかじめダウンロードします。具体的には、管理サーバーは、ネットワークエージェントが次に接続された時にアップデートのダウンロードを開始します。ネットワークエージェントによってすべてのアップデートがクライアントデバイスにダウンロードされると、そのデバイスのアプリケーションでこれらのアップデートが利用可能になります。

クライアントデバイス上の管理対象アプリケーションがアップデートのためにネットワークエージェントにアクセスしようとすると、ネットワークエージェントは必要なアップデートがあるかどうか確認します。管理対象アプリケーションから要求された時点で、管理サーバーからアップデートを受信してから経過した時間が 25 時間以内の場合、ネットワークエージェントは管理サーバーと接続せずに、ローカルキャッシュからアップデートを管理対象アプリケーションに渡します。ネットワークエージェントからクライアントデバイス上のアプリケーションへアップデートを配信する際には、アップデートのために管理サーバーへの接続を確立する必要はありません。

このオプションをオフにすると、オフライン方式でのアップデートのダウンロードは使用されません。アップデートは、アップデートダウンロードタスクのスケジュールに従って配信されます。

既定では、このオプションはオンです。

接続

［**接続**］セクションには 3 つのサブセクションが含まれます：

- **ネットワーク**
- **接続プロファイル**（Windows のみ）
- **接続スケジュール**

［**ネットワーク**］サブセクションでは、管理サーバーからクライアントコンピューターへの接続を設定したり、UDP ポートの使用を有効化したり、ポート番号を定義したりできます。次のオプションを使用できます：

- ［**管理サーバーへの接続**］セクションでは、管理サーバーへの接続を設定し、クライアントデバイスと管理サーバーを同期する間隔を指定できます：

  - **ネットワークトラフィックを圧縮する**

    このオプションをオンにすると、送信される情報量が減ることでネットワークエージェントによるデータ送信速度が向上し、これにより管理サーバーの負荷が軽減されます。

    クライアントコンピューターの CPU の負荷は増加する可能性があります。

    既定では、このチェックボックスはオンです。

  - **Microsoft Windows ファイアウォールでネットワークエージェントのポートを開く**

    このオプションをオンにすると、ネットワークエージェントの動作に必要なポートが Microsoft Windows ファイアウォールの除外リストに追加されます。

    既定では、このオプションはオンです。

- **SSL を使用する**

  このオプションをオンにすると、SSL を使用してセキュアなポート経由で管理サーバーへの接続が確立されます。

  既定では、このオプションはオンです。

- **既定の接続設定でディストリビューションポイントの接続ゲートウェイを使用する（使用可能な場合）**

  このオプションをオンにすると、ディストリビューションポイントの接続ゲートウェイが、管理グループのプロパティで指定された設定で使用されます。

  既定では、このオプションはオンです。

- **UDP ポートを使用する**

  ネットワークエージェントが UDP ポートを経由して管理サーバーを接続する場合は、［**UDP ポートを使用**］をオンにして、［**UDP ポート番号**］を指定します。既定では、このオプションはオンです。管理サーバーに接続するための既定の UDP ポートは 15000 です。

- **UDP ポート番号**

  このフィールドに、UDP ポート番号を入力できます。既定のポート番号は 15000 です。

  レコードには 10 進法が使用されます。

  Windows XP Service Pack 2 で稼働するクライアントデバイスでは、UDP ポート 15000 が OS のファイアウォールによりブロックされます。このポートを手動で開く必要があります。

- **ディストリビューションポイントを使用して管理サーバーへ強制的に接続する**

  ［**ディストリビューションポイントをプッシュサーバーとして使用する**］をディストリビューションポイントの設定ウィンドウでオンにする場合、このオプションをオンにします。オンにしないと、ディストリビューションポイントはプッシュサーバーとして動作しません。

［**接続プロファイル**］サブセクションでは、ネットワークロケーションを設定したり、管理サーバーの接続プロファイルを設定したりできます。また、管理サーバーが使用できない場合にモバイルユーザーモードを有効化することもできます。［**接続プロファイル**］セクションの設定は、Windows または macOS を実行しているデバイスでのみ使用できます：

- **ネットワークロケーションの設定**

  ネットワークロケーションの設定では、クライアントデバイスが接続するネットワークの特性を定義し、ネットワークの特性が変更された時にネットワークエージェントが管理サーバーの接続プロファイルを切り替えるためのルールを指定します。

- **管理サーバー接続プロファイル**

このセクションでは、ネットワークエージェントから管理サーバーへの接続のプロファイルを表示して追加することができます。次のイベントの発生時、ネットワークエージェントから別の管理サーバーに切り替えるルールを作成することもできます：

- クライアントデバイスが別のローカルネットワークに接続した場合
- デバイスから組織のローカルネットワークへの接続が切断した場合
- 接続ゲートウェイアドレスまたは DNS サーバーアドレスが変更された場合

接続プロファイルは、Windows および macOS を実行しているデバイスでのみサポートされます。

- **管理サーバーが使用できない時にモバイルユーザーモードを有効にする**

このオプションを有効にすると、このプロファイルで接続しているクライアントデバイスにインストールされているアプリケーションは、モバイルユーザーモードおよびモバイルユーザーポリシーを使用します。モバイルユーザーポリシーがアプリケーションに対して定義されていない場合は、アクティブポリシーが使用されます。

このオプションを無効にすると、アプリケーションはアクティブポリシーを使用します。

既定では、このオプションはオフです。

［**接続スケジュール**］サブセクションでは、ネットワークエージェントから管理サーバーにデータを送信する時間間隔を指定できます。

- **要求時に接続**

このオプションをオンにすると、ネットワークエージェントが管理サーバーへのデータ送信を要求された時に、接続が確立されます。

既定では、このオプションがオンです。

- **指定の時間帯に接続**

このオプションをオンにすると、ネットワークエージェントは指定した時間に管理サーバーへ接続します。複数の接続時間帯を追加できます。

ディストリビューションポイント

［**ディストリビューションポイント**］セクションには 4 つのサブセクションが含まれます。

- **ネットワークポーリング**
- **インターネット接続設定**
- **KSN プロキシ**
- **アップデート**

［**ネットワークポーリング**］サブセクションでは、ネットワークの自動ポーリングを設定できます。ネットワークポーリング、IP アドレス範囲のポーリング、ActiveDirectory ポーリングの 3 種類のポーリングを有効にできます。

- **ネットワークポーリングを有効にする**

  このオプションをオンにすると、［**簡易ポーリングのスケジュールを設定する**］と［**完全ポーリングのスケジュールを設定する**］をクリックして設定したスケジュールに従って、管理サーバーによってネットワークが自動的にポーリングされます。

  このオプションをオフにすると、管理サーバーは［**ネットワークポーリングの間隔（分）**］フィールドで指定された間隔でネットワークをポーリングします。

  ネットワークエージェントのバージョンが 10.2 より前の場合、デバイスの検索間隔は、［**Windows ドメインをポーリングする間隔（分）**］（簡易の Windows ネットワークポーリング）と［**ネットワークポーリングの間隔（分）**］（簡易の Windows ネットワークポーリング）で設定できます。

  既定では、このオプションはオフです。

- **IP アドレス範囲のポーリングを有効にする**

  このオプションをオンにすると、［**ポーリングのスケジュールを設定する**］をクリックして設定したスケジュールに従って、ディストリビューションポイントによって IP アドレス範囲が自動的にポーリングされます。

  このオプションをオフにすると、ディストリビューションポイントは IP アドレス範囲をポーリングしません。

  ネットワークエージェントのバージョンが 10.2 より前の場合、IP アドレス範囲のポーリング頻度は、［**ポーリング間隔（分）**］で設定できます。このフィールドは、オプションをオンにすると使用可能になります。

  既定では、このオプションはオフです。

- **Zeroconf ポーリングを使用する（Linux プラットフォームのみ。手動で指定した IP 範囲は無視されます）**

  このオプションをオンにすると、ディストリビューションポイントは自動的にゼロコンフィギュレーションネットワーキング（「*Zeroconf*」とも表記）を使用して IPv6 ネットワークを検索します。この場合、ディストリビューションポイントはネットワーク全体を検索するため、有効な IP 範囲の検索は無視されます。

  Zeroconf の使用を開始するには、次の条件が満たされている必要があります：

  - ディストリビューションポイントが Linux を実行している必要があります。
  - ディストリビューションポイントで avahi-browse ユーティリティをインストールする必要があります。

  このオプションをオフにすると、ディストリビューションポイントは IPv6 デバイスを持つネットワークを検索しません。

  既定では、このオプションはオフです。

- **Active Directory のポーリングを有効にする**

このオプションをオンにすると、［**ポーリングのスケジュールを設定する**］をクリックして設定したスケジュールに従って、ディストリビューションポイントによって Active Directory が自動的にポーリングされます。

このオプションをオフにすると、管理サーバーは Active Directory をポーリングしません。

ネットワークエージェントのバージョンが 10.2 より前の場合、Active Directory のポーリング頻度は、［**ポーリング間隔（分）**］で設定できます。このフィールドは、このオプションをオンにすると使用可能になります。

既定では、このオプションはオフです。

［**インターネット接続設定**］サブセクションでは、インターネットアクセスを設定できます。

- **プロキシサーバーを使用する**

  このチェックボックスをオンにすると、入力フィールドでプロキシサーバー接続を設定できます。

  既定では、このチェックボックスはオフです。

- **プロキシサーバーアドレス**

  プロキシサーバーのアドレス。

- **ポート番号**

  接続に使用されるポート番号。

- **ローカルアドレスにプロキシサーバーを使用しない**

  このオプションをオンにすると、ローカルネットワークのデバイスへの接続にプロキシサーバーが使用されません。

  既定では、このオプションはオフです。

- **プロキシサーバー認証**

  このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。

  既定では、このチェックボックスはオフです。

- **ユーザー名**

  プロキシサーバーへの接続の確立に使用されるユーザーアカウント。

- **パスワード**

  タスクが実行されるアカウントのパスワード。

［**KSN プロキシ**］サブセクションでは、ディストリビューションポイントを使用して管理対象デバイスからの KSN リクエストを転送するようにアプリケーションを設定できます。

- **ディストリビューションポイントで KSN プロキシを有効にする**

  ディストリビューションポイントとして使用しているデバイス上で KSN プロキシサービスが実行されます。この機能を使用することで、ネットワーク上でトラフィックを分配しなおし、最適化できます。

  ディストリビューションポイントは、Kaspersky Security Network に関する声明に記載されている KSN の統計情報をカスペルスキーに送信します。既定では、KSN 声明は「%ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula」にあります。

  既定では、このオプションはオフです。管理サーバーのプロパティウィンドウで、［**管理サーバーをプロキシサーバーとして使用する**］と［**Kaspersky Security Network への参加に同意する**］がオンになっている場合にのみ使用できます。

  アクティブ / パッシブモードのクラスターのノードをディストリビューションポイントに割り当て、ノード上で KSN プロキシサーバーを有効にできます。

- **KSN リクエストを管理サーバーに転送する**

  ディストリビューションポイントは管理対象デバイスからの KSN リクエストを管理サーバーに転送します。

  既定では、このオプションはオンです。

- **インターネット経由で直接 KSN クラウド / KPSN にアクセスする**

  ディストリビューションポイントは管理対象デバイスからの KSN リクエストを KSN クラウドまたは KPSN に転送します。ディストリビューションポイント自体で生成された KSN リクエストも、KSN クラウドまたは KPSN に直接送信されます。

  バージョン 11 以前のネットワークエージェントをインストールしているディストリビューションポイントでは、KPSN に直接アクセスできません。これらのディストリビューションポイントで KPSN リクエストを KPSN に送信するように設定を編集するには、各ディストリビューションポイントで［**KSN リクエストを管理サーバーに転送する**］をオンにします。

  バージョン 12 以降のネットワークエージェントをインストールしているディストリビューションポイントでは、KPSN に直接アクセスできません。

- **TCP ポート**

  管理対象デバイスが KSN プロキシサーバーへの接続に使用する TCP ポートの番号。既定のポート番号は 13111 です。

- **UDP ポートを使用する**

  ネットワークエージェントが UDP ポートを経由して管理サーバーを接続する場合は、［**UDP ポートを使用**］をオンにして、［**UDP ポート番号**］を指定します。既定では、このオプションはオンです。管理サーバーに接続するための既定の UDP ポートは 15000 です。

［**アップデート**］サブセクションで、［**差分ファイルのダウンロード**］を有効または無効に設定することで、ネットワークエージェントが差分ファイルをダウンロードするかどうかを指定できます（既定では、このオプションはオンです）。

変更履歴

［**変更履歴**］タブでは、［ネットワークエージェントのポリシーのリビジョンの履歴］を確認できます。リビジョンの比較やリビジョンの表示に加えて、リビジョンのロールバック、リビジョンのファイル保存、リビジョンのロールバック、リビジョンの説明の追加と編集などの高度な操作も実行可能です。

ネットワークエージェントのオペレーティングシステムによる機能の比較

次の表は、特定のオペレーティングシステムでネットワークエージェントの設定に使用できるネットワークエージェントのポリシー設定を示しています。

ネットワークエージェントのポリシー設定：オペレーティングシステムによる比較

［ポリシー］セクション	Windows	Mac	Linux
全般	✓	✓	✓
イベントの設定	✓	✓	✓
設定	✓	✓	✓ 次のオプションを使用できます： • **ディストリビューションポイント経由でのみファイルを配信する** • **イベントキューの最大サイズ（MB）** • **アプリケーションがポリシーの拡張データをデバイスから取得可能である**
リポジトリ	✓	—	✓ 次のオプションを使用できます： • **インストール済みアプリケーションの詳細** • **ハードウェアレジストリの詳細**
ソフトウェアのアップデートと脆弱性	✓	—	—
再起動の設定	✓	—	—
Windows デスクトップ共有	✓	—	—
パッチとアップデートの管理	✓	—	—
［**接続**］→［**ネットワーク**］	✓	✓	✓ ［**Microsoft Windows ファイアウォールでネットワークエージェントのポートを開く**］以外。
［**接続**］→［**接続プロファイル**］	✓	✓	—
［**接続**］→［**接続スケジュール**］	✓	✓	✓
［**ディストリビューションポイント**］→［**ネットワークポーリング**］	✓	—	✓ 次のオプションを使用できます： • **Zeroconf** • **IP アドレス範囲**
［**ディストリビューションポイント**］→［**インターネット接続設定**］	✓	✓	✓
［**ディストリビューションポイント**］→［**KSN プロキシ**］	✓	—	✓
［**ディストリビューションポイント**］→［**アップデート**］	✓	—	✓
変更履歴	✓	✓	✓

ユーザーアカウントの管理

このセクションでは、製品がサポートするユーザーアカウントとロールについて説明します。また、Kaspersky Security Center のユーザー向けにアカウントとロールを作成する方法を説明します。

Kaspersky Security Center では、ユーザーアカウントとアカウントグループを管理できます。次の 2 種類のアカウントをサポートしています。

- 組織の従業員のアカウント。管理サーバーは、組織のネットワークをポーリングする時に、ユーザーのアカウントのデータを取得します。
- 内部ユーザーのアカウント：このアカウントは、仮想管理サーバーの使用時に用いられます。内部ユーザーのアカウントは、Kaspersky Security Center 内でのみ作成および使用されます。

ユーザーアカウントの使用

Kaspersky Security Center では、ユーザーアカウントとアカウントグループを管理できます。次の 2 種類のアカウントをサポートしています。

- 組織の従業員のアカウント。管理サーバーは、組織のネットワークをポーリングする時に、ユーザーのアカウントのデータを取得します。
- 内部ユーザーのアカウント：このアカウントは、仮想管理サーバーの使用時に用いられます。内部ユーザーのアカウントは、Kaspersky Security Center 内でのみ作成および使用されます。

次のいずれかの方法でユーザーアカウントのリストを表示できます。

- コンソールツリーで、［**詳細**］→［**ユーザーアカウント**］に移動します。
- コンソールツリーで［**管理対象デバイス**］→［**デバイス**］タブ→<デバイス名>リンク→［**セッション**］セクションに移動します。

  ［**セッション**］セクションには、Windows を実行しているデバイス上でアクティブなセッションを持つユーザーアカウントが表示されます。

次の要件が満たされている場合、ユーザーアカウントリストが正しく表示されます。

- 管理サーバーと同じバージョン以降のネットワークエージェントを使用します。
- ドメインユーザーのアカウントを表示するために、Active Directory ポーリングが有効になっています。
- Windows を実行している管理対象デバイスでは、［**サーバー（LanmanServer）**］サービスが実行されています。

ユーザーアカウントおよびアカウントのグループで次の操作を実行できます：

- ロールを使用して、アプリケーションにアクセスするユーザー権限を設定します。
- メールおよび SMS を使用してユーザーにメッセージを送信します。
- ユーザーのモバイルデバイスのリストを表示します。

- ユーザーのモバイルデバイスの証明書を発行し、インストールします。
- ユーザーに発行された証明書のリストを表示します。
- ユーザーアカウントの二段階認証を無効にします。

内部ユーザーのアカウントの追加

Kaspersky Security Center に新しい内部ユーザーアカウントを追加するには：

1. コンソールツリーで、［**ユーザーアカウント**］フォルダーを開きます。
   既定では、［**ユーザーアカウント**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。
2. 作業領域で、［**ユーザーを追加**］をクリックします。
3. ［**新規ユーザー**］ウィンドウで、新しいユーザーアカウントの設定を指定します：
   - ユーザー名（  ）

     > ユーザー名は十分に検討してから入力してください。保存した後に変更することはできません。

   - **説明**
   - **名前**
   - **メールアドレス**
   - **電話番号**
   - **パスワード**：Kaspersky Security Center へのユーザーの接続用
     パスワードは次のルールに従う必要があります：
     - パスワードは、8 文字以上 256 文字以下にしてください。
     - パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
       - アルファベット大文字（A-Z）
       - アルファベット小文字（a-z）
       - 数字（0 - 9）
       - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）
     - パスワードに空白文字や Unicode 文字を含めることはできません。また「.」の後に続けて「@」を入力することは避けてください。

     入力したパスワードを表示するには、［**入力した文字を表示する**］をクリックしたままにします。

パスワードの入力試行回数には制限があります。既定では、許可されるパスワードの入力試行回数の上限は 10 回です。「許可されるパスワード入力試行回数の変更」の説明に従って、許可されるパスワードの入力試行回数を変更できます。

ユーザーが無効なパスワードを指定された回数以上入力すると、ユーザーアカウントは 1 時間ブロックされます。ユーザーアカウントのリストで、ブロックされたアカウントのユーザーアイコン（  ）が選択不可になります。パスワードを変更することでのみ、ユーザーアカウントのロックを解除できます。

- 必要に応じて［**アカウントの無効化**］をオンにすると、ユーザーは本製品に接続できなくなります。たとえば、アカウントの作成のみ先に行って有効化は後で行いたい場合などに、アカウントの無効化を活用できます。
- 不正な変更からユーザーアカウントを保護するために追加のオプションを有効にする場合は、［**アカウント設定の変更時にパスワードを要求する**］をオンにします。このオプションを有効にすると、ユーザーアカウントの設定の変更には、［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限を持つユーザーの認証が必要になります。

4. ［OK］をクリックします。

新しく作成されたユーザーアカウントが、［**ユーザーアカウント**］フォルダーの作業領域に表示されます。

内部ユーザーのアカウントの編集

Kaspersky Security Center で内部ユーザーアカウントを編集するには：

1. コンソールツリーで、［**ユーザーアカウント**］フォルダーを開きます。
   既定では、［**ユーザーアカウント**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。
2. 作業領域で、編集する内部ユーザーアカウントをダブルクリックします。
3. ユーザーのプロパティウィンドウが表示されるので、ユーザーアカウントの設定を変更します。
   - **説明**
   - **名前**
   - **メールアドレス**
   - **電話番号**
   - **パスワード**：Kaspersky Security Center へのユーザーの接続用
     パスワードは次のルールに従う必要があります：
     - パスワードは、8 文字以上 256 文字以下にしてください。
     - パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
       - アルファベット大文字（A-Z）
       - アルファベット小文字（a-z）

- 数字（0 - 9）
- 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）

- パスワードに空白文字や Unicode 文字を含めることはできません。また「.」の後に続けて「@」を入力することは避けてください。

入力したパスワードを表示するには、［**入力した文字を表示する**］をクリックしたままにします。

パスワードの入力試行回数には制限があります。既定では、許可されるパスワードの入力試行回数の上限は 10 回です。「許可されるパスワード入力試行回数の変更」の説明に従って、許可されるパスワードの入力試行回数を変更できます。

ユーザーが無効なパスワードを指定された回数以上入力すると、ユーザーアカウントは 1 時間ブロックされます。ユーザーアカウントのリストで、ブロックされたアカウントのユーザーアイコン（  ）が選択不可になります。パスワードを変更することでのみ、ユーザーアカウントのロックを解除できます。

- 必要に応じて［**アカウントの無効化**］をオンにすると、ユーザーは本製品に接続できなくなります。たとえば、従業員が退職したあとなどにアカウントを無効化できます。
- 不正な変更からユーザーアカウントを保護するために追加のオプションを有効にする場合は、［**アカウント設定の変更時にパスワードを要求する**］をオンにします。このオプションを有効にすると、ユーザーアカウントの設定の変更には、［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限を持つユーザーの認証が必要になります。

4. ［OK］をクリックします。

編集したユーザーアカウントが、［**ユーザーアカウント**］フォルダーの作業領域に表示されます。

許可されるパスワード入力試行回数の変更

Kaspersky Security Center ユーザーが無効なパスワードを入力できる回数には上限があります。入力回数が上限に達すると、ユーザーアカウントが 1 時間ブロックされます。

既定では、許可されるパスワードの入力試行回数の上限は 10 回です。このセクションの手順に従って、許可されるパスワード入力試行回数を変更できます。

許可されるパスワード入力試行回数を変更するには：

1. 管理サーバーがインストールされたデバイスのシステムレジストリを開きます（たとえば、ローカルで［**スタート**］→［**ファイル名を指定して実行**］で regedit コマンドを使用します）。
2. 次のキーに移動します：
   - 32 ビットシステム：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - 64 ビットシステム：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. 「SrvSplPpcLogonAttempts」という値が存在しない場合は、これを作成します。値の種別は DWORD です。

   既定では、この値は Kaspersky Security Center のインストール時に作成されません。

4. SrvSplPpcLogonAttempts に希望する値を入力します。

5. ［**OK**］をクリックして変更内容を保存します。

6. 管理サーバーサービスを再起動します。

   許可されるパスワードの入力試行回数の上限が変更されます。

内部ユーザーの名前に重複がないことの確認の設定

Kaspersky Security Center の内部ユーザーの名前を製品に追加する際、同じ名前がないかどうか確認するよう設定できます。内部ユーザーの名前に重複がないことの確認は、作成されるユーザーアカウントの対象となる仮想管理サーバーないしプライマリ管理サーバー、またはすべての仮想管理サーバーおよびプライマリ管理サーバーでのみ実行できます。既定では、内部ユーザーの名前は、すべての仮想管理サーバーおよびプライマリ管理サーバーで重複しないかどうかチェックされます。

内部ユーザーの名前を特定の仮想管理サーバーないしプライマリ管理サーバーで重複しないかどうかチェックするには：

1. 管理サーバーがインストールされたデバイスのシステムレジストリを開きます（たとえば、ローカルで［**スタート**］→［**ファイル名を指定して実行**］で regedit コマンドを使用します）。

2. 次のレジストリエントリに移動します：

   - 32 ビットシステム：

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

   - 64 ビットシステム：

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. LP_InterUserUniqVsScope（DWORD）キーの値を 00000001 に設定します。

   このキーの既定値は 0 です。

4. 管理サーバーサービスを再起動します。

   内部ユーザーの名前は、内部ユーザーが作成された仮想管理サーバー、またはプライマリ管理サーバーで内部ユーザーを作成した場合はプライマリ管理サーバーでのみ重複がないかどうかチェックされます。

内部ユーザーの名前をすべての仮想管理サーバーおよびプライマリ管理サーバーで重複しないかどうかチェックするには：

1. 管理サーバーがインストールされたデバイスのシステムレジストリを開きます（たとえば、ローカルで［**スタート**］→［**ファイル名を指定して実行**］で regedit コマンドを使用します）。

2. 次のレジストリエントリに移動します：

   - 64 ビットシステム：

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

- 32 ビットシステム：

  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. LP_InterUserUniqVsScope（DWORD）キーの値を 00000000 に設定します。

   このキーの既定値は 0 です。

4. 管理サーバーサービスを再起動します。

内部ユーザーの名前は、すべての仮想管理サーバーおよびプライマリ管理サーバーで重複しないかどうかチェックされます。

セキュリティグループの追加

セキュリティグループ（ユーザーのグループ）を追加し、様々なアプリケーションの機能に対して柔軟にグループやセキュリティグループのアクセス権を設定することができます。セキュリティグループには、個別の目的に対応した名前を割り当てることができます。たとえば、ユーザーのオフィスの場所や、所属している企業の組織単位に関連した名前を割り当てることができます。

1人のユーザーに対して複数のセキュリティグループを設定できます。仮想管理サーバーで管理されているユーザーアカウントは、仮想サーバー内のセキュリティグループにのみ所属し、仮想サーバー内でのみアクセス権を持つことができます。

セキュリティグループを追加するには：

1. コンソールツリーで、［**ユーザーアカウント**］フォルダーを選択します。

   既定では、［**ユーザーアカウント**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。

2. ［**セキュリティグループを追加**］をクリックします。

   ［**セキュリティグループを追加**］ウィンドウが表示されます。

3. ［**セキュリティグループを追加**］ウィンドウの［**全般**］セクションで、グループ名を指定します。

   グループ名は 255 文字以内で指定してください。特殊文字（*、<、>、?、\、:、| など）を使用することはできません。グループ名は一意である必要があります。

   グループの説明は［**説明**］に入力できます。［**説明**］への入力はオプションです。

4. ［**OK**］をクリックします。

追加したセキュリティグループは、コンソールツリーの［**ユーザーアカウント**］フォルダーに表示されます。新規作成したグループにユーザーを追加できます。

グループへのユーザーの追加

ユーザーをグループに追加するには：

1. コンソールツリーで、［**ユーザーアカウント**］フォルダーを選択します。

   既定では、［**ユーザーアカウント**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。

2. ユーザーアカウントとグループのリストから、ユーザーを追加するグループを選択します。

3. グループのプロパティウィンドウで、［**グループユーザー**］セクションを選択し、［**追加**］をクリックします。

ユーザーのリストのウィンドウが開きます。

4. リストの中から、グループに含めるユーザーを選択します。

5. ［**OK**］をクリックします。

ユーザーがグループに追加され、グループユーザーのリストに表示されます。

製品機能のアクセス権の設定：ロールベースのアクセス制御

Kaspersky Security Center には、Kaspersky Security Center と管理対象のカスペルスキー製品の機能へロールに基づくアクセスを提供する機能があります。

Kaspersky Security Center ユーザーのアプリケーション機能へのアクセス権は、次のいずれかの方法で設定できます：

- 各ユーザーまたはユーザーグループに対する権限を個別に設定します。
- 権限のセットが定義されている標準的なユーザーロールを作成し、職務範囲に応じてそれらのロールをユーザーに割り当てます。

ユーザーロール（ロールとも呼ばれます）は、Kaspersky Security Center または管理対象のカスペルスキー製品への事前定義された一連のアクセス権です。ロールは、ユーザーまたはユーザーグループに割り当てることができます。

ユーザーロールの適用は、アプリケーション機能に対するユーザーのアクセス権を設定する定型的な手順を簡素化および短縮することを目的としています。ロール内のアクセス権は、標準タスクとユーザーの職務範囲に従って設定されます。

ユーザーロールには、それぞれの目的に対応する名前を割り当てることができます。作成できるロール数に制限はありません。

事前定義されたユーザーロールを設定済みの権限セットで使用することも、新しいロールを作成して必要な権限を自分で設定することもできます。

アプリケーション機能へのアクセス権

次の表は、関連するタスク、レポート、設定を管理し、関連するユーザー操作を実行するためのアクセス権を備えた Kaspersky Security Center の機能を示しています。

表に一覧表示されているユーザー操作を実行するには、ユーザーは操作内容の横に指定された権限を有している必要があります。

［**読み取り**］、［**書き込み**］、および［**実行**］の各権限は、あらゆるタスク、レポート、設定に適用されます。これらの権限に加えて、ユーザーは、デバイスの抽出でタスクとレポートおよび設定を管理するため、**デバイスの抽出操作を実行**する権限を持っている必要があります。

表にないすべてのタスク、レポート、設定、およびインストールパッケージは、**一般的な機能：基本機能**にあります。

製品機能のアクセス権

機能領域	権限	ユーザー操作：操作を実行す	タスク	レポート	その他

		るために必要な権限			
一般的な機能：管理グループの管理	**書き込み**	• デバイスを管理グループに追加：**書き込み** • 管理グループからデバイスを削除：**書き込み** • 管理グループを別の管理グループに追加：**書き込み** • 別の管理グループから管理グループを削除：**書き込み**	なし	なし	なし
一般的な機能：ACL にかかわらずオブジェクトにアクセスする	**読み取り**	すべてのオブジェクトへの読み取り権限の取得：**読み取り**	なし	なし	なし
一般的な機能：基本的な機能	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• 仮想サーバーのデバイス移動ルール（作成、変更、または削除）：**書き込み**、**デバイスの選択に対する操作を実行** • モバイル（LWNGT）プロトコルのカスタム証明書の取得：**読み取り** • モバイル（LWNGT）プロトコルのカスタム証明書の取得：**書き込み** • NLA 定義のネットワークリストの取得：**読み取り** • NLA 定義のネットワークリストの追加、変更、または削除：**書き込み** • グループのアクセスコントロールリストの表示：**読み取り** • Kaspersky イベントログの表示：**読み取り**	• ［管理サーバーのリポジトリへのアップデートのダウンロード］ • ［レポートの配信］ • ［インストールパッケージの配布］ • ［セカンダリ管理サーバーへのアプリケーションのリモートインストール］	• ［保護ステータスレポート］ • ［脅威レポート］ • ［感染が多いデバイスのレポート］ • ［定義データベースのステータスレポート］ • ［エラーレポート］ • ［ネットワーク攻撃のレポート］ • ［インストールされているメールシステム保護製品のサマリーレポート］ • ［インストールされている境界防御製品のサマリーレポート］ • ［インストールされているアプリケーションの種別のサマリーレポート］ • ［感染したデバイスのユーザーに関するレポート］ • ［インシデントのレポート］ • ［イベントのレポート］ • ［ディストリビューションポイントのアクティ	なし

				ビティレポート］ • 「セカンダリ管理サーバーのレポート」 • ［デバイスコントロールイベントのレポート］ • ［脆弱性レポート］ • ［ブロック対象アプリケーションのレポート］ • 「ウェブコントロールレポート」 • ［管理対象デバイスの暗号化ステータスレポート］ • ［大容量ストレージデバイスの暗号化ステータスレポート］ • ［ファイル暗号化エラーのレポート］ • ［暗号化されたファイルへのアクセスのブロックに関するレポート］ • ［暗号化されたドライブへのアクセス権に関するレポート］ • 「有効なユーザー権限のレポート」 • ［ユーザー権限のレポート］	
一般的な機能：削除されたオブジェクト	• **読み取り** • **書き込み**	• ごみ箱に削除されたオブジェクトの表示：**読み取り** • ごみ箱からオブジェクトを削除：**書き込み**	なし	なし	なし
一般的な機能：イベント処理	• **イベントの削除** • **イベント通知設定の編集** • **イベントログ設定の編集** • **書き込み**	• イベント登録設定の変更：**イベントログ設定の編集** • イベント通知設定の変更：**イベント通知設定の編集** • イベントの削除：**イベントの削除**	なし	なし	設定： • ウイルスアウトブレイク の設定：ウイルスアウトブレイクイベントの作成に必要なウイルスアウトブレイクの検知数 • ウイルスアウトブレイクの設定：ウイルス検知の評価期間

					• データベース内に保存されるイベント数の上限 • 削除されたデバイスからのイベントを保存する期間
一般的な機能：管理サーバー上での操作	• **読み取り** • **書き込み** • **実行** • **オブジェクト ACL の変更** • **デバイスの抽出での操作の実行**	• ネットワークエージェント接続用の管理サーバーのポートを指定：**書き込み** • 管理サーバーで起動した Activation Proxy のポートを指定：**書き込み** • 管理サーバー上で開始したモバイル用の Activation Proxy のポートを指定：**書き込み** • スタンドアロンパッケージの配布用の Web サーバーのポートを指定：**書き込み** • MDM プロファイル配布用の Web サーバーのポートを指定：**書き込み** • Kaspersky Security Center Web コンソール経由で接続するための管理サーバーの SSL ポートを指定：**書き込み** • モバイル接続用の管理サーバーのポートを指定：**書き込み** • 管理サーバーデータベースに記録するイベント数の上限を指定：**書き込み** • 管理サーバーが送信可能なイベント数の上限を指定：**書き込み** • 管理サーバーがイベントを送信できる期間を指定：**書き込み**	• ［管理サーバーデータのバックアップ］ • データベースのメンテナンス	なし	なし
一般的な機能： カスペルスキー製品の導入	• **カスペルスキー製品のパッチの管理** • **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	パッチのインストールの承認または拒否： **カスペルスキー製品のパッチの管理**	なし	• ［仮想管理サーバーによるライセンス使用のレポート］ • ［カスペルスキー製品バージョンレポート］ • ［互換性のないアプリケーションのレポート］ • ［カスペルスキー製品のモジュールアップデートのバージョンに関するレポート］	インストールパッケージ：「カスペルスキー」

				• ［製品導入レポート］	
一般的な機能：ライセンス管理	• **ライセンス情報ファイルのエクスポート** • **書き込み**	• ライセンス情報ファイルのエクスポート：**ライセンス情報ファイルのエクスポート** • 管理サーバーのライセンス設定を変更：**書き込み**	なし	なし	なし
一般的な機能：適用されたレポートの管理	• **読み取り** • **書き込み**	• ACL にかかわらずレポートを作成：**書き込み** • ACL にかかわらずレポートを実行：**読み取り**	なし	なし	なし
一般的な機能：管理サーバーの階層構造	**管理サーバー階層の設定**	セカンダリ管理サーバーの登録、アップデート、または削除：**管理サーバー階層の設定**	なし	なし	なし
一般的な機能：ユーザー権限	**オブジェクト ACL の変更**	• 任意のオブジェクトのセキュリティプロパティの変更：**オブジェクト ACL の変更** • ユーザーロールの管理：**オブジェクト ACL の変更** • 内部ユーザーの管理：**オブジェクト ACL の変更** • セキュリティグループの管理：**オブジェクト ACL の変更** • エイリアスの管理：**オブジェクト ACL の変更**	なし	なし	なし
一般的な機能：仮想管理サーバー	• **仮想管理サーバーの管理** • **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• 仮想管理サーバーのリストの取得：**読み取り** • 仮想管理サーバーに関する情報の取得：**読み取り** • 仮想管理サーバーの作成、更新、または削除：**仮想管理サーバーの管理** • 仮想管理サーバーの別のグループへの移動：**仮想管理サーバーの管理** • 仮想管理サーバーの権限の設定：**仮想管理サーバーの管理**	なし	［サードパーティソフトウェアのアップデートのインストール結果に関するレポート］	なし
全般的な機能：暗号化鍵の管理	• **読み取り** • **書き込み**	• 暗号化鍵をエクスポート：**読み取り** • 暗号化鍵をインポート：**書き込み**	なし	なし	なし
モバイルデバイス管理：全般	• **新しいデバイスの接続**	• ライセンス管理サービスの復元データの取得：**読み取り**	なし	なし	なし

	• **モバイルデバイスへの情報コマンドのみの送信** • **モバイルデバイスへのコマンドの送信** • **証明書の管理** • **読み取り** • **書き込み**	• ユーザー証明書の削除：**証明書の管理** • ユーザー証明書の公開部分の取得：**読み取り** • 公開鍵インフラストラクチャが有効になっているかどうかの確認：**読み取り** • 公開鍵インフラストラクチャアカウントの確認：**読み取り** • 公開鍵インフラストラクチャテンプレートの入手：**読み取り** • 拡張キー使用証明書による公開キーインフラストラクチャテンプレートの取得：**読み取り** • 公開鍵インフラストラクチャが取り消されているかどうかの確認：**読み取り** • ユーザー証明書の発行設定の更新：**証明書の管理** • ユーザー証明書の発行設定の取得：**読み取り** • アプリケーション名とバージョンによるパッケージの取得：**読み取り** • ユーザー証明書の設定またはキャンセル：**証明書の管理** • ユーザー証明書の更新：**証明書の管理** • ユーザー証明書タグの設定：**証明書の管理** • MDM インストールパッケージ生成の実行、MDM インストールパッケージ生成のキャンセル：**新しいデバイスの接続**			
システム管理：接続性	• **RDP セッションの開始** • **既存の RDP セッションへの接続** • **トンネリングの開始** • **デバイスから管理者のワークステーションへ**	• デスクトップ共有セッションの作成：**デスクトップ共有セッションの作成権限** • RDPセッションの作成：**既存の RDP セッションへの接続** • トンネルの作成：**トンネリングの開始** • コンテンツネットワークリストの保存：**デバイスから管理者のワークステーションへのファイルの保存**	なし	［デバイスのユーザーに関するレポート］	なし

	のファイルの保存 • **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**				
システム管理：ハードウェアインベントリ	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• ハードウェアインベントリオブジェクトの取得またはエクスポート：**読み取り** • ハードウェアインベントリオブジェクトの追加、設定、または削除：**書き込み**	なし	• ［ハードウェアレジストリレポート］ • ［設定変更レポート］ • ［ハードウェアレポート］	なし
システム管理：ネットワークアクセスコントロール	• **読み取り** • **書き込み**	• CISCO の設定の表示：**読み取り** • CISCO の設定の変更：**書き込み**	なし	なし	なし
システム管理：オペレーティングシステムの導入	• **PXE サーバーの導入** • **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• PXE サーバーの導入：**PXE サーバーの導入** • PXE サーバーのリストの表示：**読み取り** • PXE クライアントでのインストールプロセスの開始または停止：**実行** • WinPE およびオペレーティングシステムイメージのドライバーの管理：**書き込み**	［基準デバイスの OS イメージに基づくインストールパッケージの作成］	なし	インストールパッケージ：［OS イメージ］
システム管理：脆弱性とパッチ管理	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• サードパーティのパッチプロパティの表示：**読み取り** • サードパーティのパッチプロパティを変更：**書き込み**	• ［Windows Update の同期の実行］ • ［Windows Update 更新プログラムのインストール］ • ［脆弱性の修正］ • ［アップデートのインストールと脆弱性の修正］	［ソフトウェアアップデートレポート］	なし
システム管理：リモートインストール	• **読み取り** • **書き込み** • **実行**	• サードパーティの脆弱性とパッチ管理に基づくインストールパッケージのプロパティの表示：**読み取り**	なし	なし	インストールパッケージ： • ［カスタムアプリケーション］ • ［VAPM パッケージ］

	• **デバイスの抽出での操作の実行**	• サードパーティの脆弱性とパッチ管理に基づくインストールパッケージのプロパティの変更：**書き込み**			
システム管理：**ソフトウェアインベントリ**	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	なし	なし	• ［インストール済みアプリケーションのレポート］ • ［アプリケーションのレジストリ履歴のレポート］ • ［ライセンス認証済みアプリケーショングループのステータスレポート］ • ［サードパーティ製品のライセンスに関するレポート］	なし

事前定義済みのユーザーロール

Kaspersky Security Center のユーザーに割り当てられたユーザーロールによって、アプリケーション機能への一連のアクセス権がユーザーに付与されます。

仮想サーバー上で作成されたユーザーには、管理サーバー上のロールを割り当てることはできません。

事前定義のユーザーロールを設定済みの権限セットで使用することも、新しいロールを作成して必要な権限を自分で設定することもできます。Kaspersky Security Center で利用可能な事前定義済みのユーザーロールの一部は、**監査**、**セキュリティ責任者**、**監督者**などの特定の役職（これらのロールは、バージョン 11 以降の Kaspersky Security Center に設定されています）に関連付けることができます。これらのロールのアクセス権は、関連する役職の標準タスクと職務の範囲に従って事前設定されています。次の表に、役割を特定の職位に関連付ける方法を示します。

特定の職位の役割の例

ロール	コメント
監査	削除されたオブジェクトの表示を含む、すべてのタイプのレポートでのすべての操作、すべての表示操作を許可します（［**削除されたオブジェクト**］領域で［**読み取り**］および［**書き込み**］の許可を付与します）。他の操作は許可されません。このロールは、組織の監査を実行する人に割り当てることができます。
上長・監督者	すべての表示操作を許可します。他の操作は許可されません。組織の IT セキュリティを担当しているセキュリティ責任者やその他のマネージャーにこのロールを割り当てることができます。
セキュリティ責任者	すべての表示操作を許可し、レポート管理を許可します。**システム管理**：**接続**領域で制限付きのアクセス許可を付与します。組織の IT セキュリティを担当しているセキュリティ責任者にこのロールを割り当てることができます。

次の表に、事前定義された各ユーザーロールに割り当てられているアクセス権を示します。

事前定義されたユーザーロールのアクセス権

ロール	説明
管理サーバーの管理者	次の機能領域でのすべての操作を許可します： • **一般的な機能**：

	• **基本機能** • **イベント処理** • **管理サーバーの階層構造** • **仮想管理サーバー** • **システム管理**： • **接続** • **ハードウェアインベントリ** • **ソフトウェアインベントリ** **一般的な機能：暗号化鍵の管理**機能領域における［**読み取り**］と［**書き込み**］の権限を付与します。
管理サーバーのオペレーター	次のすべての機能領域で**読み取り**および**実行**権限を付与します： • **一般的な機能**： • **基本機能** • **仮想管理サーバー** • **システム管理**： • **接続** • **ハードウェアインベントリ** • **ソフトウェアインベントリ**
監査	**一般的な機能**の機能領域で、すべての動作を許可します： • **ACL にかかわらずオブジェクトにアクセスする** • **削除されたオブジェクト** • **適用されたレポートの管理** このロールは、組織の監査を実行する人に割り当てることができます。
インストールの管理者	次の機能領域でのすべての操作を許可します： • **一般的な機能**： • **基本機能** • **カスペルスキー製品の導入** • **ライセンス管理** • **システム管理**： • **オペレーティングシステムの導入：** • **脆弱性とパッチ管理** • **リモートインストール** • **ソフトウェアインベントリ** ［**一般的な機能：仮想管理サーバー**］機能領域における**読み取り**と**実行**の権限を付与します。
インストールのオペレーター	次のすべての機能領域で**読み取り**および**実行**権限を付与します： • **一般的な機能**： • **基本機能** • **カスペルスキー製品の導入**（この領域で**カスペルスキー製品のパッチの管理**も許可されます） • **仮想管理サーバー**

	• **システム管理**： • **オペレーティングシステムの導入：** • **脆弱性とパッチ管理** • **リモートインストール** • **ソフトウェアインベントリ**
Kaspersky Endpoint Security の管理者	次の機能領域でのすべての操作を許可します： • **一般的な機能：基本的な機能** • すべての機能を含む Kaspersky Endpoint Security のエリア **一般的な機能：暗号化鍵の管理**機能領域における［**読み取り**］と［**書き込み**］の権限を付与します。
Kaspersky Endpoint Security オペレーター	次のすべての機能領域で**読み取り**および**実行**権限を付与します： • **一般的な機能：基本的な機能** • すべての機能を含む Kaspersky Endpoint Security のエリア
メインの管理者	次の領域を*除く*、**一般的な機能**の機能領域でのすべての操作を許可します。 • **ACL にかかわらずオブジェクトにアクセスする** • **適用されたレポートの管理** **一般的な機能：暗号化鍵の管理**機能領域における［**読み取り**］と［**書き込み**］の権限を付与します。
メインのオペレーター	次のすべての機能領域で**読み取り**および**実行**（該当する場合）権限を付与します： • **一般的な機能**： • **基本機能** • **削除されたオブジェクト** • **管理サーバー上での操作** • **カスペルスキー製品の導入** • **仮想管理サーバー** • **モバイルデバイス管理：全般** • すべての機能を含む**システム管理** • すべての機能を含む Kaspersky Endpoint Security のエリア
モバイルデバイス管理の管理者	次の機能領域でのすべての操作を許可します： • **一般的な機能：基本的な機能** • **モバイルデバイス管理：全般**
モバイルデバイス管理のオペレーター	**一般的な機能**：**基本機能**機能領域で**読み取り**および**実行**権限を付与します。 ［**モバイルデバイス管理**：**全般**］機能領域における**読み取り**権限と**モバイルデバイスに情報コマンドのみを送信する**権限を付与します。
セキュリティ責任者	［**一般的な機能**］の次の機能領域におけるすべての操作を許可します： • **ACL にかかわらずオブジェクトにアクセスする** • **適用されたレポートの管理** **システム管理：接続**機能領域の［**読み取り**］、［**書き込み**］、［**実行**］、［**デバイスから管理者のワークステーションにファイルを保存**］、［**デバイスの抽出を対象に処理を実行**］の各権限を付与します。 組織の IT セキュリティを担当しているセキュリティ責任者にこのロールを割り当てることができます。
セルフサービスポータルのユーザー	［**モバイルデバイス管理：セルフサービスポータル**］機能領域におけるすべての操作を許可します。この機能は、Kaspersky Security Center のバージョン 11 以降ではサポートされていません。

上長・監督者	［**一般的な機能**：**ACL に依存せずオブジェクトにアクセスする**］と［**一般的な機能**：**適用されたレポートの管理**］の機能領域における**読み取り**権限を付与します。 組織の IT セキュリティを担当しているセキュリティ責任者やその他のマネージャーにこのロールを割り当てることができます。
脆弱性とパッチ管理の管理者	［**一般的な機能**：**基本機能**］および［**システム管理**］（すべての機能を含む）機能領域でのすべての操作を許可します。
脆弱性とパッチ管理機能のオペレーター	［**一般的な機能**：**基本機能**］および［**システム管理**］（すべての機能を含む）機能領域で、**読み取り**および**実行**（該当する場合）の権限を付与します。

ユーザーロールの追加

ユーザーロールを追加するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウの［**セクション**］ペインで、［**ユーザーロール**］を選択し、［**追加**］をクリックします。

   ［**セキュリティ設定タブの表示**］をオンにすると、［**ユーザーロール**］セクションが使用できます。

4. **新規ロール**のプロパティウィンドウで、ロールを設定します：
   - ［**セクション**］から［**全般**］を選択し、ロールの名前を指定します。
     ロール名は 100 文字より長くすることはできません。
   - ［**権限**］セクションで、機能の横にある［**許可**］および［**拒否**］を選択して、権限セットを設定します。

   プライマリ管理サーバーで操作している場合は、［**ロールのリストをセカンダリ管理サーバーに転送する**］をオンにできます。
5. ［OK］をクリックします。

ロールが追加されます。

管理サーバー用に作成されたユーザーロールは、管理サーバーのプロパティウィンドウの［**ユーザーロール**］セクションに表示されます。ユーザーロールを変更および削除できます。同様に、ロールをセキュリティグループや選択したユーザーに割り当てることができます。

ユーザーまたはセキュリティグループへのロールの割り当て

ロールをユーザーまたはユーザーのグループに割り当てるには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウで、［**セキュリティ**］セクションを選択します。

インターフェイスの設定ウィンドウで［**セキュリティ設定タブの表示**］をオンにすると、［**セキュリティ**］セクションが使用できます。

4. ［**グループ名またはユーザー名**］で、ロールを割り当てるユーザーまたはユーザーグループを選択します。

   ユーザーまたはユーザーのグループがフィールドに含まれていない場合は、［**追加**］をクリックして追加できます。

   ［**追加**］をクリックしてユーザーを追加すると、ユーザー認証の種別を選択できます（Microsoft Windows または Kaspersky Security Center）。Kaspersky Security Center による認証は、仮想管理サーバーでの作業で使用される内部ユーザーのアカウントを選択する場合に使用されます。

5. ［**ロール**］タブを選択し、［**追加**］をクリックします。

   ［**ユーザーロール**］ウィンドウが表示されます。このウィンドウには、作成したユーザーロールが表示されます。

6. ［**ユーザーロール**］ウィンドウで、セキュリティグループのロールを選択します。

7. ［OK］をクリックします。

管理サーバーで作業するための権限セットが指定されたロールがユーザーまたはセキュリティグループに割り当てられます。割り当てられたロールは、管理サーバーのプロパティウィンドウの［**セキュリティ**］セクションの［**ロール**］タブに表示されます。

ユーザーとグループへの権限の割り当て

ユーザーとグループに、管理サーバーの様々な機能や、管理プラグインが組み込まれたカスペルスキー製品（例：Kaspersky Endpoint Security for Windows）の様々な機能を使用する権限を付与できます。

権限をユーザーまたはユーザーのグループに割り当てるには：

1. コンソールツリーで、次のいずれかの操作を行います：

   - **管理サーバー**フォルダーを展開し、目的の管理サーバーの名前の付いたフォルダーを選択します。
   - 管理グループを選択します。

2. 管理サーバーまたは管理グループのコンテキストメニューから［**プロパティ**］を選択します。

3. 管理サーバー（または管理グループ）のプロパティウィンドウが開いたら、左側の［**セクション**］ペインで［**セキュリティ**］を選択します。

   インターフェイスの設定ウィンドウで［**セキュリティ設定タブの表示**］をオンにすると、［**セキュリティ**］セクションが使用できます。

4. ［**セキュリティ**］セクションの［**グループ名またはユーザー名**］リストで、ユーザーまたはグループを選択します。

5. 作業領域下部の［**権限**］タブで、選択したユーザーまたはグループに付与する権限を設定します。

   a. 権限リストのフォルダーを展開して個別の権限の設定を編集するには、プラス記号（+）をクリックします。

b. 目的の権限の横にある［**許可**］および［**拒否**］を、必要に応じてオンにします。

例1：［**ACL にかかわらずオブジェクトにアクセスする**］フォルダーまたは［**削除されたオブジェクト**］フォルダーを展開して、［**読み取り**］権限を設定します。

例2：［**基本機能**］フォルダーを展開して、［**書き込み**］権限を設定します。

6. 権限の設定が完了したら、［**適用**］をクリックします。

ユーザーまたはユーザーグループに対する一連の権限が設定されます。

管理サーバー（または管理グループ）の権限は、次の領域から構成されます。

- 一般的な機能：
  - 管理グループの管理
  - ACL にかかわらずオブジェクトにアクセスする
  - 基本機能
  - 削除されたオブジェクト
  - イベント処理
  - 管理サーバー上での操作（管理サーバーのプロパティウィンドウのみ）
  - カスペルスキー製品の導入
  - ライセンス管理
  - 適用されたレポートの管理
  - サーバーの階層
  - ユーザー権限
  - 仮想管理サーバー
- モバイルデバイス管理：
  - 全般
- システム管理：
  - 接続
  - ハードウェアインベントリ
  - ネットワークアクセスコントロール
  - オペレーティングシステムの導入
  - 脆弱性とパッチの管理
  - リモートインストール

- ソフトウェアインベントリ

［**許可**］と［**拒否**］のどちらもオンになっていない場合、権限は［*未定義*］とみなされ、ユーザーに対して明示的に許可ないし拒否されるまでは拒否されます。

ユーザーの権限は次から構成されます：

- ユーザー自身の権限
- ユーザーに割り当てられたすべてのロールの権限
- ユーザーが属するすべてのセキュリティグループの権限
- ユーザーが属するセキュリティグループに割り当てられたすべてのロールの権限

これらの権限のうち1つでも［**拒否**］として設定されている場合、他の権限が許可または未定義でも、ユーザーは該当する権限が拒否されます。

セカンダリ管理サーバーにユーザーロールを反映させるには

既定では、プライマリ管理サーバーとセカンダリ管理サーバーのユーザーロールのリストは互いに独立しています。プライマリ管理サーバーで作成したユーザーロールをすべてのセカンダリ管理サーバーに自動的に反映するように、本製品を設定できます。任意のセカンダリ管理サーバーからその下位にあるセカンダリ管理サーバーにユーザーロールを反映できます。

プライマリ管理サーバーからセカンダリ管理サーバーにユーザーロールを反映するには：

1. メインウィンドウを開きます。
2. 次のいずれかの手順を実行します：
   - コンソールツリーで、管理サーバーの名前を右クリックし、コンテキストメニューの［**プロパティ**］を選択します。
   - 管理サーバーのアクティブなポリシーを使用できる場合、［**ポリシー**］フォルダーの作業領域でこのポリシーを右クリックし、コンテキストメニューの［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウまたはポリシーの設定ウィンドウの［**セクション**］ペインで、［**ユーザーロール**］を選択します。

   ［**セキュリティ設定タブの表示**］をオンにすると、［**ユーザーロール**］セクションが使用できます。

4. ［**ロールのリストをセカンダリ管理サーバーに転送する**］をオンにします。
5. ［OK］をクリックします。

プライマリ管理サーバーからセカンダリ管理サーバーにユーザーロールがコピーされます。

［**ロールのリストをセカンダリ管理サーバーに転送する**］がオンでユーザーロールが反映されている場合、セカンダリ管理サーバーの側でこれらのユーザーロールを編集したり削除したりすることはできません。プライマリ管理サーバーで新しいロールを作成したり既存のロールを編集すると、これらの変更を自動的にセカンダリ管理サーバーに反映します。プライマリ管理サーバーでユーザーロールを削除した場合、該当するロールはセカンダリ管理サーバーにそのまま残りますが、このロールの編集や削除が可能になります。

プライマリ管理サーバーからセカンダリ管理サーバーに反映されたロールにはロックアイコン（🔒）が表示されます。これらのロールはセカンダリ管理サーバーでは編集できません。

プライマリ管理サーバーで作成したロールと同じ名前のロールがセカンダリ管理サーバーに存在した場合、新しいロールがセカンダリ管理サーバーにコピーされる時に「~~1」や「~~2」のような接尾辞が追加されます（接尾辞はランダムに生成されます）。

［**ロールのリストをセカンダリ管理サーバーに転送する**］を無効にすると、すべてのユーザーロールはセカンダリ管理サーバーにそのまま残りますが、プライマリ管理サーバーのユーザーロールとは互いに独立した状態になります。独立した状態になった後は、セカンダリ管理サーバーでユーザーロールを編集、削除できます。

デバイスの所有者ユーザーの指定

ユーザーにデバイスを割り当て、デバイスの所有者として指定することができます。デバイス上で操作が必要な場合（ハードウェアのアップグレードなど）、管理者はデバイスの所有者にそれらの操作を行うように通知することができます。

デバイスの所有者としてユーザーを指定するには：

1. コンソールツリーで、［**管理対象デバイス**］フォルダーを選択します。
2. フォルダーの作業領域の［**デバイス**］タブで、所有者を指定するデバイスを選択します。
3. デバイスのコンテキストメニューで［**プロパティ**］を選択します。
4. デバイスのプロパティウィンドウで［**システム情報**］→［**セッション**］を選択します。
5. ［**デバイスの所有者**］の横にある［**割り当て**］をクリックします。
6. ［**ユーザーの選択**］ウィンドウで、デバイスの所有者として指定するユーザーを選択し、［**OK**］をクリックします。
7. ［**OK**］をクリックします。

デバイスの所有者が割り当てられます。既定では、［**デバイスの所有者**］には Active Directory からの値が表示され、Active Directory をポーリングするたびに値が更新されます。［**デバイスの所有者のレポート**］でデバイスの所有者のリストを表示することができます。新規レポートテンプレートウィザードを使用してレポートを作成できます。

ユーザーへのメッセージの配信

メッセージをメールでユーザーに送るには：

1. コンソールツリーで、［**ユーザーアカウント**］フォルダーからユーザーを選択します。
   既定では、［**ユーザーアカウント**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。
2. ユーザーのコンテキストメニューで、［**メールで通知**］を選択します。
3. ［**ユーザーにメッセージを送信**］ウィンドウの関連フィールドに入力し、［**OK**］をクリックします。

メッセージは、ユーザーのプロパティで指定されているメールアドレス宛てに送信されます。

SMS メッセージをユーザーに送るには：

1. コンソールツリーで、［**ユーザーアカウント**］フォルダーからユーザーを選択します。
2. ユーザーのコンテキストメニューで、［**SMS を送信**］を選択します。
3. ［**SMS テキスト**］ウィンドウの関連フィールドに入力し、［**OK**］をクリックします。

メッセージは、ユーザーのプロパティで指定されている番号のモバイルデバイスに送信されます。

ユーザーのモバイルデバイスのリストの表示

ユーザーのモバイルデバイスのリストを表示するには：

1. コンソールツリーで、［**ユーザーアカウント**］フォルダーからユーザーを選択します。
   既定では、［**ユーザーアカウント**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。
2. ユーザーアカウントのコンテキストメニューで、［**プロパティ**］を選択します。
3. ユーザーアカウントのプロパティウィンドウで、［**モバイルデバイス**］セクションを選択します。

［**モバイルデバイス**］セクションでは、ユーザーのモバイルデバイスのリストとそれらに関する情報を確認できます。［**ファイルへのエクスポート**］をクリックすると、モバイルデバイスのリストがファイルに保存されます。

ユーザー用証明書のインストール

次の 3 つの種別の証明書をインストールできます：

- 共有証明書：モバイルデバイスを識別するために必要です。
- メール証明書：モバイルデバイスで企業メールを設定するために必要です。
- VPN 証明書：モバイルデバイスで仮想プライベートネットワークを設定するために必要です。

ユーザーに証明書を発行してインストールするには：

1. コンソールツリーで、［**ユーザーアカウント**］フォルダーからユーザーアカウントを選択します。
   既定では、［**ユーザーアカウント**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。
2. ユーザーアカウントのコンテキストメニューで、［**証明書のインストール**］を選択します。

証明書インストールウィザードが起動します。ウィザードの指示に従ってください。

証明書インストールウィザードの終了後、証明書はユーザー用に作成およびインストールされます。インストール済みのユーザー証明書のリストを表示し、ファイルにエクスポートできます。

ユーザーに発行された証明書のリストの表示

ユーザーに発行されたすべての証明書のリストを表示するには：

1. コンソールツリーで、［**ユーザーアカウント**］フォルダーからユーザーを選択します。

既定では、［**ユーザーアカウント**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。

2. ユーザーアカウントのコンテキストメニューで、［**プロパティ**］を選択します。

3. ユーザーアカウントのプロパティウィンドウで、［**証明書**］セクションを選択します。

［**証明書**］セクションでは、ユーザーの証明書のリストとそれらに関する情報を確認できます。［**ファイルへのエクスポート**］をクリックすると、証明書のリストがファイルに保存されます。

仮想管理サーバーの管理について

仮想管理サーバーによって管理される組織ネットワークの管理者が Kaspersky Security Center Web コンソールを起動し、このウィンドウで指定したアカウント名で、アンチウイルスによる保護に関するデータを表示できます。

必要に応じて、複数の管理者アカウントを仮想サーバーに作成できます。

仮想サーバー上で作成されたユーザーには、管理サーバー上のロールを割り当てることはできません。

仮想管理サーバーの管理者は Kaspersky Security Center の内部ユーザーです。内部ユーザーに関するデータは、オペレーティングシステムには送信されません。Kaspersky Security Center が内部ユーザーを認証します。

オペレーティングシステムとアプリケーションのリモートインストール

Kaspersky Security Center では、オペレーティングシステムイメージを作成し、それをネットワーク上のクライアントデバイスに導入できます。また、カスペルスキー製品や他の製造元のアプリケーションのリモートインストールを行うこともできます。

オペレーティングシステムのイメージを作成するには、Windows ADK の導入ツールと Windows ADK ツール用の Windows PE アドオンを管理サーバーにインストールします。Kaspersky Security Center の要件を満たす任意のバージョンの Windowsオペレーティングシステムのイメージを作成できます 。

Kaspersky Security Center は、64 ビット版の Windows ADK および Windows PE をサポートしていません。

オペレーティングシステムイメージの取得

Kaspersky Security Center は、デバイスからオペレーティングシステムイメージを取得し、それを管理サーバーに転送できます。そのようなオペレーティングシステムイメージは管理サーバー上の専用フォルダーに格納されます。基準となるデバイスのオペレーティングシステムイメージの取得と作成は、インストールパッケージ作成タスクにより行われます。

オペレーティングシステムイメージを取得する機能には、次の特徴があります：

- オペレーティングシステムイメージは、管理サーバーがインストールされているデバイスでは取得できません。

- オペレーティングシステムイメージの取得中、sysprep.exe ユーティリティにより基準となるデバイスの設定がリセットされます。基準となるデバイスの設定を復元する場合は、OS イメージ作成タスク作成ウィザードで［**デバイスのステータスのバックアップコピーを作成する**］をオンにします。

- イメージの取得時、基準となるデバイスが再起動されます。

新規デバイスへのオペレーティングシステムイメージの導入

イメージを使用して、オペレーティングシステムがまだインストールされていない新しくネットワーク接続されたデバイスにオペレーティングシステムを導入できます。この場合、Preboot eXecution Environment（PXE）というテクノロジーが使用されます。PXE サーバーとして動作する、ネットワークに接続されたデバイスを選択します。このデバイスは次の要件を満たしている必要があります：

- ネットワークエージェントがデバイスにインストールされている。

- PXE サーバーで DHCP サーバーと同じポートが使用されているため、デバイス上で DHCP サーバーがアクティブになることはない。

- デバイスを含むネットワークセグメントには、他の PXE サーバーは含まれていない。

オペレーティングシステムを導入する場合、次の条件を満たしている必要があります：

- ネットワークエージェントがデバイスでマウントされている。

- デバイスがネットワークに接続されている。

- デバイスをブートする際、ネットワークブートオプションは BIOS で選択される。

オペレーティングシステムの導入は次のように実行されます：

1. クライアントデバイスは、起動プロセス中に PXE サーバーとの接続を確立します。

2. クライアントデバイスが Windows プレインストール環境（WinPE）で起動します。

   > デバイスを WinPE に追加するには、WinPE 用のドライバーの設定が必要な場合があります。

3. クライアントデバイスが管理サーバーに登録されます。

4. オペレーティングシステムイメージを含むインストールパッケージを管理者がクライアントデバイスに割り当てます。

   > 管理者は、オペレーティングシステムのイメージが含まれるインストールパッケージに必要なドライバーを追加できます。また管理者は、インストール時に適用されるオペレーティングシステムの設定が含まれる設定ファイル（アンサーファイル）を指定することもできます。

5. オペレーティングシステムがクライアントデバイスに導入されます。

管理者は、まだ接続されていないクライアントデバイスの MAC アドレスを手動で指定し、それらにオペレーティングシステムイメージを含むインストールパッケージを割り当てることができます。選択されたクライアントデバイスが PXE サーバーに接続すると、これらのデバイスに自動的にオペレーティングシステムがインストールされます。

既に別のオペレーティングシステムがインストールされているデバイスへのオペレーティングシステムイメージの導入

既に別のオペレーティングシステムがインストールされているクライアントデバイスにオペレーティングシステムイメージを導入するには、特定のデバイスに対するリモートインストールタスクを使用します。

オペレーティングシステムのクリーンインストールが実行されることに注意してください。すべてのデータが削除されます。

カスペルスキー製品および他の製造元のアプリケーションのインストール

管理者は、ユーザーから指定されたアプリケーションを含むインストールパッケージを作成し、リモートインストールタスクを使用して、そのアプリケーションをクライアントデバイスにインストールできます。

オペレーティングシステムイメージの作成

オペレーティングシステムのイメージは、基準となるデバイスのオペレーティングシステムイメージを削除するタスクを使用して作成されます。

オペレーティングシステムのイメージ作成タスクを作成するには：

1. コンソールツリーの［**リモートインストール**］フォルダーで、［**インストールパッケージ**］サブフォルダーを選択します。
2. ［**インストールパッケージの作成**］をクリックして、新規パッケージウィザードを実行します。
3. ウィザードの［**インストールパッケージの種別の選択**］ウィンドウで、［**オペレーティングシステムイメージを含むインストールパッケージを作成する**］をクリックします。
4. ウィザードの指示に従ってください。

   ウィザードが終了すると、［**基準デバイスの OS イメージに基づくインストールパッケージの作成**］という管理サーバーのタスクが作成されます。作成されたタスクは、［**タスク**］フォルダーで確認できます。

基準デバイスの OS イメージに基づくインストールパッケージの作成タスクが完了すると、インストールパッケージが作成され、これを使用して、PXE サーバーまたはリモートインストールタスクによりクライアントデバイスにオペレーティングシステムを導入することができます。［**インストールパッケージ**］フォルダーでインストールパッケージを確認できます。

オペレーティングシステムイメージのインストール

Kaspersky Security Center では、デスクトップおよびサーバーベースの Windows オペレーティングシステムの WIM イメージを、組織ネットワーク内のデバイスに導入することができます。

Kaspersky Security Center ツールを使用して導入可能なオペレーティングシステムイメージを取得するために、次の手法が使用できます：

- Windows 配布パッケージに含まれているファイル install.wim からのインポート
- 基準デバイスからのイメージの取得

オペレーティングシステムイメージの導入に対しては、次の 2 つの手法がサポートされています：

- オペレーティングシステムがインストールされていない「クリーンな」デバイスへの導入
- Windows を実行中のデバイスへの導入

オペレーティングシステムイメージをキャプチャして展開するには、Windows プレインストール環境（Windows PE）を使用します。すべての対象デバイスが正常に機能するために必要なドライバーをすべて WinPE に追加する必要があります。通常、ネットワークアダプターとストレージコントローラーのドライバーを追加する必要があります。

イメージの導入と取得を実行するには、次の要件を満たしている必要があります：

- Windows 自動インストールキット（WAIK）バージョン 2.0 以降、または Windows ADK の Windows PE アドオン を使用する Windows ADK が管理サーバーにインストールする必要があります。Windows XP でイメージのインストールまたは取得を実行するには、WAIK をインストールする必要があります。
- 対象デバイスが置かれているネットワーク上で DHCP サーバーが使用可能である。
- 対象デバイスが置かれているネットワークから読み取る場合は、管理サーバーの共有フォルダーを開く必要がある。共有フォルダーが管理サーバー内にある場合、KlPxeUser アカウントにアクセス権限を付与してください（管理サーバーのインストーラー実行中に自動的に作成されるアカウントです）。共有フォルダーが管理サーバー外に置かれている場合、すべてのユーザーにアクセス権限を付与する必要があります。

インストールするオペレーティングシステムイメージを選択する際には、管理者が対象デバイスの CPU アーキテクチャ（x86 または x86-64）を明示的に指定する必要があります。

KSN のプロキシサーバーアドレスの設定

既定では、管理サーバーの接続名または IP アドレスは、KSN プロキシサーバーのアドレスと一致しています。管理サーバーの接続名または IP アドレスを変更した場合、ホスト機器と KSN 間の接続の切断を避けるため、正しい KSN プロキシサーバーアドレスを指定する必要があります。

KSN のプロキシサーバーアドレスを設定するには：

1. コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］の順に選択します。
2. ［**インストールパッケージ**］のコンテキストメニューで、［**プロパティ**］を選択します。
3. 表示されたウィンドウの［**全般**］タブで、新しい KSN のプロキシサーバーアドレスを指定します。
4. ［**適用**］をクリックします。

以降、指定したアドレスが KSN のプロキシサーバーアドレスとして使用されます。ネットワーク上のトラフィックを最適化するには、［**KSN プロキシの使用**］をオンにすることを推奨します。

Windows プレインストール環境（WinPE）用のドライバーの追加

Windows プレインストール環境（WinPE）用のドライバーを追加するには：

1. コンソールツリーの［**リモートインストール**］フォルダーで、［**デバイスイメージの導入**］サブフォルダーを選択します。

2. ［**デバイスイメージの導入**］フォルダーの作業領域で、［**その他の操作**］をクリックし、ドロップダウンリストから［**Windows プレインストール環境(WinPE)のドライバーセットの設定**］を選択します。

   ［**Windows プレインストール環境ドライバー**］ウィンドウが表示されます。

3. ［**Windows プレインストール環境ドライバー**］ウィンドウで、［**追加**］をクリックします。

   ［**ドライバーの選択**］ウィンドウが表示されます。

4. ［**ドライバーの選択**］ウィンドウで、リストからドライバーを選択します。

   必要なドライバーがリストに表示されない場合は、［**追加**］をクリックし、開かれる［**ドライバーの追加**］ウィンドウでドライバー名とドライバー配布パッケージのフォルダーを指定します。

   フォルダーを選択するには、［**参照**］をクリックします。

   ［**ドライバーの追加**］ウィンドウで、［**OK**］をクリックします。

5. ［**ドライバーの選択**］ウィンドウで、［**OK**］をクリックします。

   ドライバーが管理サーバーリポジトリに追加されます。リポジトリに追加されたドライバーは、［**ドライバーの選択**］ウィンドウに表示されます。

6. ［**Windows プレインストール環境ドライバー**］ウィンドウで、［**OK**］をクリックします。

ドライバーが Windows プレインストール環境（WinPE）に追加されます。

オペレーティングシステムイメージを含むインストールパッケージへのドライバーの追加

オペレーティングシステムイメージを含むインストールパッケージにドライバーを追加するには：

1. コンソールツリーの［**リモートインストール**］フォルダーで、［**インストールパッケージ**］サブフォルダーを選択します。

2. オペレーティングシステムイメージを含むインストールパッケージのコンテキストメニューから、［**プロパティ**］を選択します。

   インストールパッケージのプロパティウィンドウが表示されます。

3. インストールパッケージのプロパティウィンドウで、［**追加ドライバー**］セクションを選択します。

4. ［**追加ドライバー**］セクションの［**追加**］をクリックします。

   ［**ドライバーの選択**］ウィンドウが表示されます。

5. ［**ドライバーの選択**］ウィンドウで、オペレーティングシステムイメージを含むインストールパッケージに追加するドライバーを選択します。

   ［**ドライバーの選択**］ウィンドウで［**追加**］をクリックすることにより、管理サーバーリポジトリに新しいドライバーを追加できます。

6. ［**OK**］をクリックします。

追加したドライバーが、オペレーティングシステムイメージを含むインストールパッケージのプロパティウィンドウの［**追加ドライバー**］セクションに表示されます。

sysprep.exe ユーティリティの設定

sysprep.exe ユーティリティは、オペレーティングシステムのイメージ作成のためにデバイスを準備するためのユーティリティです。

sysprep.exe ユーティリティを設定するには：

1. コンソールツリーの［**リモートインストール**］フォルダーで、［**インストールパッケージ**］サブフォルダーを選択します。
2. オペレーティングシステムイメージを含むインストールパッケージのコンテキストメニューから、［**プロパティ**］を選択します。

   インストールパッケージのプロパティウィンドウが表示されます。
3. インストールパッケージのプロパティウィンドウで、［**sysprep.exe 設定**］セクションを選択します。
4. ［**sysprep.exe 設定**］セクションで、クライアントデバイスにオペレーティングシステムを導入する時に使用する設定ファイルを指定します：

   - **既定の設定ファイルの使用**：オペレーティングシステムイメージの取得時に既定で生成されたアンサーファイルを使用するには、このオプションを選択します。
   - **主要な設定のカスタム値の指定**：ユーザーインターフェイスを介して設定値を指定するには、このオプションを選択します。
   - **設定ファイルの指定**：カスタムアンサーファイルを使用するには、このオプションを選択します。
5. 変更を適用するには［**適用**］をクリックします。

ネットワークに新たに接続されたデバイスへのオペレーティングシステムの導入

オペレーティングシステムがまだインストールされていない新規デバイスにオペレーティングシステムを導入するには：

1. コンソールツリーの［**リモートインストール**］フォルダーで、［**デバイスイメージの導入**］サブフォルダーを選択します。

   ［**インターフェイスの設定**］ウィンドウで［**脆弱性とパッチ管理の表示**］がオンになっていることを確認します。それ以外の場合、［**リモートインストール**］フォルダーは表示されません。
2. ［**その他の操作**］をクリックして、ドロップダウンリストで［**ネットワーク内の PXE サーバーリストの管理**］を選択します。

   ［**PXE サーバー**］セクションに、**デバイスイメージの導入**のプロパティウィンドウが開きます。
3. ［**PXE サーバー**］セクションの［**追加**］をクリックし、［**PXE サーバー**］ウィンドウが表示されたら、PXE サーバーとして使用するデバイスを選択します。

   追加したデバイスが［PXE サーバー］セクションに表示されます。作成された WinPE ファイルは、管理サーバーからデバイスに転送されます。ファイル転送プロセスには通常 10 分かかります。転送が完了すると、表示される［**ステータス**］の値が［**開始中**］から［**準備完了**］に変わります。

4. ［**PXE サーバー**］セクションで PXE サーバーを選択し、［**プロパティ**］をクリックします。

5. 選択した PXE サーバーのプロパティウィンドウの［**PXE サーバーの接続設定**］タブで、管理サーバーと PXE サーバーとの間の接続を設定します。

6. オペレーティングシステムを導入するクライアントデバイスを起動します。

7. クライアントデバイスの BIOS で、ネットワーク起動インストールオプションを選択します。

   クライアントデバイスが PXE サーバーに接続され、［**デバイスイメージの導入**］フォルダーの作業領域に表示されます。

8. ［**処理**］セクションで［**インストールパッケージの割り当て**］をクリックして、選択したデバイスにオペレーティングシステムをインストールするために使用するインストールパッケージを選択します。

   抽出したデバイスで DiskPart ツールを使用して、使用可能なディスクを確認します。Windows PE コマンドプロンプトで `diskpart` と入力し、DiskPart ツールを開きます。`list disk` と入力してディスクを一覧表示します。

   デバイスを追加し、インストールパッケージを割り当てると、そのデバイスでオペレーティングシステム導入が自動的に開始されます。

9. クライアントデバイスへのオペレーティングシステムの導入をキャンセルするには、［**処理**］セクションで［**OS イメージのインストールのキャンセル**］をクリックします。

MAC アドレスでデバイスを追加するには：

- ［**デバイスイメージの導入**］フォルダーで［**デバイスの MAC アドレスの追加**］をクリックします。［**新しいデバイス**］ウィンドウが表示されたら、追加するデバイスの MAC アドレスを指定します。

- ［**デバイスイメージの導入**］フォルダーで［**デバイスの MAC アドレスをファイルからインポート**］をクリックして、オペレーティングシステムを導入するすべてのデバイスの MAC アドレスのリストが記述されたファイルを選択します。

クライアントデバイスへのオペレーティングシステムの導入

別のオペレーティングシステムが既にインストールされているクライアントデバイスに、オペレーティングシステムを導入するには：

1. コンソールツリーで［**リモートインストール**］フォルダーを開き、［**管理対象デバイス（ワークステーション）にインストールパッケージを配布**］をクリックして製品導入ウィザードを起動します。

2. ウィザードの［**インストールパッケージの選択**］ウィンドウで、オペレーティングシステムイメージが入ったインストールパッケージを指定します。

3. ウィザードの指示に従ってください。

ウィザードの処理が完了すると、クライアントデバイスにオペレーティングシステムをインストールするためのリモートインストールタスクが作成されます。作成されたタスクは、［**タスク**］フォルダーで開始または停止できます。

アプリケーションのインストールパッケージの作成

アプリケーションインストールパッケージを作成するには：

1. コンソールツリーの［**リモートインストール**］フォルダーで、［**インストールパッケージ**］サブフォルダーを選択します。

2. ［**インストールパッケージの作成**］をクリックして、新規パッケージウィザードを実行します。

3. ウィザードの［**インストールパッケージの種別の選択**］ウィンドウで、次のいずれかのボタンをクリックします：

- **カスペルスキー製品のインストールパッケージを作成する**：カスペルスキー製品のインストールパッケージを作成する場合、このオプションを選択します。

- **指定した実行ファイルのインストールパッケージを作成する**：実行ファイルを使用してサードパーティ製品のインストールパッケージを作成する場合、このオプションを選択します。通常、実行ファイルはアプリケーションのセットアップファイルです。

  - **フォルダー全体をインストールパッケージへコピー**

    アプリケーションのインストールに、実行ファイル以外のファイルが追加で必要となる場合、このオプションを選択します。このオプションをオンにする前に、必要なすべてのファイルが同じフォルダーに保存されていることを確認してください。このオプションをオンにすると、指定した実行ファイルを含めてフォルダー内のすべてのファイルがインストールパッケージに追加されます。

  - **インストールパラメータの指定**

    リモートインストールを正常に完了させるには、ほとんどの製品において、サイレントモードでのインストールの実行が適しています。この場合は、サイレントインストール用のパラメータを指定する必要があります。

    インストール設定を編集します：

    - **実行ファイルのコマンドライン**

      インストール対象のアプリケーションでサイレントインストールのパラメータを指定する必要がある場合は、このフィールドで指定します。詳細については、該当する製品の製造元の資料を参照してください。

      その他のパラメータを指定することもできます。

    - **Kaspersky Security Center で認識されたアプリケーションの設定値を推奨値に変換する**

      カスペルスキーのデータベースに該当するアプリケーションの情報が含まれていた場合は、アプリケーションは推奨設定でインストールされます。

      ［**実行ファイルのコマンドライン**］でパラメータを指定していた場合も、推奨設定でパラメータが上書きされます。

      既定では、このオプションはオンです。

      カスペルスキーのデータベースは、カスペルスキーの担当者によって作成・維持されています。データベースに追加されたそれぞれのアプリケーションに対して、カスペルスキーの担当者が最適なインストール設定を指定しています。これらの設定は、クライアントデバイスへのリモートインストールが正常に完了するように指定されます。管理サーバー上のこのデータベースは、管理サーバーのリポジトリへのアップデートのダウンロードタスクの実行時に自動的にアップデートされます。

- **カスペルスキーのデータベースからアプリケーションを選択してインストールパッケージを作成する**：カスペルスキーのデータベースからサードパーティ製品を選択し、インストールパッケージを選択する場合、このオプションを選択します。データベースは管理サーバーのリポジトリへのアップデートのダウンロードタスクの実行時に自動的に作成され、リスト内にアプリケーションが表示されます。

- **オペレーティングシステムイメージを含むインストールパッケージを作成する**：このオプションは、基準となるデバイスのオペレーティングシステムイメージが入ったインストールパッケージを作成する必要がある場合に選択します。

  ウィザードが終了すると、［**基準デバイスの OS イメージに基づくインストールパッケージの作成**］という名前の管理サーバータスクが作成されます。このタスクが完了すると、インストールパッケージが作成され、これを使用して、PXE サーバーまたはリモートインストールタスクによりオペレーティングシステムイメージを導入することができます。

4. ウィザードの指示に従ってください。

ウィザードが終了すると、クライアントデバイスにアプリケーションをインストールするのに使用できるインストールパッケージが作成されます。コンソールツリーの［**インストールパッケージ**］フォルダーを選択すると、インストールパッケージを確認できます。

アプリケーションのインストールパッケージ用の証明書の発行

アプリケーションのインストールパッケージ用の証明書を発行するには：

1. コンソールツリーの［**リモートインストール**］フォルダーで、［**インストールパッケージ**］サブフォルダーを選択します。

   既定では［**リモートインストール**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。

2. ［**インストールパッケージ**］フォルダーのコンテキストメニューで、［**詳細**］を選択します。

   ［**インストールパッケージ**］フォルダーのプロパティウィンドウが開きます。

3. ［**インストールパッケージ**］フォルダーのプロパティウィンドウで、［**スタンドアロンパッケージに署名**］セクションを選択します。

4. ［**スタンドアロンパッケージに署名**］セクションで、［**設定**］をクリックします。

   ［**証明書**］ウィンドウ。

5. ［**証明書の種別**］で、証明書の種別について、プライベート証明書か公開証明書かを選択します。

   - ［**PKCS #12 コンテナー**］を選択した場合は、証明書を指定してパスワードを設定します。
   - ［**X.509 証明書**］を選択した場合：

     a. 秘密鍵ファイルを指定します（拡張子が *.prk または *.pem のファイル）。

     b. 秘密鍵のパスワードを指定します。

     c. 公開鍵のパスワードを指定します（拡張子が *.cer のファイル）。

6. ［**OK**］をクリックします。

アプリケーションのインストールパッケージ用の証明書が作成されます。

クライアントデバイスへのアプリケーションのインストール

アプリケーションをクライアントデバイスにインストールするには：

1. コンソールツリーで［**リモートインストール**］フォルダーを開き、［**管理対象デバイス（ワークステーション）にインストールパッケージを配布**］をクリックして製品導入ウィザードを起動します。
2. ウィザードの［**インストールパッケージの選択**］ウィンドウで、インストールするアプリケーションのインストールパッケージを指定します。
3. ウィザードの指示に従ってください。

ウィザードが終了すると、リモートインストールタスクが作成され、クライアントデバイスにアプリケーションがインストールされます。作成されたタスクは、［**タスク**］フォルダーで開始または停止できます。

製品導入ウィザードを使用することにより、Windows、Linux および macOS が動作しているクライアントデバイスにネットワークエージェントをインストールすることができます。

Kaspersky Security Center を使用し、Linux オペレーティングシステムが動作しているデバイスで 64 ビットのセキュリティ製品を管理するには、64 ビット版の Linux 用のネットワークエージェントを使用する必要があります。目的のバージョンのネットワークエージェントは、テクニカルサポートサイトからダウンロードできます。

Linux で動作するデバイスにネットワークエージェントをリモートインストールするには、デバイスを準備する必要があります。

オブジェクトリビジョンの管理

このセクションでは、オブジェクトのリビジョン管理について説明します。Kaspersky Security Center では、オブジェクトの変更を追跡できます。オブジェクトに変更を加えるたびに、*リビジョン*が作成されます。各リビジョンには番号が付いています。

リビジョン管理に対応するアプリケーションオブジェクトは次の通りです：

- 管理サーバーのプロパティ
- ポリシー
- タスク
- 管理グループ
- ユーザーアカウント
- インストールパッケージ

オブジェクトのリビジョンには次の処理を行うことができます：

- 選択したリビジョンを現在のリビジョンと比較する
- 選択したリビジョンを比較
- 同じ種別の別のオブジェクトのリビジョンを比較対象として選択し、オブジェクトと比較する

- 選択したリビジョンを表示する
- オブジェクトに対して行った変更を、選択したリビジョンにロールバックする
- リビジョンをテキストファイルとして保存する

リビジョン管理に対応するオブジェクトのプロパティウィンドウの［**変更履歴**］セクションには、オブジェクトのリビジョンのリストが次の詳細とともに表示されます：

- オブジェクトのリビジョン番号
- オブジェクトが変更された日時
- オブジェクトを変更したユーザーの名前
- オブジェクトに対する操作
- オブジェクト設定に対して行われた変更に関連するリビジョンの説明

オブジェクトリビジョンについて

オブジェクトのリビジョンには次の処理を行うことができます：

- 選択したリビジョンを現在のリビジョンと比較する
- 選択したリビジョンを比較
- 同じ種別の別のオブジェクトのリビジョンを比較対象として選択し、オブジェクトと比較する
- 選択したリビジョンを表示する
- オブジェクトに対して行った変更を、選択したリビジョンにロールバックする
- リビジョンをテキストファイルとして保存する

リビジョン管理に対応するオブジェクトのプロパティウィンドウの［**変更履歴**］セクションには、オブジェクトのリビジョンのリストが次の詳細とともに表示されます：

- オブジェクトのリビジョン番号
- オブジェクトが変更された日時
- オブジェクトを変更したユーザーの名前
- オブジェクトに対する操作
- オブジェクト設定に対して行われた変更に関連するリビジョンの説明

［変更履歴］セクションの表示

オブジェクトのリビジョンを現在のリビジョンと比較したり、リストで選択した複数のリビジョンを比較したりすることができます。また、オブジェクトのリビジョンを同じ種別の別のオブジェクトのリビジョンと比較することも可能です。

*オブジェクトの［**変更履歴**］セクションを表示するには：*

1. コンソールツリーで、次のいずれかのオブジェクトを選択します：
   - ［**管理サーバー**］フォルダー
   - ［**ポリシー**］フォルダー
   - ［**タスク**］フォルダー
   - 管理グループのフォルダー
   - ［**ユーザーアカウント**］フォルダー
   - ［**削除されたオブジェクト**］フォルダー
   - ［**インストールパッケージ**］サブフォルダー（［**リモートインストール**］フォルダーの下）
2. 該当するオブジェクトの場所に応じて、次のいずれかの手順を実行します：
   - オブジェクトが［**管理サーバー**］ノードまたは管理グループノードにある場合、ノードを右クリックして、コンテキストメニューで［**プロパティ**］を選択します。
   - オブジェクトが［**ポリシー**］、［**タスク**］、［**ユーザーアカウント**］、［**削除されたオブジェクト**］、［**インストールパッケージ**］フォルダーのいずれかに存在する場合、フォルダーを選択して、表示される作業領域でオブジェクトを選択します。

   オブジェクトのプロパティウィンドウが開きます。
3. 左側の［**セクション**］ペインで、［**変更履歴**］を選択します。

   変更履歴が作業領域に表示されます。

オブジェクトリビジョンの比較

オブジェクトの過去のリビジョンを現在のリビジョンと比較したり、リストで選択した複数のリビジョンを比較したりすることができます。また、オブジェクトのリビジョンを同じ種別の別のオブジェクトのリビジョンと比較することも可能です。

オブジェクトのリビジョンを比較するには：

1. オブジェクトを選択して、プロパティウィンドウを開きます。
2. プロパティウィンドウで［**変更履歴**］セクションに移動します。
3. 作業領域のオブジェクトのリビジョンのリストで、比較するリビジョンを選択します。
   オブジェクトの 2 つ以上のリビジョンを選択するには、**SHIFT** キーと **CTRL** キーを使用します。
4. 次のいずれかの手順を実行します：

- ［**比較**］をクリックして、ドロップダウンリストからいずれかの値を選択します。
  - **現在のリビジョンと比較**

    このオプションをオンにすると、選択したリビジョンと現在のリビジョンを比較できます。

  - **選択したリビジョンを比較**

    このオプションをオンにすると、選択した 2 つのリビジョンを比較できます。

  - **他のタスクと比較**

    タスクのリビジョンが対象の場合、選択したリビジョンを他のタスクのリビジョンと比較するには、［**他のタスクと比較**］をオンにします。

    ポリシーのリビジョンが対象の場合、選択したリビジョンを他のポリシーのリビジョンと比較するには、［**他のポリシーと比較**］をオンにします。

- リビジョン名をダブルクリックし、リビジョンのプロパティウィンドウが表示されたら、次のいずれかのボタンをクリックします。
  - **最新と比較**

    このボタンをクリックすると、選択したリビジョンと最新のリビジョンを比較できます。

  - **直前と比較**

    このボタンをクリックすると、選択したリビジョンと直前のリビジョンを比較できます。

既定のブラウザーで、リビジョンの比較に関する HTML 形式のレポートが表示されます。

このレポートでは、リビジョン設定を含むセクションを一部最小化することができます。オブジェクトのリビジョン設定のセクションを最小化するには、セクション名に隣接する矢印アイコン（▲）をクリックします。

管理サーバーのリビジョンには、これまでの変更の詳細がすべて記載されていますが、次の領域の情報は含まれていません：

- ［**トラフィック**］セクション
- ［**タグルール**］セクション
- ［**通知**］セクション
- ［**ディストリビューションポイント**］セクション
- ［**ウイルスアウトブレイク**］セクション

  ［**ウイルスアウトブレイク**］セクションからは、ウイルスアウトブレイクイベントが発生した時に起こるポリシーのアクティブ化の設定に関する情報は記録されません。

削除されたオブジェクトのリビジョンを既存のオブジェクトのリビジョンと比較することはできますが、比較対象を逆にして、既存のオブジェクトのリビジョンを削除されたオブジェクトのリビジョンと比較することはできません。

オブジェクトリビジョンと削除されたオブジェクトの情報の保存期間の設定

オブジェクトリビジョンの保存期間と削除されたオブジェクトの情報の保存期間は同じです。既定では、保存期間は 90 日です。これは、プログラムの定期的な監査にとって十分な期間となります。

［**削除されたオブジェクト**］領域で［**変更**］権限を付与されたユーザーだけが保存期間を変更できます。

オブジェクトリビジョンと削除されたオブジェクトの情報の保存期間を変更するには：

1. コンソールツリーで、保存期間を変更する管理サーバーを選択します。
2. 右クリックして、コンテキストメニューから［**プロパティ**］を選択する。
3. 表示される管理サーバーのプロパティウィンドウの［**変更履歴リポジトリ**］セクションで、希望する保存期間を入力します（日単位）。
4. ［**OK**］をクリックします。

オブジェクトリビジョンと削除されたオブジェクトの情報が、指定した日数保存されます。

オブジェクトリビジョンの表示

特定の期間中にオブジェクトに対して行われた変更を把握する必要がある場合は、このオブジェクトのリビジョンを表示できます。

オブジェクトのリビジョンを表示するには：

1. オブジェクトの［**変更履歴**］セクションに移動します。
2. オブジェクトのリビジョンのリストで、表示する設定のリビジョンを選択します。
3. 次のいずれかの手順を実行します：
   - ［**リビジョンの表示**］をクリックします。
   - リビジョン名をダブルクリックし、［**リビジョンの表示**］をクリックして、リビジョンのプロパティウィンドウを開きます。

選択したオブジェクトのリビジョンの設定を示す HTML 形式のレポートが表示されます。このレポートでは、オブジェクトのリビジョン設定のセクションを一部最小化することができます。オブジェクトのリビジョン設定のセクションを最小化するには、セクション名に隣接する矢印アイコン（▲）をクリックします。

ファイルへのオブジェクトリビジョンの保存

たとえば、メールで送信するために、オブジェクトのリビジョンをテキストファイルに保存できます。

オブジェクトのリビジョンをファイルに保存するには：

1. オブジェクトの［**変更履歴**］セクションに移動します。
2. オブジェクトのリビジョンのリストで、設定を保存するリビジョンを選択します。
3. ［**詳細**］をクリックして、ドロップダウンリストから［**ファイルに保存**］を選択します。

   リビジョンが txt ファイルとして保存されます。

変更のロールバック

必要に応じて、オブジェクトの変更をロールバックできます。たとえば、ポリシーの設定を特定の日付の状態まで戻さなければならない場合があります。

オブジェクトの変更をロールバックするには：

1. オブジェクトの［**変更履歴**］セクションに移動します。
2. オブジェクトのリビジョンのリストで、変更のロールバック先となるリビジョンの番号を選択します。
3. ［**詳細**］をクリックして、ドロップダウンリストから［**ロールバック**］を選択します。

   オブジェクトが、選択したリビジョンにロールバックされます。オブジェクトのリビジョンのリストには、実行された処理の記録が表示されます。リビジョンの説明には、オブジェクトを元に戻したリビジョン番号に関する情報が表示されます。

リビジョンの説明の追加

リスト内でリビジョンが検索しやすくなるように、リビジョンに説明を追加することができます。

リビジョンに説明を追加するには：

1. オブジェクトの［**変更履歴**］セクションに移動します。
2. オブジェクトのリビジョンのリストから、説明を追加するリビジョンを選択します。
3. ［**説明**］をクリックします。
4. ［**オブジェクトのリビジョンの説明**］ウィンドウで、リビジョンの説明を入力します。

   既定では、オブジェクトのリビジョンの説明は空になっています。
5. ［**OK**］をクリックします。

オブジェクトの削除

このセクションでは、オブジェクトの削除と、削除後にオブジェクトの情報を表示する方法について説明します。

次のオブジェクトを削除できます：

- ポリシー
- タスク
- インストールパッケージ
- 仮想管理サーバー
- ユーザー
- セキュリティグループ
- 管理グループ

オブジェクトを削除しても、オブジェクトの情報はデータベースに保存されます。削除されたオブジェクトの情報の保存期間は、オブジェクトの履歴の保存期間（推奨期間は 90 日）と同じです。［**削除されたオブジェクト**］領域の権限で**変更**権限を付与されたユーザーのみが、保存期間を変更できます。

クライアントデバイスの削除について

管理グループから管理対象デバイスを削除すると、アプリケーションはそのデバイスを未割り当てデバイスグループに移動します。デバイスの削除後、インストールされているカスペルスキー製品（ネットワークエージェント、Kaspersky Endpoint Security などのセキュリティ製品）はデバイス上に残ります。

Kaspersky Security Center は、次のルールに従って、未割り当てデバイスグループ内のデバイスを処理します：

- デバイス移動ルールを設定しており、デバイスが移動ルールの基準を満たしている場合、デバイスはルールに従って管理グループに自動的に移動されます。
- デバイスは未割り当てデバイスグループに保存され、デバイス保持ルールに従ってグループから自動的に削除されます。

  デバイスの保持ルールは、ディスク全体の暗号化で暗号化された 1 つ以上のドライブを備えたデバイスには影響しません。このようなデバイスは自動的に削除されず、手動でのみ削除できます。暗号化されたドライブを含むデバイスを削除する必要がある場合は、まずドライブを復号化してから、デバイスを削除します。

  > 暗号化されたドライブを含むデバイスを削除すると、ドライブの復号化に必要なデータも削除されます。このようなデバイス（［Unassigned devices**未割り当てデバイス**Managed Devices**管理対象デバイス**リスクを理解した上で、選択したデバイスを削除します］をオンにした場合は、その後のデータ削除を認識していることを意味します。

  ドライブを復号化するには、次の条件を満たす必要があります：

  - デバイスは管理サーバーに再接続され、ドライブの復号化に必要なデータが復元されます。
  - デバイスのユーザーは復号化パスワードを覚えています。
  - ドライブの暗号化に使用されたセキュリティ製品（Kaspersky Endpoint Security for Windows など）は、デバイスにまだインストールされています。

  ドライブが Kaspersky Disk Encryption 技術によって暗号化されている場合は、FDERT 復元ユーティリティを使用してデータの回復を試行することもできます。

未割り当てデバイスグループからデバイスを手動で削除すると、アプリケーションはそのデバイスをリストから削除します。デバイスを削除した後、インストールされているカスペルスキー製品はデバイス上に残ります。その後、デバイスがまだ管理サーバーに表示されており、定期的なネットワークポーリングを設定している場合、Kaspersky Security Center はネットワークポーリング中にデバイスを検出し、未割り当てデバイスグループに追加します。したがって、デバイスが管理サーバーに表示されない場合にのみ、デバイスを手動で削除することが合理的です。

オブジェクトの削除

［基本機能］領域の権限で［変更］権限を付与されている場合（詳しくは「ユーザーとグループへの権限の割り当て」を参照）、ポリシーやタスク、インストールパッケージ、内部ユーザー、内部セキュリティグループなどのオブジェクトを削除できます。

オブジェクトを削除するには：

1. コンソールツリーで、目的のフォルダーの作業領域でオブジェクトを選択します。
2. 次のいずれかの手順を実行します：
   - オブジェクトを右クリックして、［**削除**］を選択します。
   - **DELETE** キーを押します。

オブジェクトは削除され、オブジェクトに関する情報はデータベースに保存されます。

削除されたオブジェクトの情報の表示

削除されたオブジェクトの情報はオブジェクトの履歴と同じ期間（推奨する長さは 90 日）、［**削除されたオブジェクト**］フォルダーに保存されます。

［**削除されたオブジェクト**］領域の権限で**読み取り**権限を付与されたユーザーのみが、削除されたオブジェクトのリストを表示できます（詳しくは「ユーザーとグループへの権限の割り当て」を参照）。

削除されたオブジェクトのリストを表示するには：

コンソールツリーで、［**削除されたオブジェクト**］を選択します（既定では、［**削除されたオブジェクト**］は［**詳細**］フォルダーのサブフォルダーとして含まれています）。

［**削除されたオブジェクト**］領域の権限で読み取り権限を付与されていない場合、［**削除されたオブジェクト**］フォルダーには空白のリストが表示されます。

［**削除されたオブジェクト**］フォルダーの作業領域では、削除されたオブジェクトに関する次の情報があります：

- **名前**：オブジェクトの名前
- **種別**：オブジェクトの種別（ポリシー、タスク、インストールパッケージなど）
- **日時**：オブジェクトが削除された日時

- **ユーザー**：オブジェクトを削除したユーザーのアカウント名

オブジェクトの詳細を表示するには：

1. コンソールツリーで、［**削除されたオブジェクト**］を選択します（既定では、［**削除されたオブジェクト**］は［**詳細**］フォルダーのサブフォルダーとして含まれています）。
2. ［**削除されたオブジェクト**］作業領域で、目的のオブジェクトを選択します。
   選択したオブジェクトに対する操作を実行できるボックスが作業領域の右側に表示されます。
3. 次のいずれかの手順を実行します：
   - 右側のボックス内で［**プロパティ**］をクリックする
   - 作業領域で選択したオブジェクトを右クリックし、コンテキストメニューから［**プロパティ**］を選択する

   オブジェクトのプロパティウィンドウが開き、次のタブが表示されます：
   - **全般**
   - **変更履歴**

削除されたオブジェクトのリストからオブジェクトを完全に削除する

［**削除されたオブジェクト**］領域の権限で**変更**権限を付与されたユーザーのみが、削除されたオブジェクトのリストからオブジェクトを完全に削除できます（詳しくは「ユーザーとグループへの権限の割り当て」を参照）。

削除されたオブジェクトのリストからオブジェクトを削除するには

1. コンソールツリーで、目的の管理サーバーのフォルダーを選択し、［**削除されたオブジェクト**］フォルダーを選択します。
2. 作業領域で、目的のオブジェクトを選択します。
3. 次のいずれかの手順を実行します：
   - **DELETE** キーを押します。
   - 選択したオブジェクトのコンテキストメニューで、［**削除**］を選択します。
4. 確認用のダイアログボックスで、［**はい**］をクリックします。

   オブジェクトが、削除されたオブジェクトのリストから完全に削除されます。このオブジェクトに関する情報（すべての履歴を含めて）がデータベースからすべて完全に削除されます。この情報を復元することはできません。

モバイルデバイス管理

Kaspersky Security Center からのモバイルデバイス保護の管理は、専用のライセンスを使用して利用できるモバイルデバイス管理機能を使用して行われます。自社の従業員が使用しているモバイルデバイスを管理する場合は、モバイルデバイス管理を有効にする必要があります。

このセクションでは、モバイルデバイス管理の有効化、設定、無効化を行う手順について説明します。また、管理サーバーに接続されたモバイルデバイスを管理する方法も確認できます。

Kaspersky Security for Mobile の詳細については、 *Kaspersky Security for Mobile のヘルプ*を参照してください。

シナリオ：モバイルデバイス管理の導入

このセクションでは、Kaspersky Security Center のモバイルデバイス管理機能を設定する手順を説明しています。

必須条件

モバイルデバイス管理機能の利用に必要なライセンスを保有していることを確認します。

実行するステップ

モバイルデバイス管理機能の導入は、以下の手順で進みます：

1. **ポートの準備**

   管理サーバーでポート 13292 が利用できることを確認します。このポートはモバイルデバイスへの接続で必要になります。また、必要に応じて、17100 も利用できるようにしておいた方がよい場合があります。このポートは、管理対象のモバイルデバイス用のアクティベーションプロキシサーバーを使用する場合にのみ必要となります。管理対象のモバイルデバイスがインターネットに接続できる場合、このポートを使用可能にする必要はありません。

2. **モバイルデバイス管理の有効化**

   管理サーバークイックスタートウィザードの実行中または以降の任意のタイミングで、モバイルデバイス管理を有効にできます。

3. **管理サーバーの外部アドレスの指定**

   管理サーバーのクイックスタートウィザードの実行中または以降の任意のタイミングで、外部アドレスを指定できます。インストール対象としてモバイルデバイス管理を選択しておらず、インストールウィザードでも外部アドレスを指定していない場合、インストールパッケージのプロパティで外部アドレスを指定します。

4. **管理対象デバイスグループへのモバイルデバイスの追加**

   モバイルデバイスを管理対象デバイスグループに追加し、ポリシーを使用して保護できるようにします。管理サーバーのクイックスタートウィザードに含まれる手順で、この設定を行えます。また、移動ルールを後で作成することもできます。こうしたルールを作成しない場合も、管理対象デバイスグループにモバイルデバイスを手動で追加できます。

   モバイルデバイスを管理対象デバイスグループに直接追加することも、1つ以上のサブグループを作成してそこにモバイルデバイスを追加することもできます。

   また、以降の任意のタイミングで、モバイルデバイスの接続ウィザードを使用して新しいモバイルデバイスを管理サーバーに接続できます。

5. **モバイルデバイス用のポリシーの作成**

   モバイルデバイスを管理するために、デバイスが属するグループでポリシーを作成します。作成したポリシーの設定は後からいつでも編集できます。

結果

これらの手順を完了すると、Kaspersky Security Center を使用して Android デバイスと iOS デバイスを管理できます。モバイルデバイスの証明書の操作や、モバイルデバイスへのコマンドの送信ができます。

iOS MDM デバイスを管理用グループポリシーについて

iOS MDM デバイスを管理するには、Kaspersky Device Management for iOS 管理プラグインを使用できます。これは Kaspersky Security Center のディストリビューションキットに含まれます。Kaspersky Device Management for iOS では、iPhone® 設定ユーティリティを使用せずに、iOS MDM デバイスの設定を指定するためのグループポリシーを作成できます。

iOS MDM デバイスの管理用グループポリシーによって、次の操作を実行できます。

- デバイスのパスワードのセキュリティ設定
- デバイスのハードウェア機能の使用を制限し、モバイルアプリのインストールと削除を制限する設定
- YouTube™、iTunes® Store、Safari など、事前にインストール済みのモバイルアプリの使用を制限する設定
- デバイスがある地域ごとにメディアコンテンツ（映画や TV 番組など）の表示を制限する設定
- プロキシサーバー（グローバル HTTP プロキシ）を使用してインターネットに接続するデバイスの設定
- ユーザーが企業アプリケーションや企業サービス（シングルサインオン技術）にアクセスできるアカウントの設定
- モバイルデバイスでのインターネット使用（Web サイトへのアクセス）の監視
- 異なる認証メカニズムとネットワークプロトコルを使用する無線ネットワーク（Wi-Fi）、アクセスポイント（APN）、および仮想プライベートネットワーク（VPN）の設定
- 写真、音楽、映像をストリーミングする AirPlay® デバイスへの接続の設定
- デバイスからドキュメントをワイヤレス印刷する AirPrint™ プリンターへの接続の設定
- デバイスで会社のメールを使用するためのユーザーアカウントと Microsoft Exchange サーバーを同期させる設定
- LDAP ディレクトリサービスと同期させるユーザー認証情報の設定
- ユーザーが会社のカレンダーや連絡先のリストにアクセスできるようになる、CalDAV および CardDAV サービスに接続するためのユーザー認証情報の設定
- ユーザーのデバイスでのお気に入り Web サイトのフォントやアイコンなど、iOS インターフェイスの設定
- デバイスでの新しいセキュリティ証明書の追加

- 認証局からデバイスで証明書を自動的に受領するための SCEP（Simple Certificate Enrollment Protocol）サーバーの設定
- モバイルアプリを操作するカスタム設定の追加

iOS MDM デバイスを管理するためのポリシーは、iOS MDM サーバー（「モバイルデバイスサーバー」と呼ばれる）を含む管理グループに割り当てられるという点が特徴です。このポリシーで指定されたすべての設定は、最初にモバイルデバイスサーバーに適用され、その後サーバーによって管理されるモバイルデバイスに適用されます。管理グループが階層構造を持つ場合は、セカンダリのモバイルデバイスサーバーがプライマリのモバイルデバイスサーバーからポリシー設定を受け取り、それらをモバイルデバイスに配信します。

Kaspersky Security Center 管理コンソールで iOS MDM デバイスの管理用グループポリシーを使用する方法についての詳細は、*Kaspersky Security for Mobile* のヘルプを参照してください。

モバイルデバイス管理の有効化

モバイルデバイスを管理するには、モバイルデバイス管理を有効にする必要があります。この機能をクイックスタートウィザードで有効にしなかった場合でも、後で有効にすることができます。モバイルデバイス管理を使用するにはライセンスが必要です。

モバイルデバイス管理の有効化は、プライマリ管理サーバーでのみ利用できます。

モバイルデバイス管理を有効にするには：

1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを開きます。
2. フォルダーの作業領域で［**モバイルデバイス管理を有効にする**］をクリックします。このボタンは、［**モバイルデバイス管理**］をオンにしていない場合に使用可能になります。

   管理サーバークイックスタートウィザードの［**追加コンポーネント**］ページが表示されます。
3. モバイルデバイスを管理するために、［**モバイルデバイス管理を有効にする**］を選択します。
4. ［**アプリケーションのアクティベーション方法の選択**］ウィンドウで、ライセンス情報ファイルまたはアクティベーションコードを使用してアプリケーションをアクティベートします。

   モバイルデバイスの管理は、モバイルデバイス管理機能をアクティベートしないと開始できません。
5. インターネットへの接続時にプロキシサーバーを使用する場合は、［**インターネットへのアクセス用のプロキシサーバー設定**］ウィンドウで［**プロキシサーバーを使用する**］をオンにします。このチェックボックスをオンにすると、設定を入力するフィールドが使用可能になります。プロキシサーバーの接続には、次の設定を行います：
6. ［**プラグインとインストールパッケージのアップデートを確認する**］ウィンドウで、次のいずれかのオプションをオンにします：
   - **プラグインとインストールパッケージが最新であるかどうか確認する**

     最新の状態かどうか確認を開始します。確認によって、一部のプラグインやインストールパッケージの古いバージョンが検出されると、最新バージョンをダウンロードして、古いバージョンを置き換えるように指示するメッセージが表示されます。
   - **確認しない**

プラグインとインストールパッケージが最新であるかどうかを確認せずに使用を続けます。たとえば、インターネットにアクセスできない場合や、何らかの理由で旧バージョンのアプリケーションを使用し続ける必要がある場合に、このオプションをオンにします。

プラグインのアップデートの確認を省略すると、アプリケーションが適切に動作しなくなる可能性があります。

7. ［**プラグインの利用可能な最新のバージョン**］ウィンドウで、適切な言語の最新バージョンのプラグインをダウンロードしてインストールしてください。プラグインを更新するには、ライセンスは必要ありません。

   プラグインとパッケージのインストール後、モバイルデバイスを正しく機能させるために必要なプラグインがすべてインストールされたかどうかが確認されます。古いバージョンのプラグインが検出されると、最新のバージョンをダウンロードして、古いバージョンを置き換えるように指示するメッセージが表示されます。

8. ［**モバイルデバイス接続設定**］ウィンドウで、管理サーバーのポートを設定します。

ウィザードが完了すると、次の変更が行われます。

- Kaspersky Endpoint Security for Android のポリシーが作成されます。
- Kaspersky Device Management for iOS のポリシーが作成されます。
- 管理サーバーでモバイルデバイス用のポートが開かれます。

モバイルデバイス管理設定の変更

モバイルデバイスのサポートを有効にするには：

1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを開きます。
2. フォルダーの作業領域で［**モバイルデバイス用接続ポート**］をクリックします。
   管理サーバーのプロパティウィンドウの［**追加のポート**］セクションが表示されます。
3. ［**追加のポート**］セクションで、関連する設定を変更します：
   - **アクティベーションプロキシサーバーの SSL ポート**
   - **モバイルデバイス用ポートを開く**

     モバイルデバイスをライセンス管理サーバーに接続するためのポートを開きます。その下のフィールドでポート番号とその他の設定を定義できます。

     既定では、このオプションはオンです。

   - **モバイルデバイスとの同期用のポート**

モバイルデバイスが管理サーバーに接続し、管理サーバーとデータをやり取りするために経由するポートの番号です。既定のポート番号は 13292 です。

ポート 13292 が他の目的で使用されている場合は、別のポートを割り当てることができます。

- **モバイルデバイスのアクティベーション用のポート**

  Kaspersky Endpoint Security for Android をカスペルスキーのアクティベーションサーバーに接続するポートです。

  既定のポート番号は 17100 です。

4. ［**OK**］をクリックします。

モバイルデバイス管理の無効化

モバイルデバイス管理の無効化は、プライマリ管理サーバーでのみ利用できます。

モバイルデバイス管理を無効にするには：

1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを開きます。
2. フォルダーの作業領域で［**追加コンポーネントの設定**］をクリックします。
   管理サーバークイックスタートウィザードの［**追加コンポーネント**］ページが表示されます。
3. モバイルデバイスの管理が不要な場合は、［**モバイルデバイス管理を有効にしない**］を選択します。
4. ［**OK**］をクリックします。

以前接続していたモバイルデバイスは管理サーバーに接続できなくなります。モバイルデバイス接続用のポートとモバイルデバイスアクティベーション用のポートは自動的に閉じられます。

Kaspersky Endpoint Security for Android および Kaspersky Device Management for iOS のために作成されたポリシーは削除されません。証明書の発行ルールは変更されません。インストールされているプラグインは削除されません。モバイルデバイス移動ルールも削除されません。

管理対象モバイルデバイスでのモバイルデバイス管理を再度有効化した後、モバイルデバイス管理に必要なモバイルアプリを再インストールする必要がある場合もあります。

モバイルデバイスのコマンドの使用

このセクションでは、Kaspersky Security Center でサポートされるモバイルデバイスを管理するためのコマンドについて説明します。また、モバイルデバイスにコマンドを送信する方法と、コマンドタグにおけるコマンドの実行ステータスを表示する方法について説明します。

モバイルデバイス管理のコマンド

Kaspersky Security Center では、モバイルデバイス管理用のコマンドがサポートされています。

このコマンドは、モバイルデバイスのリモート管理に使用されます。たとえば、ユーザーのモバイルデバイスの紛失時に、コマンドを使用して、デバイスから企業データを削除できます。

次の種別の管理対象モバイルデバイスに対してコマンドを使用できます：

- iOS MDM デバイス
- Kaspersky Endpoint Security（KES）デバイス

デバイスの各種別は、コマンドの専用セットをサポートします。

特定のコマンドに関する特別な考慮事項

- すべてのデバイス種別において、［**工場出荷状態にリセットする**］コマンドが問題なく実行された場合、すべてのデータはデバイスから消去され、デバイスの設定は工場出荷時の値に戻ります。
- iOS MDM デバイスで［**企業データ消去**］コマンドが問題なく実行されると、インストール済みのすべての設定プロファイル、プロビジョニングプロファイル、iOS MDM プロファイル、および［**iOS MDM プロファイルと一緒に削除する**］がオンになっているアプリケーションがデバイスから削除されます。
- ［**企業データ消去**］コマンドが KES デバイスでされると、すべての企業データ、連絡先、SMS 履歴、通話記録、カレンダー、インターネット接続設定、ユーザーのアカウントが、デバイスから削除されます（Google™ アカウントを除く）。KES デバイスでは、メモリカードのデータもすべて消去されます。
- ［**GPS 追跡**］コマンドを KES デバイスに送信する前に、このコマンドの使用目的は、組織または従業員の一人が所有する紛失したデバイスの捜索であり、その捜索が承認されていることを確認する必要があります。［**GPS 追跡**］コマンドを受信したモバイルデバイスはロックされません。

モバイルデバイス用のコマンドのリスト

次の表では、iOS MDM デバイス種別のコマンドセットを示しています。

サポートされるモバイルデバイス管理コマンド：iOS MDM デバイス

コマンド	コマンドの実行結果
ロック	モバイルデバイスがロックされます。
ロック解除	PIN を使用したモバイルデバイスのロックが無効になります。以前に指定した PIN はリセットされます。
工場出荷状態にリセットする	すべてのデータがモバイルデバイスから消去され、設定が既定値に戻ります。
企業データ消去	インストール済みのすべての設定プロファイル、プロビジョニングプロファイル、iOS MDM プロファイル、および［**iOS MDM プロファイルと一緒に削除する**］がオンになっているアプリケーションが、デバイスから削除されます。
デバイスの同期	モバイルデバイスのデータが管理サーバーと同期します。
プロファイルのインストール	設定プロファイルがモバイルデバイスにインストールされます。
プロファイルの削除	設定プロファイルがモバイルデバイスから削除されます。
プロビジョニングプロファイルのインス	プロビジョニングプロファイルがモバイルデバイスにインストールされます。

トール	
プロビジョニングプロファイルの削除	プロビジョニングプロファイルがモバイルデバイスから削除されます。
アプリのインストール	アプリがモバイルデバイスにインストールされます。
アプリの削除	アプリがモバイルデバイスから削除されます。
リデンプションコードの入力	リデンプションコードが有償アプリに入力されます。
ローミングの設定	データローミングおよび音声ローミングが有効または無効になります。

次の表では、KES デバイスのコマンドセットを示しています。

サポートされるモバイルデバイス管理コマンド：KES デバイス

コマンド	コマンドの実行結果
ロック	モバイルデバイスがロックされます。
ロック解除	PIN を使用したモバイルデバイスのロックが無効になります。以前に指定した PIN はリセットされます。
工場出荷状態にリセットする	すべてのデータがモバイルデバイスから消去され、設定が既定値に戻ります。
企業データ消去	企業データ、連絡先のエントリ、SMS 履歴、通話記録、カレンダー、インターネット接続設定、ユーザーのアカウント（Google アカウントを除く）が削除されます。メモリカードのデータが消去されます。
デバイスの同期	モバイルデバイスのデータが管理サーバーと同期します。
GPS 追跡	モバイルデバイスを GPS 追跡し、Google マップ™ で表示します。SMS メッセージの送付とインターネット接続には、モバイル通信業者の料金請求が発生します。
遠隔撮影	モバイルデバイスがロックされます。写真をデバイスのフロントカメラで撮影し、管理サーバーに保存します。写真はコマンドログに表示できます。SMS メッセージの送付とインターネット接続には、モバイル通信業者の料金請求が発生します。
遠隔アラーム	モバイルデバイスでアラームが鳴ります。

Firebase Cloud Messaging の使用

Android オペレーティングシステムが管理する KES デバイスにコマンドがタイミングよく確実に配信されるようにするため、Kaspersky Security Center ではプッシュ通知のメカニズムが使用されます。プッシュ通知は、Firebase Cloud Messaging（以下、FCM）を介して KES デバイスと管理サーバー間で交換されます。Kaspersky Security Center 管理コンソールで、Firebase Cloud Messaging サービスの設定を指定することで、サービスに KES デバイスを接続できます。

Firebase Cloud Messaging の設定を取得するには、Google アカウントが必要です。

FCM の使用を有効化するには：

1. 管理コンソールで、［**モバイルデバイス管理**］フォルダー、および［**モバイルデバイス**］フォルダーを選択します。
2. ［**モバイルデバイス**］フォルダーのコンテキストメニューで、［**プロパティ**］を選択します。
3. フォルダーのプロパティで、［**Firebase Cloud Messaging の設定**］セクションを選択します。
4. ［**Firebase プロジェクト番号**］フィールドに、FCM 送信者 ID を指定します。
5. ［**秘密鍵ファイル（JSON 形式）**］フィールドで、秘密鍵ファイルを選択します。

管理サーバーとの次回の同期時に、Android オペレーティングシステムが管理する KES デバイスが、Firebase Cloud Messaging に接続されます。

Firebase Cloud Messaging の設定は、［**設定をリセット**］をクリックして編集できます。

コマンドの送信

ユーザーのモバイルデバイスにコマンドを送信するには：

1. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。
   フォルダーの作業領域には、管理対象のモバイルデバイスのリストが表示されます。
2. コマンドを送信する必要があるモバイルデバイスを選択します。
3. モバイルデバイスのコンテキストメニューから、［**コマンドログの表示**］を選択します。
4. ［**モバイルデバイスの管理コマンド**］ウィンドウで、モバイルデバイスに送信する必要があるコマンドの名前を使用して、セクションを進めます。その後、［**コマンドを送信する**］をクリックします。
   選択したコマンドによっては、［**コマンドを送信する**］をクリックすると詳細設定のウィンドウを開けてしまう可能性があります。たとえば、モバイルデバイスからプロビジョニングプロファイルを削除するためにコマンドを送信する場合、モバイルデバイスから削除すべきプロビジョニングプロファイルを選択するよう促されます。そのウィンドウでコマンドの詳細設定を定義し、選択を確認します。その後、コマンドはモバイルデバイスに送信されます。
   ［**再送信**］をクリックして、コマンドをモバイルデバイスに再度送信できます。
   送信したコマンドがまだ実行されていない場合は、［**キューから削除**］をクリックしてそのコマンドの実行をキャンセルできます。
   ［**コマンドログ**］セクションには、個別の実行ステータスも合わせて、モバイルデバイスに送信されているコマンドが表示されます。［**更新**］をクリックすると、コマンドのリストが更新されます。
5. ［OK］をクリックすると、［**モバイルデバイスの管理コマンド**］ウィンドウが閉じられます。

コマンドログでのコマンドのステータスの表示

モバイルデバイスに送信されているすべてのコマンドに関する情報がコマンドログに保存されます。コマンドログには、各コマンドがモバイルデバイスに送信された日時、それぞれのステータス、およびコマンドの実行結果の詳細に関する情報が記録されます。たとえば、コマンドの実行に失敗した場合、コマンドログにはエラーの原因が表示されます。レコードは、コマンドログに最大で 30 日間保存されます。

モバイルデバイスに送信されたコマンドのステータスは次の通りです：

- *実行中* - コマンドがモバイルデバイスに送信されました。
- *完了* - コマンドの実行が問題なく完了しました。
- *エラー終了* - コマンドの実行に失敗しました。
- *削除中* - モバイルデバイスに送信されたコマンドのキューからコマンドを削除しています。
- *削除済み* - モバイルデバイスに送信されたコマンドがコマンドキューから正常に削除されました。

- *削除エラー*- モバイルデバイスに送信されたコマンドをコマンドキューから削除できませんでした。

モバイルデバイスごとに、コマンドログが管理されます。

モバイルデバイスに送信されたコマンドのログを表示するには：

1. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。
   フォルダーの作業領域には、管理対象のモバイルデバイスのリストが表示されます。
2. モバイルデバイスのリストで、コマンドログを表示したいものを1つ選択します。
3. モバイルデバイスのコンテキストメニューから、［**コマンドログの表示**］を選択します。
   ［**モバイルデバイス管理コマンド**］ウィンドウが表示されます。［**モバイルデバイス管理のコマンド**］ウィンドウのセクションは、モバイルデバイスに送信可能なコマンドに対応しています。
4. ［**コマンドログ**］セクションで、必要なコマンドが含まれるセクションを選択し、それらのコマンドが送信および実行される方法に関する情報を表示します。

［**コマンドログ**］セクションでは、モバイルデバイスに送信したコマンドのリストとそれらコマンドの詳細を表示できます。［**コマンドの表示**］フィルターにより、選択したステータスのコマンドのみのリストを表示できます。

モバイルデバイスの証明書の使用

このセクションでは、モバイルデバイスの証明書の使用方法について説明します。

モバイルデバイスのルート証明書の有効期限は、生成後700日に固定されています。準備証明書は有効期限の60日前に生成されます。次のコマンドを使用して、予備証明書を生成する期間を変更できます。

`klscflag.exe -fset -pv klserver -n KLSRV_AKLWNGT_MDM_CERT_CHANGE_TIMEOUT -t d -v <`頻度の値（秒）`>`

予備証明書を生成する期間は、管理対象のすべてのモバイルデバイスが管理サーバーと同期して証明書を取得するのに十分な長さである必要があります。

klscflagユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

モバイルデバイスのルート証明書の手動更新はサポートされていません。

証明書インストールウィザードの開始

ユーザーのモバイルデバイスには、次の種別の証明書をインストールできます：

- モバイルデバイスを識別するための共有証明書
- モバイルデバイスで企業メールを設定するためのメール証明書
- モバイルデバイスの仮想プライベートネットワークへのアクセスを設定するためのVPN証明書

ユーザーのモバイルデバイスに証明書をインストールするには：

1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを展開し、［**証明書**］サブフォルダーを選択します。

2. ［**証明書**］フォルダーの作業領域で、［**証明書の追加**］をクリックして証明書インストールウィザードを実行します。

ウィザードの指示に従ってください。

ウィザードが終了すると、証明書が作成されてユーザーの証明書リストに追加されます。さらに、ユーザーに通知が送信され、モバイルデバイスで証明書をダウンロードおよびインストールするためのリンクが提供されます。すべての証明書のリストを表示し、ファイルにエクスポートできます。証明書を削除および再発行するとともに、そのプロパティを表示することができます。

ステップ 1：証明書の種別の選択

ユーザーのモバイルデバイスにインストールする証明書の種別を指定します。

- **モバイル証明書** - モバイルデバイスの識別用
- **メール証明書** - モバイルデバイスでの企業メールの設定用
- **VPN 証明書** - モバイルデバイスの仮想プライベートネットワークへのアクセスの設定用

ステップ 2：デバイス種別の選択

このウィンドウは、証明書の種別で［**メール証明書**］または［**VPN 証明書**］を選択した場合に表示されます。

デバイスのオペレーティングシステムの種別を指定します：

- **iOS MDM デバイス**：iOS MDM プロトコルを使用して iOS MDM サーバーに接続しているモバイルデバイスに証明書をインストールする場合、このオプションを選択します。
- **Kaspersky Security for Mobile により管理される KES デバイス**：KES デバイスに証明書をインストールする必要がある場合にこのオプションを選択します。この場合、管理サーバーに接続するたびに、証明書を使用してユーザーが識別されます。
- **ユーザー証明書の認証なしで管理サーバーに接続された KES デバイス**：証明書による認証を使用しない KES デバイスに証明書をインストールする場合、このオプションを選択します。この場合、ウィザードの最終ステップの［**ユーザー通知方法**］ウィンドウで、管理サーバーに接続するたびに使用されるユーザー認証の種別を選択する必要があります。

ステップ 3：ユーザーの選択

リストから、証明書をインストールするユーザー、セキュリティグループ、Active Directory セキュリティグループを選択します。

［**ユーザーの選択**］ウィンドウで、Kaspersky Security Center の内部ユーザーを検索できます。［**追加**］をクリックすると、内部ユーザーを追加できます。

ステップ 4：証明書の配信元の選択

このウィンドウでは、管理サーバーがモバイルデバイスの認証に使用する証明書の発行元を選択できます。次のいずれかの方法で、証明書を選択します：

- 管理サーバーツールを使用して自動で証明書を作成した後、デバイスに配信します。
- 以前に作成した証明書ファイルを指定します。この方法は、前のステップで複数のユーザーを選択した場合には使用できません。

証明書の作成に関する通知をユーザーのモバイルデバイスに送信する必要がある場合、［**証明書の発行**］をオンにします。

ユーザーのモバイルデバイスが証明書より認証済みで、新規証明書の取得にアカウント名とパスワードが不要な場合、［**証明書の発行**］をオフにします。この場合、［**ユーザー通知方法**］ウィンドウは表示されません。

ステップ 5：証明書へのタグの割り当て

［**デバイス種別**］で「**iOS MDM デバイス**」が選択されている場合、［**証明書タグ**］ウィンドウが表示されます。

ドロップダウンリストから、ユーザーの iOS MDM デバイスの証明書にタグを割り当てることができます。たとえば、Kaspersky Device Management for iOS ポリシーのプロパティで設定された特定のパラメータをタグに対応させ、そのタグを証明書に割り当てることができます。

ドロップダウンリストでは、「*証明書テンプレート 1*」「*証明書テンプレート 2*」「*証明書テンプレート 3*」のいずれかのタグを選択できます。これらのタグを設定する方法は、以下のセクションで説明します：

- ［**証明書の種別**］ウィンドウで「**メール証明書**」が選択されている場合、証明書のタグは、モバイルデバイスの Exchange ActiveSync アカウントのプロパティで設定できます（［**管理対象デバイス**］→［**ポリシー**］→ Kaspersky Device Management for iOS ポリシーのプロパティ →［**Exchange ActiveSync**］セクション →［**追加**］→［**詳細**］）。
- ［**証明書の種別**］ウィンドウで「**VPN 証明書**」が選択されている場合、証明書のタグは、モバイルデバイスの VPN のプロパティで設定できます（［**管理対象デバイス**］→［**ポリシー**］→ Kaspersky Device Management for iOS ポリシーのプロパティ →［**VPN**］セクション →［**追加**］→［**詳細**］）。VPN で L2TP、PPTP、IPSec（Cisco™）のいずれかの接続種別が選択されている場合、VPN 証明書に使用するタグは設定できません。

ステップ 6：証明書発行設定の指定

このウィンドウでは、次の証明書発行設定を指定できます：

- **新しい証明書をユーザーに通知しない**

ユーザーのモバイルデバイス用の証明書の作成に関する通知をユーザーに送信しない場合は、このオプションをオンにします。この場合、［**ユーザー通知方法**］ウィンドウは表示されません。

このオプションは、Kaspersky Endpoint Security for Android をインストールしているデバイスにのみ適用されます。

たとえば、ユーザーのモバイルデバイスが既に証明書によって認証されており、新規証明書の取得にアカウント名とパスワードが必要ない場合、このオプションをオンにすることを検討できます。

- **単一の証明書を複数回デバイスが受信することを許可する (Kaspersky Endpoint Security for Android がインストールされたデバイスのみ)**

  証明書の有効期限がもうすぐ切れる時、または対象のデバイスで証明書が見つからない時、Kaspersky Security Center で証明書を自動的に再送する場合はこのオプションをオンにします。

  証明書の有効期限の数日前に証明書が自動的に再送されます。事前送付の具体的な日数は、［証明書発行ルール］ウィンドウで指定できます。

  デバイス上で証明書が見つからない場合があります。たとえば、ユーザーがカスペルスキーのセキュリティ製品をデバイスに再インストールしていたり、デバイスの設定とデータを工場出荷時の設定にリセットしている場合です。この場合、デバイスが管理サーバーへの接続を次に試行したタイミングで、Kaspersky Security Center はデバイス ID を確認します。デバイス ID が、証明書発行当時と同じ場合、デバイスに証明書が再送されます。

ステップ 7：ユーザー通知方法の選択

デバイス種別として［**iOS MDM デバイス**］を選択している場合、あるいは［**新しい証明書をユーザーに通知しない**］をオンにしている場合は、このウィンドウは表示されません。

［**ユーザー通知方法**］ウィンドウでは、モバイルデバイスへの証明書のインストールをユーザーに通知する方法を設定できます。

［**認証方法**］で、ユーザー認証の種別を指定します：

- **資格情報（ドメインまたはエイリアス）**

  この場合、ユーザーはドメインパスワードまたは Kaspersky Security Center 内部ユーザーのパスワードを使用して、新しい証明書を取得します。

- **ワンタイムパスワード**

  この場合、ユーザーはメールまたは SMS で送信されるワンタイムパスワードを受信します。新しい証明書を取得するには、このパスワードを入力する必要があります。

  ［**証明書発行設定**］ウィンドウで、［**デバイスが証明書を複数回受信することを許可する（モバイルデバイス向けカスペルスキー製品がインストールされたデバイスのみ）**］をオンにしている場合、オプションは［**パスワード**］に変化します。

- **パスワード**

  この場合、証明書がユーザーに送信されるたびに同じパスワードが使用されます。

  ［**証明書発行設定**］ウィンドウで、［**デバイスが証明書を複数回受信することを許可する（モバイルデバイス向けカスペルスキー製品がインストールされたデバイスのみ）**］をオフにしている場合、オプションは［**ワンタイムパスワード**］に変化します。

このフィールドは、［**証明書の種別**］ウィンドウで［**モバイル証明書**］を選択している場合、またはデバイスの種別として［**ユーザー証明書の認証なしで管理サーバーに接続された KES デバイス**］を選択している場合に表示されます。

ユーザー通知のオプションを選択します：

- **ウィザードの終了後に認証パスワードを表示する**

  このオプションをオンにすると、証明書インストールウィザードの最終ステップで、選択した各ユーザーに対して、ユーザー名、セキュリティアカウントマネージャー内のユーザー名、証明書を回復するためのパスワードが表示されます。インストールされた証明書についてのユーザー通知が設定できなくなります。

  複数のユーザーに証明書を追加する場合、証明書インストールウィザードの最終ステップで［**エクスポート**］をクリックすると、提供された認証情報をファイルに保存できます。

  証明書インストールウィザードの［**ユーザー通知方法**］で［**資格情報（ドメインまたはエイリアス）**］を選択した場合、このオプションは使用できません。

- **新しい証明書をユーザーに通知**

  このオプションをオンにすると、新しい証明書についてのユーザー通知を設定できます。

  - **メール**

    このセクションで、新規証明書をユーザーのモバイルデバイスへインストールしたことをメールで伝えるユーザー通知を設定できます。この通知方法は、SMTP サーバーが有効な場合のみ使用できます。

    必要に応じて、［**メッセージの編集**］をクリックし、通知メッセージを表示して編集します。

  - **SMS 経由**

    このセクションで、証明書をユーザーのモバイルデバイスへインストールしたことを SMS で伝えるユーザー通知を設定できます。この通知方法は、SMS 通知が有効な場合のみ使用できます。

    必要に応じて、［**メッセージの編集**］をクリックし、通知メッセージを表示して編集します。

ステップ 8：証明書の生成中

このステップでは証明書が作成されます。

［**終了**］をクリックすると、ウィザードを終了できます。

証明書が生成され、［**証明書**］フォルダーの作業領域の証明書のリストに表示されます。

証明書の作成設定の指定

証明書は、管理サーバーによるデバイスの認証に使用されます。すべての管理対象モバイルデバイスには証明書を発行する必要があります。証明書の発行方法を設定できます。

証明書の発行ルールを設定するには：

1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを展開し、［**証明書**］サブフォルダーを選択します。
2. ［**証明書**］フォルダーの作業領域で［**証明書の発行ルールを指定する**］をクリックし、［**証明書発行ルール**］を開きます。
3. 証明書の種別名のセクションに進みます：

   モバイル証明書の発行 - モバイル証明書の発行方法を設定します。

   メール証明書の発行 - メール証明書の発行方法を設定します。

   VPN 証明書の発行 - VPN 証明書の発行方法を設定します。
4. ［**発行の設定**］セクションで、証明書の発行方法を設定します：
   - 証明書の有効期間を日単位で指定します。

     モバイルデバイスの証明書は、ルート証明書の有効期限によって制限されます。ルート証明書の有効期限よりも長い証明書の有効期間を指定した場合、証明書の有効期間は生成時に自動的に調整されます。
   - 証明書のソースを選択します（［**管理サーバー**］または［**証明書を手動で指定**］）。

     管理サーバーが証明書の既定のソースとして選択されます。
   - 証明書のテンプレートを指定します（［**既定のテンプレート**］または［**他のテンプレート**］）。

     ［**PKI（公開鍵基盤）の統合**］セクションで、公開鍵基盤との統合を有効にしている場合、テンプレートの設定が利用可能です。
5. ［**自動更新設定**］セクションで、証明書の自動アップデートを設定します：
   - ［**証明書の有効期間の残りが次の日数になったら更新**］で、証明書を更新する必要がある有効期限までの日数を指定します。
   - 証明書の自動更新を有効にするには、［**可能であれば証明書を自動で再発行**］をオンにします。
6. ［**パスワードによる保護**］セクションで、証明書の復号化時のパスワードの使用を設定して有効にします。

   > パスワードによる保護は、モバイル証明書の場合にのみ使用できます。

   a. ［**証明書のインストール時にパスワードを要求する**］をオンにします。

   b. スライダーを使用して、暗号化用パスワードに使う文字数の上限を定義します。

7. ［**OK**］をクリックします。

公開鍵基盤との統合

公開鍵基盤（PKI）との製品の統合は、ユーザーへのドメイン証明書の発行を簡略化するために必要とされます。統合後、証明書が自動的に発行されます。

サポートされる PKI サーバーの最小バージョンは Windows Server 2008 です。

PKI（公開鍵基盤）を統合するアカウントを設定する必要があります。アカウントは次の要件を満たしている必要があります：

- 管理サーバーがインストールされているデバイスのドメインユーザーおよび管理者であること
- 管理サーバーがインストールされているデバイスで SeServiceLogonRight 権限が与えられていること

永続的なユーザープロファイルを作成するには、管理サーバーがインストールされているデバイスに、設定されたアカウントで少なくとも 1 回ログオンします。管理サーバーデバイスのこのユーザーの証明書リポジトリに、ドメイン管理者によって提供される登録エージェント証明書をインストールします。

公開鍵基盤との統合を設定するには：

1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを展開し、［**証明書**］サブフォルダーを選択します。
2. 作業領域で、［**公開鍵基盤と統合する**］をクリックして、［**証明書発行ルール**］ウィンドウの［**PKI（公開鍵基盤）の統合**］セクションを開きます。
   ［**証明書発行ルール**］ウィンドウの［**PKI（公開鍵基盤）の統合**］セクションが開きます。
3. ［**PKI（公開鍵基盤）と証明書の発行を統合する**］をオンにします。
4. ［**アカウント**］で、PKI の統合に使用されるユーザーアカウントの名前を指定します。
5. ［**パスワード**］にアカウントのドメインパスワードを入力します。
6. ［**PKI システムの証明書のテンプレート名**］リストで、ドメインユーザーへの証明書発行で使用される証明書テンプレートを選択します。
   専用のサービスが、指定されたユーザーアカウントで開始されます。このサービスでは、ユーザーのドメイン証明書の発行を担当します。［**リストの更新**］をクリックすることで証明書のテンプレートのリストが読み込まれる際、または証明書が生成される際に、サービスが実行されます。
7. ［**OK**］をクリックして設定を保存します。

統合後、証明書が自動的に発行されます。

Kerberos の制約付き委任のサポートを有効化

Kerberos の制約付き委任の使用がサポートされます。

Kerberos の制約付き委任のサポートを有効にするには：

1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを開きます。
2. コンソールツリーの［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイスサーバー**］サブフォルダーを選択します。
3. ［**モバイルデバイスサーバー**］フォルダーの作業領域で、iOS MDM サーバーを選択します。
4. iOS MDM サーバーのコンテキストメニューで、［**プロパティ**］を選択します。
5. iOS MDM サーバーのプロパティウィンドウで［**設定**］セクションを選択します。
6. ［**設定**］セクションで、［**Kerberos の制約付き委任との互換性を確保する**］をオンにします。
7. ［**OK**］をクリックします。

管理対象デバイスのリストへの iOS モバイルデバイスの追加

ユーザーの iOS モバイルデバイスを管理対象デバイスのリストに追加するには、共有証明書をデバイスに配信してインストールする必要があります。共有証明書は、モバイルデバイスを識別するために管理サーバーで使用されます。iOS モバイルデバイス用の共有証明書は iOS MDM プロファイルに含まれるかたちで配信されます。共有証明書がモバイルデバイスに配信されてインストールされると、管理対象デバイスのリストにそのモバイルデバイスが表示されます。

Kaspersky Safe Browser のサポートは終了しました。

ユーザーのモバイルデバイスを、モバイルデバイスの接続ウィザードを使用して管理対象デバイスのリストに追加できます。

iOS デバイスを共有証明書を使用して管理サーバーに接続するには：

1. 次のいずれかの方法でモバイルデバイスの接続ウィザードを起動します：
   - ［**ユーザーアカウント**］フォルダーのコンテキストメニューを使用する：
     1. コンソールツリーで、［**詳細**］フォルダーを展開し、［**ユーザーアカウント**］サブフォルダーを選択します。
     2. ［**ユーザーアカウント**］フォルダーの作業領域で、管理対象デバイスのリストに追加するモバイルデバイスを所有しているユーザー、セキュリティグループ、または Active Directory セキュリティグループを選択します。
     3. ユーザーアカウントを右クリックし、コンテキストメニューで［**モバイルデバイスの追加**］を選択します。

        モバイルデバイスの接続ウィザードが起動します。
   - ［**モバイルデバイス**］フォルダーの作業領域で［**モバイルデバイスの追加**］をクリックします。
     1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを展開し、［**モバイルデバイス**］サブフォルダーを選択します。
     2. ［**モバイルデバイス**］サブフォルダーの作業領域で［**モバイルデバイスの追加**］をクリックします。

        モバイルデバイスの接続ウィザードが起動します。

2. ウィザードの［**オペレーティングシステム**］ウィンドウで、モバイルデバイスのオペレーティングシステム種別として［**iOS**］を選択します。

3. ウィザードの［**iOS MDM サーバーの選択**］ウィンドウで、iOS MDM サーバーを選択します。

4. ［**管理対象のモバイルデバイスを所有しているユーザーを選択してください**］ウィンドウで、管理対象デバイスのリストに追加するモバイルデバイスを所有しているユーザー、セキュリティグループ、または Active Directory セキュリティグループを選択します。

   ［**ユーザーアカウント**］フォルダーのコンテキストメニューで［**モバイルデバイスの追加**］を選択してウィザードを開始した場合、この手順はスキップされます。

   新しいユーザーアカウントをリストに追加するには、［**追加**］をクリックして表示されるウィンドウで、ユーザーアカウントの情報を入力します。既存のユーザーアカウントの情報を変更したり確認するには、リストからユーザーアカウントを選択し［**プロパティ**］をクリックします。

5. ウィザードの［**証明書ソース**］ウィンドウで、管理サーバーがモバイルデバイスの識別に使用する共有証明書の作成方法を指定します。次のいずれかの方法で、共有証明書を指定できます：

   - **管理サーバーツール経由で証明書を発行する**

     以前に証明書を作成していない場合は、管理サーバーのツールを使用して新しい証明書を作成するためにこのオプションを選択してください。

     このオプションをオンにすると、管理サーバーによって自動的に生成された証明書で iOS MDM プロファイルが署名されます。

     既定ではこのオプションが選択されます。

   - **証明書ファイルを指定する**

     以前に作成した証明書ファイルを指定する場合は、このオプションを選択します。

     この方法は、前のステップで複数のユーザーを選択した場合には使用できません。

6. ウィザードの［**ユーザー通知方法**］ページで、証明書の作成に関する SMS またはメールによってモバイルデバイスユーザーに通知する場合の設定を定義します。

   - **ウィザード内で QR コードを表示**

     このオプションをオンにすると、モバイルデバイスの接続ウィザードの最後の手順で、インストールパッケージへのリンクが表示されます。

     このオプションは、デバイスを選択するユーザーを複数選択した場合には使用できません。

   - **QR コードをユーザーに送信**

このオプションをオンにすると、新しいモバイルデバイスが接続された時のユーザー通知を設定できます。

メールアドレスの種別の選択、追加のメールアドレスの指定、メッセージ本文の編集が可能です。SMS メッセージを送信するユーザー端末の種別の選択、追加の電話番号の指定、SMS メッセージの本文の編集も可能です。

SMTP サーバーが設定されていない場合、ユーザーへのメールは送信されません。SMS 通知が設定されていない場合、ユーザーへの SMS は送信されません。

7. ［**結果**］ページで、［**完了**］をクリックして、証明書インストールウィザードを閉じます。

iOS MDM プロファイルが Kaspersky Security Center Web サーバーで自動的に公開されます。モバイルデバイスのユーザーが、Web サーバーから iOS MDM プロファイルをダウンロードするためのリンクが記載された通知を受信します。ユーザーが、リンクをクリックします。モバイルデバイスのオペレーティングシステムが、iOS MDM プロファイルのインストールに同意するようユーザーに要求します。ユーザーは、iOS MDM プロファイルをモバイルデバイスにダウンロードできるようにするため、まず iOS MDM プロファイルのインストールに同意する必要があります。iOS MDM プロファイルがダウンロードされ、モバイルデバイスが管理サーバーと同期されると、そのデバイスが、コンソールツリーの［**モバイルデバイス管理**］フォルダーにある［**モバイルデバイス**］フォルダーに表示されます。

ユーザーがリンクを使用して Kaspersky Security Center Web サーバーに移動するには、モバイルデバイスでポート 8061 経由での管理サーバーとの接続が確立されている必要があります。

管理対象デバイスのリストへの Android モバイルデバイスの追加

ユーザーの Android モバイルデバイスを管理対象デバイスのリストに追加するには、Kaspersky Endpoint Security for Android と共有証明書をデバイスに配信してインストールする必要があります。共有証明書は、モバイルデバイスを識別するために管理サーバーで使用されます。共有証明書がモバイルデバイスに配信されてインストールされると、管理対象デバイスのリストにそのモバイルデバイスが表示されます。

ユーザーのモバイルデバイスを、モバイルデバイスの接続ウィザードを使用して管理対象デバイスのリストに追加できます。ウィザードでは、次の 2 つの方法のいずれかで、共有証明書と Kaspersky Endpoint Security for Android の配信およびインストールを実行できます：

- Google Play のリンクを使用
- Kaspersky Security Center Web サーバーのリンクを使用

  管理サーバーで配布用に保存されている Kaspersky Endpoint Security for Android のインストールパッケージをインストールに使用します。

モバイルデバイスの接続ウィザードの起動

次のいずれかの方法でモバイルデバイスの接続ウィザードを起動します：

- ［**ユーザーアカウント**］フォルダーのコンテキストメニューを使用する：

  1. コンソールツリーで、［**詳細**］フォルダーを展開し、［**ユーザーアカウント**］サブフォルダーを選択します。

2. ［**ユーザーアカウント**］フォルダーの作業領域で、管理対象デバイスのリストに追加するモバイルデバイスを所有しているユーザー、セキュリティグループ、または Active Directory セキュリティグループを選択します。

3. ユーザーアカウントを右クリックし、コンテキストメニューで［**モバイルデバイスの追加**］を選択します。

   モバイルデバイスの接続ウィザードが起動します。

- ［**モバイルデバイス**］フォルダーの作業領域で［**モバイルデバイスの追加**］をクリックします。

  1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを展開し、［**モバイルデバイス**］サブフォルダーを選択します。

  2. ［**モバイルデバイス**］サブフォルダーの作業領域で［**モバイルデバイスの追加**］をクリックします。

     モバイルデバイスの接続ウィザードが起動します。

Google Play のリンクを使用しての Android モバイルデバイスの追加

Google Play のリンクを使用して Kaspersky Endpoint Security for Android と共有証明書をモバイルデバイスにインストールするには：

1. モバイルデバイスの接続ウィザードを起動します。

2. ウィザードの［**オペレーティングシステム**］ページで、モバイルデバイスのオペレーティングシステム種別として［**Android**］を選択します。

3. ウィザードの［**デバイスに Kaspersky Endpoint Security for Android をインストールする方法**］ページで、［**Google Play からアプリをダウンロード**］を選択します。

4. ウィザードの［**管理対象のモバイルデバイスを所有しているユーザーを選択してください**］ページで、管理対象デバイスのリストに追加するモバイルデバイスを所有しているユーザー、セキュリティグループ、または Active Directory セキュリティグループを選択します。

   ［**ユーザーアカウント**］フォルダーのコンテキストメニューで［**モバイルデバイスの追加**］を選択してウィザードを開始した場合、この手順はスキップされます。

   新しいユーザーアカウントをリストに追加するには、［**追加**］をクリックして表示されるウィンドウで、ユーザーアカウントの情報を入力します。既存のユーザーアカウントの情報を変更したり確認するには、リストからユーザーアカウントを選択し［**プロパティ**］をクリックします。

5. ウィザードの［**証明書ソース**］ウィンドウで、管理サーバーがモバイルデバイスの識別に使用する共有証明書の作成方法を指定します。次のいずれかの方法で、共有証明書を指定できます：

   - **管理サーバーツール経由で証明書を発行する**

     以前に証明書を作成していない場合は、管理サーバーのツールを使用して新しい証明書を作成するためにこのオプションを選択してください。

     このオプションをオンにすると、管理サーバーのツールを使用して証明書が自動的に発行されます。

     既定ではこのオプションが選択されます。

   - **証明書ファイルを指定する**

以前に作成した証明書ファイルを指定する場合は、このオプションを選択します。
この方法は、前のステップで複数のユーザーを選択した場合には使用できません。

6. ウィザードの［**ユーザー通知方法**］ページで、証明書の作成に関する SMS またはメールによってモバイルデバイスユーザーに通知する場合の設定を定義します。

- **ウィザード内で QR コードを表示**

このオプションをオンにすると、モバイルデバイスの接続ウィザードの最後の手順で、インストールパッケージへのリンクが表示されます。

このオプションは、デバイスを選択するユーザーを複数選択した場合には使用できません。

- **QR コードをユーザーに送信**

このオプションをオンにすると、新しいモバイルデバイスが接続された時のユーザー通知を設定できます。

メールアドレスの種別の選択、追加のメールアドレスの指定、メッセージ本文の編集が可能です。SMS メッセージを送信するユーザー端末の種別の選択、追加の電話番号の指定、SMS メッセージの本文の編集も可能です。

SMTP サーバーが設定されていない場合、ユーザーへのメールは送信されません。SMS 通知が設定されていない場合、ユーザーへの SMS は送信されません。

7. ［**結果**］ウィンドウで、［**完了**］をクリックして、証明書インストールウィザードを閉じます。

ウィザードが終了すると、リンクと QR コードがユーザーのモバイルデバイスに送信され、Kaspersky Endpoint Security for Android をダウンロードできるようになります。ユーザーがリンクをクリックするか QR コードをスキャンします。その後、モバイルデバイスのオペレーティングシステムが、Kaspersky Endpoint Security for Android のインストールへの同意をユーザーに要求します。Kaspersky Endpoint Security for Android がダウンロードされてインストールされると、モバイルデバイスが管理サーバーに接続して、共有証明書をダウンロードします。証明書がモバイルデバイスにインストールされると、そのモバイルデバイスが、コンソールツリーの［**モバイルデバイス**］フォルダーにある［**モバイルデバイス管理**］フォルダーに表示されます。

Kaspersky Security Center Web サーバーのリンクを使用しての Android モバイルデバイスの追加

管理サーバーで公開された Kaspersky Endpoint Security for Android のインストールパッケージをインストールに使用します。

Web サーバーへのリンクを使用して Kaspersky Endpoint Security for Android と共有証明書をモバイルデバイスにインストールするには：

1. モバイルデバイスの接続ウィザードを起動します。

2. ウィザードの［**オペレーティングシステム**］ページで、モバイルデバイスのオペレーティングシステム種別として［**Android**］を選択します。

3. ウィザードの［**デバイスに Kaspersky Endpoint Security for Android をインストールする方法**］ページで、［**Kaspersky Security Center からアプリのインストールパッケージをダウンロード**］を選択します。

   下に表示されるフィールドで、インストールパッケージを選択するか、［**新規**］をクリックして新規インストールパッケージを作成します。

4. ウィザードの［**管理対象のモバイルデバイスを所有しているユーザーを選択してください**］ページで、管理対象デバイスのリストに追加するモバイルデバイスを所有しているユーザー、セキュリティグループ、または Active Directory セキュリティグループを選択します。

   ［**ユーザーアカウント**］フォルダーのコンテキストメニューで［**モバイルデバイスの追加**］を選択してウィザードを開始した場合、この手順はスキップされます。

   新しいユーザーアカウントをリストに追加するには、［**追加**］をクリックして表示されるウィンドウで、ユーザーアカウントの情報を入力します。既存のユーザーアカウントの情報を変更したり確認するには、リストからユーザーアカウントを選択し［**プロパティ**］をクリックします。

5. ウィザードの［**証明書ソース**］ウィンドウで、管理サーバーがモバイルデバイスの識別に使用する共有証明書の作成方法を指定します。次のいずれかの方法で、共有証明書を指定できます：

   - **管理サーバーツール経由で証明書を発行する**

     以前に証明書を作成していない場合は、管理サーバーのツールを使用して新しい証明書を作成するためにこのオプションを選択してください。

     このオプションをオンにすると、管理サーバーのツールを使用して証明書が自動的に発行されます。

     既定ではこのオプションが選択されます。

   - **証明書ファイルを指定する**

     以前に作成した証明書ファイルを指定する場合は、このオプションを選択します。

     この方法は、前のステップで複数のユーザーを選択した場合には使用できません。

6. ウィザードの［**ユーザー通知方法**］ページで、証明書の作成に関する SMS またはメールによってモバイルデバイスユーザーに通知する場合の設定を定義します。

   - **ウィザード内で QR コードを表示**

     このオプションをオンにすると、モバイルデバイスの接続ウィザードの最後の手順で、インストールパッケージへのリンクが表示されます。

     このオプションは、デバイスを選択するユーザーを複数選択した場合には使用できません。

   - **QR コードをユーザーに送信**

このオプションをオンにすると、新しいモバイルデバイスが接続された時のユーザー通知を設定できます。

メールアドレスの種別の選択、追加のメールアドレスの指定、メッセージ本文の編集が可能です。SMS メッセージを送信するユーザー端末の種別の選択、追加の電話番号の指定、SMS メッセージの本文の編集も可能です。

SMTP サーバーが設定されていない場合、ユーザーへのメールは送信されません。SMS 通知が設定されていない場合、ユーザーへの SMS は送信されません。

7. ［**結果**］ページで、［**完了**］をクリックして、証明書インストールウィザードを閉じます。

Kaspersky Endpoint Security for Android のモバイルアプリパッケージが自動的に Kaspersky Security Center Web サーバーで公開されます。モバイルアプリパッケージには、アプリ、モバイルデバイスから管理サーバーへの接続設定、および証明書が含まれます。モバイルデバイスのユーザーが、Web サーバーからパッケージをダウンロードするためのリンクが記載された通知を受信します。ユーザーが、リンクをクリックします。デバイスのオペレーティングシステムが、モバイルアプリパッケージのインストールへの同意をユーザーに要求します。ユーザーが同意すると、パッケージがモバイルデバイスにダウンロードされます。パッケージがダウンロードされ、モバイルデバイスが管理サーバーと同期されると、そのデバイスが、コンソールツリーの［**モバイルデバイス管理**］フォルダーにある［**モバイルデバイス**］フォルダーに表示されます。

iOS MDM デバイスの管理

このセクションでは、Kaspersky Security Center を使用して iOS MDM デバイスを管理するための機能を詳細に説明しています。iOS MDM デバイスを管理するために、次の機能がサポートされています：

- 一元管理モードで管理対象の iOS MDM デバイスの設定を定義し、設定プロファイルを用いてデバイスの機能を制限します。設定プロファイルを追加または変更し、モバイルデバイスにインストールできます。
- App Store を介さずに、プロビジョニングプロファイルを使用してモバイルデバイスにアプリをインストールします。たとえば、ユーザーのモバイルデバイスに社内の企業アプリをインストールするために、プロビジョニングプロファイルを使用できます。プロビジョニングプロファイルには、アプリとモバイルデバイスの情報が含まれます。
- App Store を介して iOS MDM デバイスにアプリをインストールします。アプリは、iOS MDM デバイスにインストールする前に、iOS MDM サーバーに追加しておく必要があります。

接続されているすべての iOS MDM デバイスにプッシュ通知が 24 時間ごとに送信されます。これは、データと iOS MDM サーバーを同期させるためです。

設定プロファイルとプロビジョニングプロファイル、および iOS MDM デバイスでインストールされたアプリに関する情報は、デバイスのプロパティウィンドウを参照してください。

証明書による iOS MDM プロファイルの署名

証明書で iOS MDM プロファイルに署名することができます。自分で発行した証明書または信頼できる証明書認証局から受け取った証明書を使用することができます。

iOS デバイスでは、署名されていないプロファイルに対して免責事項が表示され、プロファイルのインストール時にユーザーに署名者を信頼するように要求されます。

証明書で iOS MDM プロファイルに署名するには：

1. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。
2. ［**モバイルデバイス**］フォルダーのコンテキストメニューで、［**プロパティ**］を選択します。
3. フォルダーのプロパティウィンドウで、［**iOS デバイスの接続設定**］セクションを選択します。
4. ［**証明書ファイルの選択**］の下にある［**参照**］をクリックします。
   ［**証明書**］ウィンドウ。
5. ［**証明書の種別**］で、証明書の種別について、プライベート証明書か公開証明書かを選択します。
   - ［**PKCS #12 コンテナー**］を選択した場合は、証明書を指定してパスワードを設定します。
   - ［**X.509 証明書**］を選択した場合：
     a. 秘密鍵ファイルを指定します（拡張子が *.prk または *.pem のファイル）。
     b. 秘密鍵のパスワードを指定します。
     c. 公開鍵のパスワードを指定します（拡張子が *.cer のファイル）。
6. ［**OK**］をクリックします。

iOS MDM プロファイルは証明書で署名されました。

設定プロファイルの追加

設定プロファイルを作成するには、Apple Inc. の Web サイトで使用できる Apple Configurator 2 を使用できます。Apple Configurator 2 は macOS を実行しているデバイス上でのみ動作します。このようなデバイスがない場合は、代わりに管理コンソールのあるデバイスで iPhone 構成ユーティリティを使用することができます。しかし、Apple Inc. では iPhone 構成ユーティリティはサポート対象外になっています。

iPhone 構成ユーティリティを使用して設定プロファイルを作成し、iOS MDM サーバーに追加するには：

1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを開きます。
2. ［**モバイルデバイス管理**］フォルダーの作業領域で、［**モバイルデバイスサーバー**］サブフォルダーを選択します。
3. ［**モバイルデバイスサーバー**］フォルダーの作業領域で、iOS MDM サーバーを選択します。
4. iOS MDM サーバーのコンテキストメニューで、［**プロパティ**］を選択します。
   モバイルデバイスサーバーのプロパティウィンドウが開きます。
5. iOS MDM サーバーのプロパティウィンドウで、［**設定プロファイル**］セクションを選択します。
6. ［**設定プロファイル**］セクションで、［**作成**］をクリックします。
   ［**新しい設定プロファイル**］ウィンドウが開きます。
7. ［**新しい設定プロファイル**］ウィンドウで、プロファイルの名前と ID を指定します。

設定プロファイルの ID は一意にし、値は Reverse-DNS 形式で指定する必要があります。たとえば、「*com.companyname.identifier*」です。

8. ［**OK**］をクリックします。

   iPhone 構成ユーティリティはインストール後開始されます。

9. iPhone 構成ユーティリティでプロファイルを再設定します。

   プロファイル設定の詳細と設定方法については、iPhone 構成ユーティリティに付属のドキュメントを参照してください。

iPhone 構成ユーティリティを使用してプロファイルを設定すると、iOS MDM サーバーのプロパティウィンドウの［**設定プロファイル**］セクションに新しい設定プロファイルが表示されます。

［**変更**］をクリックすると、設定プロファイルを変更できます。

［**インポート**］をクリックして、設定プロファイルをプログラムに読み込むことができます。

［**エクスポート**］をクリックして、設定プロファイルをファイルに保存できます。

作成したプロファイルは、iOS MDM デバイスにインストールする必要があります。

設定プロファイルのデバイスでのインストール

モバイルデバイスから設定プロファイルをインストールするには：

1. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。

   フォルダーの作業領域には、管理対象のモバイルデバイスのリストが表示されます。

2. 作業領域では、プロトコル種別（「*iOS MDM*」）によって iOS MDM デバイスをフィルタリングします。

3. 設定プロファイルをインストールする必要があるユーザーのモバイルデバイスを選択します。

   複数のモバイルデバイスを選択し、それらのデバイスにプロファイルを同時にインストールできます。

4. モバイルデバイスのコンテキストメニューから、［**コマンドログの表示**］を選択します。

5. ［**モバイルデバイスの管理コマンド**］ウィンドウで、［**プロファイルのインストール**］セクションに移動し、［**コマンドを送信する**］をクリックします。

   また、モバイルデバイスのコンテキストメニューから［**すべてのコマンド**］→［**プロファイルのインストール**］の順に選択して、モバイルデバイスにコマンドを送信することもできます。

   ［**プロファイルの選択**］ウィンドウが開き、プロファイルのリストが表示されます。そのリストから、モバイルデバイスにインストールする必要があるプロファイルを選択します。複数のプロファイルを選択して、モバイルデバイスへ同時にインストールできます。プロファイルの範囲を選択するには、**SHIFT** キーを使用します。プロファイルをグループごとに組み合わせるには、**CTRL** キーを使用します。

6. ［**OK**］をクリックしてモバイルデバイスにコマンドを送信します。

   コマンド実行時、選択された設定プロファイルがユーザーのモバイルデバイスにインストールされます。コマンドが問題なく実行されると、コマンドログにあるコマンドの現在のステータスは「*完了*」と表示されます。

   ［**再送信**］をクリックして、コマンドをモバイルデバイスに再度送信できます。

送信したコマンドがまだ実行されていない場合は、［**キューから削除**］をクリックしてそのコマンドの実行をキャンセルできます。

［**コマンドログ**］セクションには、個別の実行ステータスも合わせて、モバイルデバイスに送信されているコマンドが表示されます。［**更新**］をクリックすると、コマンドのリストが更新されます。

7. ［**OK**］をクリックすると、［**モバイルデバイスの管理コマンド**］ウィンドウが閉じられます。

インストールしたプロファイルを表示したり必要に応じて削除することができます。

設定プロファイルのデバイスからの削除

モバイルデバイスから設定プロファイルを削除するには：

1. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。
   フォルダーの作業領域には、管理対象のモバイルデバイスのリストが表示されます。
2. 作業領域では、［**iOS MDM**］をクリックして、iOS MDM デバイスをフィルタリングします。
3. 設定プロファイルを削除する必要があるモバイルデバイスを選択します。
   複数のモバイルデバイスを選択し、それらのデバイスからプロファイルを同時に削除できます。
4. モバイルデバイスのコンテキストメニューから、［**コマンドログの表示**］を選択します。
5. ［**モバイルデバイスの管理コマンド**］ウィンドウで、［**プロファイルの削除**］セクションに移動し、［**コマンドを送信する**］をクリックします。
   また、デバイスのコンテキストメニューから［**すべてのコマンド**］→［**プロファイルの削除**］の順に選択して、モバイルデバイスにコマンドを送信することもできます。
   ［**プロファイルの削除**］ウィンドウが開き、プロファイルのリストが表示されます。
6. そのリストから、モバイルデバイスから削除する必要があるプロファイルを選択します。複数のプロファイルを選択して、モバイルデバイスから同時に削除することもできます。プロファイルの範囲を選択するには、**SHIFT** キーを使用します。プロファイルをグループごとに組み合わせるには、**CTRL** キーを使用します。
7. ［**OK**］をクリックしてモバイルデバイスにコマンドを送信します。
   コマンドが実行されると、選択した設定プロファイルはモバイルデバイスから削除されます。コマンドが問題なく実行されると、コマンドの現在のステータスは「*完了*」と表示されます。
   ［**再送信**］をクリックして、コマンドをモバイルデバイスに再度送信できます。
   送信したコマンドがまだ実行されていない場合は、［**キューから削除**］をクリックしてそのコマンドの実行をキャンセルできます。
   ［**コマンドログ**］セクションには、個別の実行ステータスも合わせて、モバイルデバイスに送信されているコマンドが表示されます。［**更新**］をクリックすると、コマンドのリストが更新されます。
8. ［**OK**］をクリックすると、［**モバイルデバイスの管理コマンド**］ウィンドウが閉じられます。

プロファイルのリンク公開による新規デバイスの追加

管理コンソールで、管理者は証明書インストールウィザードを使用して新しい iOS MDM プロファイルを作成します。このウィザードにより、次の操作が実行されます：

- iOS MDM プロファイルが Web サーバーで自動的に公開されます。
- iOS MDM プロファイルへのリンクが、SMS またはメールによってユーザーに送信されます。ユーザーはリンクを受信すると、iOS MDM プロファイルをモバイルデバイスにインストールします。
- モバイルデバイスは iOS MDM サーバーに接続されます。

Apple によってより厳格なセキュリティポリシーが導入されているため、iOS 11 が動作しているモバイルデバイスを公開鍵基盤（PKI）との統合が有効になった管理サーバーに接続する場合は、TLS 1.1 と TLS 1.2 のバージョンのプロトコルをセットアップする必要があります。

管理者のプロファイルインストールによる新規デバイスの追加

iOS MDM プロファイルをモバイルデバイスにインストールすることで、そのモバイルデバイスを iOS MDM サーバーに接続するには、管理者は以下の操作を実行する必要があります：

1. 管理コンソールで、証明書のインストールウィザードを開きます。
2. ウィザードウィンドウの［**ウィザードの終了後に証明書を表示**］をオンにすることで、新しい iOS MDM プロファイルを作成します。
3. iOS MDM プロファイルを保存します。
4. Apple Configurator ユーティリティを使用して、iOS MDM プロファイルをユーザーのモバイルデバイスにインストールします。

   モバイルデバイスは iOS MDM サーバーに接続されます。

Apple によってより厳格なセキュリティポリシーが導入されているため、iOS 11 が動作しているモバイルデバイスを公開鍵基盤（PKI）との統合が有効になった管理サーバーに接続する場合は、TLS 1.1 と TLS 1.2 のバージョンのプロトコルをセットアップする必要があります。

プロビジョニングプロファイルの追加

iOS MDM サーバーにプロビジョニングプロファイルを追加するには：

1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを開きます。
2. コンソールツリーの［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイスサーバー**］サブフォルダーを選択します。
3. ［**モバイルデバイスサーバー**］フォルダーの作業領域で、iOS MDM サーバーを選択します。
4. iOS MDM サーバーのコンテキストメニューで、［**プロパティ**］を選択します。

   モバイルデバイスサーバーのプロパティウィンドウが開きます。
5. **iOS MDM サーバー**のプロパティウィンドウで［**プロビジョニングプロファイル**］セクションに移動します。

6. ［**プロビジョニングプロファイル**］セクションで、［**インポート**］をクリックし、プロビジョニングプロファイルファイルへのパスを指定します。

プロファイルは、iOS MDM サーバーの設定に追加されます。

［**エクスポート**］をクリックして、プロビジョニングプロファイルをファイルに保存できます。

インポートしたプロビジョニングプロファイルをiOS MDM デバイスにインストールすることができます。

プロビジョニングプロファイルのデバイスへのインストール

モバイルデバイスでプロビジョニングプロファイルをインストールするには：

1. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。
   フォルダーの作業領域には、管理対象のモバイルデバイスのリストが表示されます。
2. 作業領域では、プロトコル種別（「*iOS MDM*」）によって iOS MDM デバイスをフィルタリングします。
3. プロビジョニングプロファイルをインストールする必要があるモバイルデバイスを選択します。
   複数のモバイルデバイスを選択し、プロビジョニングプロファイルを同時にインストールできます。
4. モバイルデバイスのコンテキストメニューから、［**コマンドログの表示**］を選択します。
5. ［**モバイルデバイスの管理コマンド**］ウィンドウで、［**プロビジョニングプロファイルのインストール**］セクションに移動し、［**コマンドを送信する**］をクリックします。
   また、デバイスのコンテキストメニューから［**すべてのコマンド**］→［**プロビジョニングプロファイルのインストール**］を選択して、デバイスにコマンドを送信することもできます。
   ［**プロビジョニングプロファイルの選択**］ウィンドウが開き、プロビジョニングプロファイルのリストが表示されます。そのリストから、モバイルデバイスにインストールする必要があるプロビジョニングプロファイルを選択します。複数のプロビジョニングプロファイルを選択して、モバイルデバイスへ同時にインストールすることもできます。プロビジョニングプロファイルの範囲を選択するには、**SHIFT** キーを使用します。プロビジョニングプロファイルをグループごとに組み合わせるには、**CTRL** キーを使用します。
6. ［**OK**］をクリックしてモバイルデバイスにコマンドを送信します。
   コマンド実行時、選択されたプロビジョニングプロファイルがユーザーのモバイルデバイスにインストールされます。コマンドが問題なく実行されると、コマンドログにあるコマンドの現在のステータスは「*完了*」と表示されます。
   ［**再送信**］をクリックして、コマンドをモバイルデバイスに再度送信できます。
   送信したコマンドがまだ実行されていない場合は、［**キューから削除**］をクリックしてそのコマンドの実行をキャンセルできます。
   ［**コマンドログ**］セクションには、個別の実行ステータスも合わせて、モバイルデバイスに送信されているコマンドが表示されます。［**更新**］をクリックすると、コマンドのリストが更新されます。
7. ［**OK**］をクリックすると、［**モバイルデバイスの管理コマンド**］ウィンドウが閉じられます。

インストールしたプロファイルを表示したり必要に応じて削除することができます。

プロビジョニングプロファイルのデバイスからの削除

モバイルデバイスからプロビジョニングプロファイルを削除するには：

1. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。
   フォルダーの作業領域には、管理対象のモバイルデバイスのリストが表示されます。
2. 作業領域では、プロトコル種別（「*iOS MDM*」）によって iOS MDM デバイスをフィルタリングします。
3. プロビジョニングプロファイルを削除する必要があるモバイルデバイスを選択します。
   複数のモバイルデバイスを選択し、それらのデバイスからプロビジョニングプロファイルを同時に削除できます。
4. モバイルデバイスのコンテキストメニューから、［**コマンドログの表示**］を選択します。
5. ［**モバイルデバイスの管理コマンド**］ウィンドウで、［**プロビジョニングプロファイルの削除**］セクションに移動し、［**コマンドを送信する**］をクリックします。
   また、コンテキストメニューから［**すべてのコマンド**］→［**プロビジョニングプロファイルの削除**］の順に選択して、モバイルデバイスにコマンドを送信することもできます。
   ［**プロビジョニングプロファイルの削除**］ウィンドウが開き、プロビジョニングプロファイルのリストが表示されます。
6. モバイルデバイスから削除する必要のあるプロビジョニングプロファイルをリストから選択します。複数のプロビジョニングプロファイルを選択して、モバイルデバイスから同時に削除することもできます。プロビジョニングプロファイルの範囲を選択するには、**SHIFT** キーを使用します。プロビジョニングプロファイルをグループごとに組み合わせるには、**CTRL** キーを使用します。
7. ［**OK**］をクリックしてモバイルデバイスにコマンドを送信します。
   コマンドが実行されると、選択したプロビジョニングプロファイルはモバイルデバイスから削除されます。削除されたプロビジョニングプロファイルに関連した製品は、操作できなくなります。コマンドが問題なく実行されると、コマンドの現在のステータスは「*完了*」と表示されます。
   ［**再送信**］をクリックして、コマンドをモバイルデバイスに再度送信できます。
   送信したコマンドがまだ実行されていない場合は、［**キューから削除**］をクリックしてそのコマンドの実行をキャンセルできます。
   ［**コマンドログ**］セクションには、個別の実行ステータスも合わせて、モバイルデバイスに送信されているコマンドが表示されます。［**更新**］をクリックすると、コマンドのリストが更新されます。
8. ［**OK**］をクリックすると、［**モバイルデバイスの管理コマンド**］ウィンドウが閉じられます。

管理対象アプリケーションの追加

アプリは、iOS MDM デバイスにインストールする前に、iOS MDM サーバーに追加しておく必要があります。アプリケーションが Kaspersky Security Center を介してデバイスにインストールされている場合、そのアプリケーションは管理対象と判断されます。管理対象アプリケーションは、Kaspersky Security Center を使用してリモートで管理することができます。

iOS MDM サーバーに管理対象アプリケーションを追加するには：

1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを開きます。
2. コンソールツリーの［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイスサーバー**］サブフォルダーを選択します。
3. ［**モバイルデバイスサーバー**］フォルダーの作業領域で、iOS MDM サーバーを選択します。

4. iOS MDM サーバーのコンテキストメニューで、［**プロパティ**］を選択します。

   iOS MDM サーバーのプロパティウィンドウが表示されます。

5. iOS MDM サーバーのプロパティウィンドウで［**管理対象の製品**］セクションを選択します。

6. ［**管理対象の製品**］セクションの［**追加**］をクリックします。

   ［**アプリケーションの追加**］ウィンドウが開きます。

7. ［**アプリケーションの追加**］ウィンドウの［**アプリ名**］で、追加するアプリケーションの名前を指定します。

8. ［**Apple ID または manifest ファイルのリンク**］に、追加するアプリケーションの Apple ID を指定するか、アプリケーションをダウンロードできるマニフェストファイルへのリンクを指定します。

9. ユーザーのモバイルデバイスから iOS MDM プロファイルを削除する時に管理対象アプリケーションを一緒に削除する場合は、［**iOS MDM プロファイルと一緒に削除する**］をオンにします。

10. iTunes を通じたアプリケーションデータのバックアップをブロックする場合は、［**データバックアップをブロックする**］をオンにします。

11. ［**OK**］をクリックします。

追加されたアプリケーションは、iOS MDM サーバーのプロパティウィンドウの［**管理対象の製品**］セクションに表示されます。

モバイルデバイスへのアプリのインストール

iOS MDM モバイルデバイスにアプリをインストールするには：

1. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。

   フォルダーの作業領域には、管理対象のモバイルデバイスのリストが表示されます。

2. アプリをインストールする iOS MDM デバイスを選択します。

   複数のモバイルデバイスを選択し、それらのデバイスにアプリケーションを同時にインストールすることができます。

3. モバイルデバイスのコンテキストメニューから、［**コマンドログの表示**］を選択します。

4. ［**モバイルデバイスの管理コマンド**］ウィンドウで、［**アプリのインストール**］セクションに移動し、［**コマンドを送信する**］をクリックします。

   また、モバイルデバイスのコンテキストメニューから［**すべてのコマンド**］→［**アプリのインストール**］の順に選択して、モバイルデバイスにコマンドを送信することもできます。

   ［**アプリの選択**］ウィンドウが開き、プロファイルのリストが表示されます。そのリストから、モバイルデバイスにインストールする必要のあるアプリケーションを選択します。複数のアプリケーションを選択して、モバイルデバイスへ同時にインストールできます。アプリの範囲を選択するには、**SHIFT** キーを使用します。複数のアプリを組み合わせるには、**CTRL** キーを使用します。

5. ［**OK**］をクリックしてモバイルデバイスにコマンドを送信します。

   コマンドが実行されると、選択したアプリケーションがモバイルデバイスにインストールされます。コマンドが問題なく実行されると、コマンドログにあるコマンドの現在のステータスは「*完了*」と表示されます。

［**再送信**］をクリックして、コマンドをモバイルデバイスに再度送信できます。送信したコマンドがまだ実行されていない場合は、［**キューから削除**］をクリックしてそのコマンドの実行をキャンセルできます。

［**コマンドログ**］セクションには、個別の実行ステータスも合わせて、モバイルデバイスに送信されているコマンドが表示されます。［**更新**］をクリックすると、コマンドのリストが更新されます。

6. ［OK］をクリックすると、［**モバイルデバイスの管理コマンド**］ウィンドウが閉じられます。

インストールされたアプリケーションに関する情報は、iOS MDM モバイルデバイスのプロパティに表示されます。コマンドログを使用するかデバイスのコンテキストメニューを使用して、モバイルデバイスからアプリケーションを削除できます。

アプリのデバイスからの削除

アプリをモバイルデバイスから削除するには：

1. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。

   フォルダーの作業領域には、管理対象のモバイルデバイスのリストが表示されます。

2. 作業領域では、プロトコル種別（「*iOS MDM*」）によって iOS MDM デバイスをフィルタリングします。

3. アプリを削除する必要があるモバイルデバイスを選択します。

   複数のモバイルデバイスを選択し、それらのデバイスからアプリを同時に削除できます。

4. モバイルデバイスのコンテキストメニューから、［**コマンドログの表示**］を選択します。

5. ［**モバイルデバイスの管理コマンド**］ウィンドウで、［**アプリの削除**］セクションに移動し、［**コマンドを送信する**］をクリックします。

   また、モバイルデバイスのコンテキストメニューから［**すべてのコマンド**］→［**アプリの削除**］の順に選択して、モバイルデバイスにコマンドを送信することもできます。

   ［**アプリの削除**］ウィンドウが開き、アプリケーションのリストが表示されます。

6. モバイルデバイスから削除する必要のあるアプリをリストから選択します。複数のアプリを選択し、同時に削除できます。アプリの範囲を選択するには、**SHIFT** キーを使用します。複数のアプリを組み合わせるには、**CTRL** キーを使用します。

7. ［OK］をクリックしてモバイルデバイスにコマンドを送信します。

   コマンドが実行されると、選択したアプリがモバイルデバイスから削除されます。コマンドが問題なく実行されると、コマンドの現在のステータスは「*完了*」と表示されます。

   ［**再送信**］をクリックして、コマンドをモバイルデバイスに再度送信できます。

   送信したコマンドがまだ実行されていない場合は、［**キューから削除**］をクリックしてそのコマンドの実行をキャンセルできます。

   ［**コマンドログ**］セクションには、個別の実行ステータスも合わせて、モバイルデバイスに送信されているコマンドが表示されます。［**更新**］をクリックすると、コマンドのリストが更新されます。

8. ［OK］をクリックすると、［**モバイルデバイスの管理コマンド**］ウィンドウが閉じられます。

iOS MDM モバイルデバイスのローミングを設定する

ローミングを設定するには：

1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを開きます。
2. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。
   フォルダーの作業領域には、管理対象のモバイルデバイスのリストが表示されます。
3. ローミングの設定対象となるユーザーが所有している iOS MDM デバイスを選択します。
   同時に複数のモバイルデバイスを選択し、それらのローミングの設定をまとめて行うこともできます。
4. モバイルデバイスのコンテキストメニューから、［**コマンドログの表示**］を選択します。
5. ［**モバイルデバイスの管理コマンド**］ウィンドウで、［**ローミングの設定**］セクションに移動し、［**コマンドを送信する**］をクリックします。
   また、デバイスのコンテキストメニューで、［**すべてのコマンド**］→［**ローミングの設定**］の順に選択して、モバイルデバイスにコマンドを送信することもできます。
6. ［**ローミングの設定**］ウィンドウで、関連する設定を指定します：
   - **データローミングを有効にする**

     このオプションをオンにすると、iOS MDM モバイルデバイスでデータローミングが有効になります。iOS MDM モバイルデバイスのユーザーは、ローミング中にインターネットにアクセスできます。

     既定では、このオプションはオフです。

選択したデバイスにローミングの設定が行われます。

iOS MDM デバイスに関する情報の表示

iOS MDM デバイスに関する情報を表示するには：

1. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。
   フォルダーの作業領域には、管理対象のモバイルデバイスのリストが表示されます。
2. 作業領域では、［**iOS MDM**］をクリックして、iOS MDM デバイスをフィルタリングします。
3. 情報を表示するモバイルデバイスを選択します。
4. モバイルデバイスのコンテキストメニューから［**プロパティ**］を選択します。
   iOS MDM デバイスのプロパティウィンドウが開きます。

モバイルデバイスのプロパティウィンドウに、接続されている iOS MDM デバイスに関する情報が表示されます。

管理からの iOS MDM デバイスの切断

iOS MDM サーバーから iOS MDM デバイスを切断するには：

1. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。
   フォルダーの作業領域には、管理対象のモバイルデバイスのリストが表示されます。
2. 作業領域では、［**iOS MDM**］をクリックして、iOS MDM デバイスをフィルタリングします。
3. 切断する必要があるモバイルデバイスを選択します。
4. モバイルデバイスのコンテキストメニューで［**削除**］を選択します。

   iOS MDM デバイスは、リスト中で削除対象としてマークされます。モバイルデバイスが、iOS MDM サーバーのデータベースから削除された後に、管理対象デバイスのリストから自動的に削除されます。モバイルデバイスは、1分以内に、iOS MDM サーバーのデータベースから削除されます。

iOS MDM デバイスが管理から切断された後、インストール済みのすべての設定プロファイル、iOS MDM プロファイル、および［**iOS MDM プロファイルと一緒に削除する**］がオンになっているアプリケーションが、デバイスから削除されます。

デバイスへのコマンドの送信

iOS MDM デバイスにコマンドを送信するには：

1. 管理コンソールで、［**モバイルデバイス管理**］フォルダーを開きます。
2. ［**モバイルデバイス**］フォルダーを選択します。
3. ［**モバイルデバイス**］フォルダーで、コマンドの送信先のモバイルデバイスを選択します。
4. モバイルデバイスのコンテキストメニューから、［**コマンドログの表示**］を選択します。
5. 表示されたリストで、モバイルデバイスに送信するコマンドを選択します。

送信されたコマンドの実行ステータスの確認

モバイルデバイスに送信されたコマンドの実行ステータスを確認するには：

1. 管理コンソールで、［**モバイルデバイス管理**］フォルダーを開きます。
2. ［**モバイルデバイス**］フォルダーを選択します。
3. ［**モバイルデバイス**］フォルダーで、選択したコマンドの実行ステータスを確認するモバイルデバイスを選択します。
4. モバイルデバイスのコンテキストメニューから、［**コマンドログの表示**］を選択します。

KES デバイスの管理

Kaspersky Security Center で、KES モバイルデバイスを次の方法で管理できます：

- コマンドを使用して KES デバイスを一元的に管理します。

- KES デバイスの管理設定に関する情報を表示します。
- モバイルアプリパッケージを使用して、アプリケーションをインストールします。
- 管理から KES デバイスを切断します。

KES デバイス用モバイルアプリケーションパッケージの作成

KES デバイス用モバイルアプリケーションパッケージを作成するには、Kaspersky Endpoint Security for Android のライセンスが必要です。

モバイルアプリケーションのパッケージを作成するには：

1. コンソールツリーの［**リモートインストール**］フォルダーで、［**インストールパッケージ**］サブフォルダーを選択します。

   既定では［**リモートインストール**］フォルダーは［**詳細**］フォルダーのサブフォルダーです。

2. ［**その他の操作**］をクリックして、ドロップダウンリストで［**モバイルアプリパッケージの管理**］を選択します。
3. ［**モバイルアプリパッケージの管理**］ウィンドウで、［**新規**］をクリックします。
4. 新規パッケージウィザードが起動します。ウィザードの指示に従ってください。

   作成した新しいモバイルアプリケーションパッケージが、［**モバイルアプリパッケージの管理**］ウィンドウに表示されます。

KES デバイスの証明書ベース認証の有効化

KES デバイスの証明書ベース認証を有効にするには：

1. 管理サーバーがインストールされたクライアントデバイスのシステムレジストリを開きます（たとえば、ローカルで［**スタート**］→［**ファイル名を指定して実行**］で regedit コマンドを使用します）。
2. 次のレジストリエントリに移動します：
   - 32 ビットシステム：

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - 64 ビットシステム：

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. LP_MobileMustUseTwoWayAuthOnPort13292 という名前のキーを作成します。
4. キーの種別に REG_DWORD を指定します。
5. キーの値に 1 を設定します。
6. 管理サーバーサービスを再起動します。

管理サーバーのサービスの実行後、共有証明書を使用する KES デバイスの強制的な証明書ベース認証が有効になります。

KES デバイスから管理サーバーへの最初の接続では、証明書は不要です。

既定では、KES デバイスの証明書ベース認証は無効になっています。

KES デバイスに関する情報の表示

KES デバイスに関する情報を表示するには：

1. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。
   フォルダーの作業領域には、管理対象のモバイルデバイスのリストが表示されます。
2. 作業領域では、プロトコル種別（「*KES*」）によって KES デバイスをフィルタリングします。
3. 情報を表示するモバイルデバイスを選択します。
4. モバイルデバイスのコンテキストメニューから［**プロパティ**］を選択します。

   KES デバイスのプロパティウィンドウが開きます。

モバイルデバイスのプロパティウィンドウに、接続されている KES デバイスに関する情報が表示されます。

管理からの KES デバイスの切断

管理から KES デバイスを切断するには、ユーザーがモバイルデバイスからネットワークエージェントを削除する必要があります。ネットワークエージェントが削除されると、モバイルデバイスの情報が管理サーバーのデータベースから削除されるため、管理者は管理対象デバイスのリストからモバイルデバイスを削除できます。

管理対象デバイスのリストから KES デバイスを削除するには：

1. ［**モバイルデバイス管理**］フォルダーで、［**モバイルデバイス**］サブフォルダーを選択します。
   フォルダーの作業領域には、管理対象のモバイルデバイスのリストが表示されます。
2. 作業領域では、プロトコル種別（「*KES*」）によって KES デバイスをフィルタリングします。
3. 管理から切断する必要があるモバイルデバイスを選択します。
4. モバイルデバイスのコンテキストメニューで［**削除**］を選択します。

   モバイルデバイスが管理対象デバイスのリストから削除されます。

Kaspersky Endpoint Security for Android がモバイルデバイスから削除されていない場合、そのモバイルデバイスは、管理サーバーと同期された後に管理対象デバイスのリストに再表示されます。

データ暗号化と保護機能

データ暗号化により、ノート PC、リムーバブルドライブ、ハードディスクの盗難や紛失、不正なユーザーやアプリケーションによるアクセスなどによる思いがけない情報漏洩の危険性を低減できます。

Kaspersky Endpoint Security for Windows には、暗号化の機能があります。Kaspersky Endpoint Security for Windows は、デバイスのローカルドライブやリムーバブルドライブに保存されているファイル、さらにリムーバブルドライブやハードディスクの全体を暗号化できます。

暗号化のルールは、Kaspersky Security Center を使用してポリシーで設定します。既存のルールに基づく暗号化と復号化は、ポリシーの適用時に行われます。

暗号化管理機能を使用するかどうかは、ユーザーインターフェイスの設定で指定します。

次の操作を実行できます：

- デバイスのローカルドライブにあるファイルの暗号化と復号化の設定と実行
- リムーバブルドライブにあるファイルの暗号化の設定と実行
- アプリケーションによる暗号化されたファイルへのアクセスに関するルールの作成
- ファイル暗号化機能がユーザーのデバイスで制限されている場合の、暗号化されたファイルへアクセスするためのキーファイルの作成とユーザーへの提供
- ハードディスクの暗号化の設定と実行
- 暗号化されたハードディスクおよびリムーバブルディスクへのユーザーによるアクセスの管理（認証エージェントアカウントの管理、アカウント名とパスワードの復旧依頼への対応、暗号化されたデバイスへのアクセス用ライセンスの作成とユーザーへの提供）
- ファイルの暗号化に関する暗号化ステータスとレポートの表示

これらの操作には、Kaspersky Endpoint Security for Windows により提供される専用ツールを使用します。操作方法の詳細と暗号化関連機能の説明は、Kaspersky Endpoint Security for Windows のオンラインヘルプを参照してください。

Kaspersky Security Center では、macOS オペレーティングシステムで動作しているデバイスの暗号化管理機能をサポートしています。暗号化は、暗号化機能をサポートする製品バージョン向けの Kaspersky Endpoint Security for Mac のツールを使用して設定されます。操作方法の詳細と暗号化関連機能の説明は、*Kaspersky Endpoint Security for Mac 管理者用ガイド*を参照してください。

暗号化されたデバイスのリストの表示

暗号化された情報を保存するデバイスのリストを表示するには：

1. 管理サーバーのコンソールツリーで、［**データ暗号化と保護機能**］フォルダーを選択します。
2. 次のいずれかの方法で、暗号化されたデバイスのリストを表示します：

- ［**暗号化されたドライブの管理**］セクションで［**暗号化されたドライブのリストへ移動**］をクリックします。
- コンソールツリーで［**暗号化されたドライブ**］フォルダーを選択します。

暗号化されたファイルが保存されているネットワーク上のデバイスおよびドライブ全体が暗号化されているデバイスの情報が作業領域に保存されます。デバイス上の情報が復号されると、そのデバイスはリストから自動的に削除されます。

デバイスのリストに含まれる情報は、任意の列で昇順または降順に並べ替えることができます。

ユーザーインターフェイス設定で、［**データ暗号化と保護機能**］フォルダーをコンソールツリーに表示するかどうかを指定します。

暗号化イベントのリストの表示

デバイス上でデータの暗号化または復号化タスクを実行する時、Kaspersky Endpoint Security for Windows は、次の種類のイベントに関する Kaspersky Security Center 情報を送信します：

- ディスクの空き容量が不足しているため、ファイルの暗号化または復号化ができないか、暗号化されたファイルを作成できない
- ライセンスの問題で、ファイルの暗号化または復号化ができないか、暗号化されたファイルを作成できない
- アクセス権がないため、ファイルの暗号化または復号化ができないか、暗号化されたファイルを作成できない
- アプリケーションが暗号化されたファイルへのアクセスをブロックされている
- 不明なエラー

デバイスでのデータの暗号化中に発生したイベントのリストを表示するには：

1. 管理サーバーのコンソールツリーで、［**データ暗号化と保護機能**］フォルダーを選択します。
2. 次のいずれかの方法で、暗号化中に発生したイベントのリストを表示します：
   - ［**データ暗号化エラー**］セクションで［**エラーリストへ移動**］をクリックします。
   - コンソールツリーで［**暗号化されたドライブ**］フォルダーを選択します。

作業領域に、デバイスでのデータ暗号化中に発生した問題に関する情報が表示されます。

暗号化イベントのリストでは次の処理を行うことができます：

- 任意の列で昇順または降順にデータレコードを並べ替える
- レコードの簡易検索（任意のリストフィールド内のテキストに対するテキスト検索）を実行する
- イベントのリストをテキストファイルにエクスポートする

ユーザーインターフェイス設定で、［**データ暗号化と保護機能**］フォルダーをコンソールツリーに表示するかどうかを指定します。

暗号化イベントのリストのテキストファイルへのエクスポート

暗号化イベントのリストをテキストファイルにエクスポートするには：

1. 暗号化イベントのリストを作成します。
2. イベントリストのコンテキストメニューから［**リストのエクスポート**］を選択します。
   ［**リストのエクスポート**］ウィンドウが表示されます。
3. ［**リストのエクスポート**］ウィンドウで、イベントリストをエクスポートするテキストファイルの名前を指定し、その保存先のフォルダーを選択し、［**保存**］をクリックします。
   暗号化イベントのリストが、指定したファイルに保存されます。

暗号化レポートの作成と表示

次のレポートを作成できます：

- 管理対象デバイスの暗号化ステータスレポート：様々な管理対象デバイスのデータ暗号化について詳細を確認できます。たとえば、暗号化ルールが設定されたポリシーが適用されるデバイスの数が表示されます。また、再起動が必要なデバイスの数なども確認できます。さらに、各デバイスの暗号化技術とアルゴリズムに関する情報も含まれています。
- 大容量ストレージデバイスの暗号化ステータスレポート：管理対象デバイスの暗号化ステータスレポートと類似の情報が含まれますが、大容量ストレージデバイスとリムーバブルドライブのデータのみが表示されます。
- 暗号化されたドライブへのアクセス権に関するレポート：暗号化されたドライブへのアクセス権を持つユーザーアカウントが表示されます。
- ファイル暗号化のエラーに関するレポート：デバイスでデータの暗号化または復号化タスクを実行した時に発生したエラーの情報を含みます。
- 暗号化されたファイルへのアクセスのブロックに関するレポート：暗号化されたファイルへのアクセスのブロックに関する情報を含みます。このレポートは、暗号化されたファイルやドライブに不正なユーザーまたはアプリケーションがアクセスしようとした場合に役立ちます。

デバイスの暗号化のレポートを生成するには：

1. 管理サーバーのコンソールツリーで、［**データ暗号化と保護機能**］フォルダーを選択します。
2. 次のいずれかの手順を実行します：
   - 管理対象デバイスの暗号化ステータスのレポートを生成するには、［**ストレージデバイスの暗号化ステータスレポートの表示**］をクリックします。
     このレポートを設定していない場合は、新規レポートテンプレートウィザードが起動します。ウィザードの指示に従ってください。

- ストレージデバイスの暗号化ステータスレポートを生成するには、コンソールツリーで［**暗号化されたドライブ**］サブフォルダーを選択し、［**ストレージデバイスの暗号化ステータスレポートの表示**］をクリックします。

レポート作成が開始されます。［**管理サーバー**］フォルダーの［**レポート**］タブにレポートが表示されます。

暗号化されたデバイスへのアクセス権のレポートを生成するには：

1. 管理サーバーのコンソールツリーで、［**データ暗号化と保護機能**］フォルダーを選択します。
2. 次のいずれかの手順を実行します：
   - ［**暗号化されたドライブの管理**］セクションの［**暗号化されたドライブへのアクセス権に関するレポート**］をクリックして、新規レポートテンプレートウィザードを起動します。
   - ［**暗号化されたドライブ**］サブフォルダーを選択し、［**暗号化されたドライブへのアクセス権に関するレポート**］をクリックして、新規レポートテンプレートウィザードを起動します。
3. 新規レポートテンプレートウィザードの指示に従います。

レポート作成が開始されます。［**管理サーバー**］フォルダーの［**レポート**］タブにレポートが表示されます。

ファイル暗号化エラーのレポートを生成するには：

1. 管理サーバーのコンソールツリーで、［**データ暗号化と保護機能**］フォルダーを選択します。
2. 次のいずれかの手順を実行します：
   - ［**データ暗号化エラー**］セクションの［**ファイル暗号化のエラーに関するレポートの表示**］をクリックして、新規レポートテンプレートウィザードを起動します。
   - ［**暗号化イベント**］サブフォルダーを選択し、［**ファイル暗号化のエラーに関するレポート**］をクリックして、新規レポートテンプレートウィザードを起動します。
3. 新規レポートテンプレートウィザードの指示に従います。

レポート作成が開始されます。［**管理サーバー**］フォルダーの［**レポート**］タブにレポートが表示されます。

管理対象デバイスの暗号化ステータスのレポートを生成するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**レポート**］タブを選択します。
3. ［**新規レポートテンプレート**］をクリックして新規レポートテンプレートウィザードを開始します。
4. 新規レポートテンプレートウィザードの指示に従います。［**レポートテンプレートの種別の選択**］ウィンドウで、［**その他**］セクションの［**管理対象デバイスの暗号化ステータスレポート**］を選択します。

新規レポートテンプレートウィザードの終了後、管理サーバーフォルダーの［**レポート**］タブに新しいレポートテンプレートが表示されます。

5. 該当する管理サーバーのフォルダーの［**レポート**］タブで、前の手順で作成したレポートテンプレートを選択します。

   レポート作成が開始されます。［**管理サーバー**］フォルダーの［**レポート**］タブにレポートが表示されます。

デバイスおよびリムーバブルドライブの暗号化ステータスが暗号化ポリシーに準拠しているかどうかについての情報は、［管理サーバー］フォルダーの［**統計**］タブにある情報ペインにも表示されます。

暗号化されたファイルへのアクセスのブロックに関するレポートを生成するには：

1. コンソールツリーで、目的の管理サーバーの名前の付いたフォルダーを選択します。
2. フォルダーの作業領域で、［**レポート**］タブを選択します。
3. ［**新規レポートテンプレート**］をクリックして、新規レポートテンプレートウィザードを開始します。
4. 新規レポートテンプレートウィザードの指示に従います。［**レポートテンプレートの種別の選択**］ウィンドウで、［**その他**］セクションを選択し、［**暗号化されたファイルへのアクセスのブロックに関するレポート**］を選択します。

   新規レポートテンプレートウィザードの終了後、［**管理サーバー**］フォルダーの［**レポート**］タブに新しいレポートテンプレートが表示されます。
5. ［**管理サーバー**］フォルダーの［**レポート**］タブで、前の手順で作成したレポートテンプレートを選択します。

   レポート作成が開始されます。［**管理サーバー**］フォルダーの［**レポート**］タブにレポートが表示されます。

管理サーバー間での暗号化鍵の送信

管理対象デバイスでデータ暗号化機能が有効になっている場合、暗号化鍵は管理サーバーに保存されます。暗号化鍵は、暗号化されたデータへのアクセスと暗号化ポリシーの管理に使用します。

次の場合は、暗号化鍵を別の管理サーバーに送信する必要があります：

- 管理対象デバイスを別の管理サーバーに割り当てるために、このデバイスでネットワークエージェントを再構成する場合。このデバイスに暗号化されたデータが含まれる場合は、暗号化鍵を対象の管理サーバーに送信する必要があります。これを行わないと、データを復号できません。
- 管理サーバー S1 で管理されているデバイス D1 に接続されたリムーバブルドライブを暗号化した後に、このリムーバブルドライブを管理サーバー S2 で管理されているデバイス D2 に接続する場合。リムーバブルドライブのデータにアクセスするには、管理サーバー S1 から管理サーバー S2 に暗号化鍵を送信する必要があります。
- 管理サーバー S1 で管理されているデバイス D1 上のファイルを暗号化した後に、管理サーバー S2 で管理されているデバイス D2 上のファイルにアクセスしようとする場合。ファイルにアクセスするには、管理サーバー S1 から管理サーバー S2 に暗号化鍵を送信する必要があります。

暗号化鍵を送信するには、次の方法があります：

- 暗号化鍵の送信が必要な 2 つの管理サーバーのプロパティで、［**管理サーバーの階層を使用して暗号化キーを取得する**］を有効にすると、自動的に送信されます。管理サーバーのいずれか一方でこのオプションが無効になっていると、暗号化鍵は自動的に送信されません。

管理サーバーのプロパティで［**管理サーバーの階層を使用して暗号化キーを取得する**］をオンにすると、管理サーバーは、独自のリポジトリに保存されているすべての暗号化鍵を、階層の1つ上のレベルのプライマリ管理サーバー（存在する場合）に送信します。

暗号化されたデータにアクセスしようとすると、管理サーバーは最初に独自のリポジトリで暗号化鍵を検索します。［**管理サーバーの階層を使用して暗号化キーを取得する**］がオンになっていて、必要な暗号化鍵がリポジトリで見つからなかった場合、管理サーバーはさらにプライマリ管理サーバーにリクエストを送信して、必要な暗号化鍵を提供します。リクエストは、階層の最上位レベルまでのすべてのプライマリ管理サーバーに送信されます。

現在、［**管理サーバーの階層を使用して暗号化キーを取得する**］オプションは、Web コンソールのインターフェイスでは使用できません。MMC ベースの管理コンソールにアクセスできない場合は、プライマリ管理サーバーを使用して暗号化されたデバイスを管理します。

- 暗号化鍵を含むファイルをエクスポートおよびインポートすることで、ある管理サーバーから別の管理サーバーへ手動で送信します。

  暗号化鍵のエクスポートとインポートは、暗号化鍵の管理機能に含まれる操作です。これらの操作を実行するには、次のように Kaspersky Security Center のユーザー向け機能へのアクセス権を設定します：

  - セカンダリ管理サーバーから暗号化鍵をエクスポートするユーザーに、暗号化鍵の管理機能への**読み取り**アクセス権を付与します。
  - 対象の管理サーバーに暗号化鍵をインポートするユーザーに、暗号化鍵の管理機能への［**書き込み**］アクセス権を付与します。

階層内の管理サーバー間で暗号化鍵の自動送信を有効にするには：

1. コンソールツリーで、暗号化鍵の自動送信を有効にする管理サーバーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. プロパティウィンドウで［**暗号化アルゴリズム**］セクションを選択します。
4. ［**管理サーバーの階層を使用して暗号化キーを取得する**］をオンにします。
5. ［**OK**］をクリックして変更を適用します。

暗号化鍵は、次回の同期（ハートビート）でプライマリ管理サーバー（存在する場合）に送信されます。また、この管理サーバーは、リクエストに応じて、独自のリポジトリからセカンダリ管理サーバーに暗号化鍵を提供します。

管理サーバー間で暗号化鍵を手動で送信するには：

1. 管理サーバーのコンソールツリーで、暗号化鍵を送信するセカンダリ管理サーバーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. プロパティウィンドウで［**暗号化アルゴリズム**］セクションを選択します。
4. ［**暗号化キーを管理サーバーからエクスポート**］をクリックします。

   サーバーから暗号化鍵をエクスポートするユーザーに、暗号化鍵の管理機能への**読み取り**アクセス権が付与されていることを確認します。
5. ［**暗号化キーのエクスポート**］ウィンドウで、以下を行います：

- ［**参照**］をクリックし、ファイルの保存場所を指定します。
- パスワードを指定して、不正アクセスからファイルを保護します。

  パスワードは忘れないように注意してください。パスワードを忘れた場合、復元することはできません。パスワードを紛失した場合は、エクスポートの手順を繰り返す必要があります。そのため、パスワードはメモして手元に保管しておいてください。

6. たとえば、共有フォルダーまたはリムーバブルドライブを使用して、ファイルを別の管理サーバーに送信します。
7. 対象の管理サーバーで、Kaspersky Security Center 管理コンソールが実行中であることを確認します。
8. 管理サーバーのコンソールツリーで、暗号化鍵を送信する対象の管理サーバーを選択します。
9. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
10. プロパティウィンドウで［**暗号化アルゴリズム**］セクションを選択します。
11. ［**暗号化キーを管理サーバーへインポート**］をクリックします。

    サーバーに暗号化鍵をインポートするユーザーに、［**暗号化鍵の管理機能**］への［書き込み］アクセス権が付与されていることを確認します。
12. ［**暗号化キーのインポート**］ウィンドウで、以下を行います：
    - ［**参照**］をクリックし、暗号化鍵を含むファイルを選択します。
    - パスワードを指定します。
13. ［OK］をクリックします。

暗号化鍵は、対象の管理サーバーに送信されます。

データリポジトリ

このセクションでは、管理サーバーに保管され、クライアントデバイスの状況の追跡とクライアントデバイスへのサービス提供に使用されるデータについて説明します。

コンソールツリーの［**リポジトリ**］フォルダーには、クライアントデバイスのステータスを監視するために使用するデータが表示されます。

［**リポジトリ**］フォルダーには、次のオブジェクトがあります：

- 管理サーバーによってダウンロードされ、クライアントデバイスに配信されるアップデート
- ネットワーク上で検出された機器のリスト
- クライアントデバイスで検出されたライセンス
- セキュリティ製品によってデバイス上の隔離フォルダーに格納されるファイル

- クライアントデバイスのバックアップに格納されるファイル
- セキュリティ製品によるスキャンが延期されたファイル

リポジトリオブジェクトリストのテキストファイルへのエクスポート

リポジトリにあるオブジェクトのリストをテキストファイルにエクスポートできます。

オブジェクトのリストをリポジトリからテキストファイルにエクスポートするには：

1. コンソールツリーで、［**リポジトリ**］フォルダーから関連リポジトリのサブフォルダーを選択します。
2. リポジトリのサブフォルダーのコンテキストメニューから、［**リストのエクスポート**］を選択します。

   ［**リストのエクスポート**］ウィンドウが表示されたら、テキストファイルの名前とファイルを保存するフォルダーのパスを指定します。

インストールパッケージ

Kaspersky Security Center は、カスペルスキー製品およびサードパーティ製アプリケーションのインストールパッケージをデータリポジトリに配置します。

*インストールパッケージ*は、アプリケーションのインストールに必要な一連のファイルです。インストールパッケージには、インストールされるアプリケーションのセットアップ設定と初期設定が含まれています。

アプリケーションをクライアントデバイスにインストールする場合、インストールパッケージを作成するか、既存のものを使用します。使用可能なインストールパッケージのリストは、コンソールツリーの［**リモートインストール**］フォルダーの［**インストールパッケージ**］サブフォルダーに格納されています。

リポジトリにあるファイルの主なステータス

セキュリティ製品は、既知のウイルスや脅威となるプログラムがないかどうか、デバイス上のファイルをスキャンし、ファイルにステータスを割り当て、一部のファイルをリポジトリに移動します。

たとえば、セキュリティ製品は以下を実行します：

- ファイルを削除する前にリポジトリにコピーする
- 感染の可能性があるファイルをリポジトリに隔離する

主なステータスは下表の通りです。ファイルに対する処理についての詳細な情報は、それぞれのセキュリティ製品のヘルプを参照してください。

リポジトリにあるファイルのステータス

ステータスの名前	ステータスの説明
感染	既知のウイルスのコード、またはカスペルスキーの定義データベースに情報のある悪意のあるソフトウェアのコードからなるセクションがファイル内に存在します。
感染なし	既知のウイルスやその他の悪意のあるソフトウェアはファイル内には存在しません。

警告	既知の脅威のコードの一部と部分的に一致するコードがファイル内に存在します。
感染の可能性あり	既知のウイルスの修正されたコード、またはカスペルスキーがまだ特定していないウイルスのコードに類似したコードがファイル内に存在します。
ユーザーによるフォルダーへの追加	ファイルの挙動から脅威が含まれている可能性があると考えられたため、ユーザーがファイルを手動でリポジトリに移動しました。最新の定義データベースを使用してスキャンし、脅威の有無を確認できます。
誤検知	感染していないファイルのコードがウイルスに似ていたため、カスペルスキー製品が「感染」ステータスを割り当てました。最新の定義データベースを使用してスキャンを実行したところ、ファイルは感染されていないと判断されました。
駆除済み	ファイルは駆除されました。
削除済み	処理の実行中にファイルが削除されました。
パスワードによる保護	ファイルがパスワードで保護されているため、処理できません。

スマートトレーニングモードでのルールの適用条件

このセクションでは、クライアントデバイス上の Kaspersky Endpoint Security for Windows によるアダプティブアノマリーコントロールルールを使用した検知結果について説明します。

ルールは、クライアントデバイス上の通常と異なるふるまいを検知し、ブロックできます。ルールをスマートトレーニングモードで動作させている場合は、ルールによって異常なふるまいが検知されると、すべての検知について Kaspersky Security Center 管理サーバーにレポートが送信されます。これらの情報は［**リポジトリ**］フォルダーの［**「スマートトレーニング」ステータスのルール適用条件**］サブフォルダーのリストに保存されます。検知結果を適切だとして確認することも、同種のふるまいが異常なふるまいとみなされないように除外として追加することもできます。

検知結果に関する情報は、管理サーバーでイベントログ（他のイベントと同様）と［アダプティブアノマリーコントロール］レポートに保存されます。

アダプティブアノマリーコントロールルールおよびルールのモードとステータスの詳細は、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

アダプティブアノマリーコントロールルールを使用した検知のリストの表示

アダプティブアノマリーコントロールルールを使用した検知のリストを表示するには：

1. コンソールツリーで、目的の管理サーバーを選択します。
2. ［**「スマートトレーニング」ステータスのルール適用条件**］を選択します（既定では［**詳細**］→［**リポジトリ**］のサブフォルダーとして含まれます）。

   リストには、アダプティブアノマリーコントロールルールを使用した検知結果について次の情報が表示されます：

   - **管理グループ**

     デバイスが属する管理グループの名前

   - **デバイス名**

     ルールが適用されたクライアントデバイスの名前

- **名前**

  適用されたルールの名前

- **ステータス**

  除外済み、同期待ち - 管理者がこの項目を処理してルールの除外対象として追加した場合。このステータスは、クライアントデバイスと管理サーバーが次に同期するまで表示されます。同期が完了すると、項目はリストに表示されなくなります。

  確認済み、同期待ち - 管理者がこの項目を処理して確認した場合。このステータスは、クライアントデバイスと管理サーバーが次に同期するまで表示されます。同期が完了すると、項目はリストに表示されなくなります。

  （空白） - 管理者が項目を処理していない場合。

- **ルールの適用回数の合計**

  ヒューリスティックルール1件、プロセス1回、クライアントデバイス1台での検知数。この数は、Kaspersky Endpoint Security によってカウントされます。

- **ユーザー名**

  検知が発生したプロセスを実行したクライアントデバイスユーザー名

- **ソースプロセスのパス**

  処理を実行したプロセスであるソースプロセスのパス（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ソースプロセスのハッシュ**

  ソースプロセスファイルの SHA256 ハッシュ（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ソースオブジェクトのパス**

  プロセスを開始したオブジェクトのパス（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ソースオブジェクトのハッシュ**

  ソースファイルの SHA256 ハッシュ（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ターゲットプロセスのパス**

  ターゲットプロセスのパス（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ターゲットプロセスのハッシュ**

  ターゲットファイルの SHA256 ハッシュ（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ターゲットオブジェクトのパス**

  ターゲットオブジェクトのパス（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ターゲットオブジェクトのハッシュ**

  ターゲットファイルの SHA256 ハッシュ（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **処理日**

  異常が検知された日付。

各情報要素のプロパティを表示するには：

1. コンソールツリーで、目的の管理サーバーを選択します。
2. ［**「スマートトレーニング」ステータスのルール適用条件**］を選択します（既定では［**詳細**］→［**リポジトリ**］のサブフォルダーとして含まれます）。
3. ［**「スマートトレーニング」ステータスのルール適用条件**］作業領域で、目的のオブジェクトを選択します。
4. 次のいずれかの手順を実行します：
   - 画面の右側に表示される情報ボックスで［**プロパティ**］をクリックする。
   - 右クリックして、コンテキストメニューから［**プロパティ**］を選択します。

   オブジェクトのプロパティウィンドウが開き、選択した要素に関する情報が表示されます。

アダプティブアノマリーコントロールルールによる検知結果のリストの任意の要素に対して確認または除外への追加を行えます。

対象の要素を確認するには：

検知結果のリストで任意の要素（または複数の要素）を選択して、［**確認**］をクリックします。

対象の要素のステータスが［**確認中**］に変更されます。

確認処理により、ルールで使用される統計が改善されます（詳しくは、Kaspersky Endpoint Security 11 for Windows のヘルプを参照してください）。

要素を除外に追加するには：

検知結果のリストで任意の要素（または複数の要素）を右クリックして、コンテキストメニューで［**除外に追加**］を選択します。

除外の追加ウィザードが起動します。ウィザードの指示に従ってください。

対象の要素を確認または拒否すると、クライアントデバイスと管理サーバーの次回の同期後にこの検知結果は検知結果リストから除外され、表示されなくなります。

アダプティブアノマリーコントロールルールから除外に追加

除外の追加ウィザードを使用して、Kaspersky Endpoint Security のアダプティブアノマリーコントロールルールに除外を追加できます。

次の 3 つの方法のうちいずれかを使用してウィザードを開始できます。

アダプティブアノマリーコントロールノードから除外の追加ウィザードを開始するには：

1. コンソールツリーで、目的の管理サーバーのフォルダーを選択します。
2. ［**「スマートトレーニング」ステータスのルール適用条件**］を選択します（既定では［**詳細**］→［**リポジトリ**］のサブフォルダーとして含まれます）。
3. 作業領域の検知結果のリストで任意の要素（または複数の要素）を右クリックして、［**除外に追加**］を選択します。

   1 回につき最大 1000 個の除外を追加できます。上限を超える要素を選択して除外に追加しようとすると、エラーメッセージが表示されます。

除外の追加ウィザードが起動します。

コンソールツリーの別のノードから除外の追加ウィザードを開始できます：

- 管理サーバーのメインウィンドウの［**イベント**］タブで（抽出イベントとして［**ユーザー要求**］と［**最近のイベント**］を使用します）
- **アダプティブアノマリーコントロールルールの状態に関するレポート**の［**検知数**］列

ステップ 1：アプリケーションの選択

導入している Kaspersky Endpoint Security for Windows のバージョンが 1 つのみで、アダプティブアノマリーコントロールルールをサポートしているその他のセキュリティ製品を使用していない場合は、この手順は省略できます。

除外の追加ウィザードに、製品管理プラグインを使用して製品のポリシーに除外を追加できるカスペルスキー製品のリストが表示されます。リストから製品を選択し、［**次へ**］をクリックして、除外が追加されるポリシーの選択に進みます。

ステップ 2：ポリシーの選択

ウィザードに、Kaspersky Endpoint Security のポリシーとそのプロファイルのリストが表示されます。

除外を追加したいポリシーとプロファイルをすべて選択し、［**次へ**］をクリックします。

ステップ 3：ポリシーの処理

ポリシーの処理の進捗に応じて、ウィザードに進捗バーが表示されます。［**キャンセル**］をクリックすると、ポリシーの処理を中断できます。

継承したポリシーの内容は更新できません。自分が変更権限を持っていないポリシーの内容も更新できません。

すべてのポリシーの処理が完了すると（または処理を中断すると）、レポートが表示されます。レポートには、正常に更新されたポリシー（緑色のアイコン）と更新されなかったポリシー（赤色のアイコン）が表示されます。

これがこのウィザードでの最後のステップです。［**終了**］をクリックしてウィザードを終了します。

隔離とバックアップ

デバイススキャン中、クライアントデバイスにインストール済みのカスペルスキー製品によって、ファイルが隔離やバックアップに移動されることがあります。

*隔離*とは、感染の可能性があるファイルおよび検知時点で駆除できないファイルを格納する特別なリポジトリです。

*バックアップ*は、駆除中に削除または変更されたファイルのバックアップコピーを保存することを目的としています。

Kaspersky Security Center は、デバイス上のカスペルスキー製品によって隔離またはバックアップに配置されたファイルをまとめたリストを作成します。クライアントデバイス上のネットワークエージェントによって、隔離とバックアップにあるファイルに関する情報が管理サーバーに転送されます。管理コンソールを使用して、クライアントデバイス上のリポジトリに保存されているファイルのプロパティを表示し、それらのリポジトリのマルウェアスキャンを実行し、リポジトリからファイルを削除できます。ファイルステータスのアイコンについては補足情報で説明します。

隔離およびバックアップでの操作は、バージョン 6.0 以降の Kaspersky Anti-Virus for Windows Workstations および Kaspersky Anti-Virus for Windows Servers、さらに Kaspersky Endpoint Security 10 for Windows 以降でサポートされています。

Kaspersky Security Center では、リポジトリのファイルは管理サーバーにコピーされません。すべてのファイルは、デバイス上のリポジトリに保存されます。ファイルは、そのファイルをリポジトリに配置したアンチウイルス製品がインストールされているデバイス上でのみ復元できます。

リポジトリにあるファイルのリモート管理の有効化

既定では、クライアントデバイス上のリポジトリに配置されているファイルを管理することはできません。

クライアントデバイス上のリポジトリに保管されているファイルのリモート管理を有効化するには：

1. コンソールツリーで、リポジトリにあるファイルのリモート管理を有効にする管理グループを選択します。
2. グループの作業領域で、［**ポリシー**］タブを開きます。
3. ［**ポリシー**］タブで、ファイルをデバイス上のリポジトリに配置したセキュリティ製品のポリシーを選択します。

4. ポリシー設定ウィンドウの［**管理サーバーへのデータ転送**］セクションで、リモート管理を有効にするリポジトリに対応するチェックボックスをオンにします。

ポリシーのプロパティウィンドウにおける［**管理サーバーへのデータ転送**］セクションの場所、およびチェックボックスの名前は、使用しているセキュリティ製品により異なります。

リポジトリに配置されているファイルのプロパティの表示

隔離またはバックアップにあるファイルのプロパティを表示するには：

1. コンソールツリーで、［**リポジトリ**］フォルダー - ［**隔離**］サブフォルダーまたは［**バックアップ**］サブフォルダーの順に選択します。
2. ［**隔離**］（［**バックアップ**］）フォルダーの作業領域で、プロパティを表示するファイルを選択します。
3. ファイルのコンテキストメニューから［**プロパティ**］を選択します。

リポジトリからのファイルの削除

隔離またはバックアップからファイルを削除するには：

1. コンソールツリーで、［**リポジトリ**］フォルダーの［**隔離**］または［**バックアップ**］サブフォルダーを選択します。
2. ［**隔離**］（または［**バックアップ**］）フォルダーの作業領域で **Shift** キーおよび **Ctrl** キーを使用して、削除するファイルを選択します。
3. 次のいずれかの方法で、ファイルを削除します：
   - ファイルのコンテキストメニューから［**削除**］を選択します。
   - 選択したファイルの情報ボックスで、［**削除**］をクリックします。

ファイルをクライアントデバイス上のリポジトリに配置したセキュリティ製品によって、これらのリポジトリからファイルが削除されます。

リポジトリからのファイルの復元

隔離またはバックアップからファイルを復元するには：

1. コンソールツリーで、［**リポジトリ**］フォルダー - ［**隔離**］サブフォルダーまたは［**バックアップ**］サブフォルダーの順に選択します。
2. ［**隔離**］（［**バックアップ**］）フォルダーの作業領域で **Shift** キーおよび **Ctrl** キーを使用して、復元するファイルを選択します。
3. 次のいずれかの方法で、ファイルの復元を開始します：
   - ファイルのコンテキストメニューから［**復元**］を選択します。

- 選択したファイルの情報ボックスで、［**復元**］をクリックします。

ファイルをクライアントデバイス上のリポジトリに配置したセキュリティ製品によって、これらのリポジトリからファイルが復元されます。

リポジトリからディスクへのファイルの保存

Kaspersky Security Center では、クライアントデバイス上でセキュリティ製品によって隔離またはバックアップに配置されたファイルのコピーをディスクに保存できます。ファイルは、Kaspersky Security Center がインストールされているデバイスの特定のフォルダーにコピーされます。

隔離またはバックアップにあるファイルのコピーをハードディスクに保存するには：

1. コンソールツリーで、［**リポジトリ**］フォルダー - ［**隔離**］サブフォルダーまたは［**バックアップ**］サブフォルダーの順に選択します。
2. ［**隔離**］（［**バックアップ**］）フォルダーの作業領域で、ハードディスクにコピーするファイルを選択します。
3. 次のいずれかの方法で、コピーを開始します：
   - ファイルのコンテキストメニューから［**ディスクに保存**］を選択します。
   - 選択したファイルの情報ボックスで、［**ディスクに保存**］をクリックします。

クライアントデバイス上の隔離にファイルを配置したセキュリティ製品によって、ファイルのコピーがハードディスクの指定されたフォルダーに保存されます。

隔離にあるファイルのスキャン

隔離されたファイルをスキャンするには：

1. コンソールツリーで、［**リポジトリ**］フォルダーの［**隔離**］サブフォルダーを選択します。
2. ［**隔離**］フォルダーの作業領域で **SHIFT** キーおよび **CTRL** キーを使用して、スキャンするファイルを選択します。
3. 次のいずれかの方法で、ファイルのスキャンを開始します：
   - ファイルのコンテキストメニューから［**スキャン**］を選択します。
   - 選択したファイルの情報ボックスで、［**スキャン**］をクリックします。

選択したファイルが格納されているデバイスで、ファイルを隔離に配置したセキュリティ製品のオンデマンドスキャンタスクが実行されます。

アクティブな脅威

クライアントデバイスで見つかった未処理ファイルに関する情報は、［**リポジトリ**］フォルダーの［**アクティブな脅威**］サブフォルダーに保存されます。

延期された処理と駆除は、要求時または特定のイベント発生後にセキュリティ製品によって実行されます。延期された処理は設定できます。

未処理ファイルの駆除

未処理ファイルの駆除を開始するには：

1. コンソールツリーで、［**リポジトリ**］フォルダーの［**アクティブな脅威**］サブフォルダーを選択します。
2. ［**アクティブな脅威**］フォルダーの作業領域で、駆除するファイルを選択します。
3. 次のいずれかの方法で、ファイルの駆除を開始します：
   - ファイルのコンテキストメニューから［**駆除**］を選択します。
   - 選択したファイルの情報ボックスで、［**駆除**］をクリックします。

   このファイルの駆除が試行されます。

ファイルが駆除された場合、クライアントデバイスにインストールされているセキュリティ製品によって、そのファイルが元の場所に復元されます。ファイルのレコードが［**アクティブな脅威**］フォルダーのリストから削除されます。ファイルが駆除できない場合、クライアントデバイスにインストールされているセキュリティ製品によって、そのファイルがデバイスから削除されます。ファイルのレコードが［**アクティブな脅威**］フォルダーのリストから削除されます。

ファイルの駆除と削除の機能は、インストールされているセキュリティ製品、そのバージョン、設定によって異なる場合があります。

未処理ファイルのディスクへの保存

Kaspersky Security Center では、クライアントデバイスで検知された未処理ファイルのコピーをディスクに保存できます。ファイルは、Kaspersky Security Center がインストールされているデバイスの特定のフォルダーにコピーされます。

駆除中に削除または変更されたファイルのコピーが管理対象デバイス上の Kaspersky Endpoint Security for Windows ストレージ に保存されている場合、それらのコピーのみを保存できます。

未処理ファイルのコピーをディスクに保存するには：

1. コンソールツリーで、［**リポジトリ**］フォルダーの［**アクティブな脅威**］サブフォルダーを選択します。
2. ［**アクティブな脅威**］フォルダーの作業領域で、ディスクにコピーするファイルを選択します。
3. 次のいずれかの方法で、コピーを開始します：
   - ファイルのコンテキストメニューから［**ディスクに保存**］を選択します。
   - 選択したファイルの情報ボックスで、［**ディスクに保存**］をクリックします。

未処理ファイルが検知されたクライアントデバイスにインストールされているセキュリティ製品によって、指定のフォルダーにファイルのコピーが保存されます。

［アクティブな脅威］フォルダーからのファイルの削除

*［**アクティブな脅威**］フォルダーからファイルを削除するには：*

1. コンソールツリーで、［**リポジトリ**］フォルダーの［**アクティブな脅威**］サブフォルダーを選択します。
2. ［**アクティブな脅威**］フォルダーの作業領域で **SHIFT** キーおよび **CTRL** キーを使用して、削除するファイルを選択します。
3. 次のいずれかの方法で、ファイルを削除します：
   - ファイルのコンテキストメニューから［**削除**］を選択します。
   - 選択したファイルの情報ボックスで、［**削除**］をクリックします。

ファイルをクライアントデバイス上のリポジトリに配置したセキュリティ製品によって、これらのリポジトリからファイルが削除されます。ファイルのレコードが［**アクティブな脅威**］フォルダーのリストから削除されます。

Kaspersky Security Network（KSN）

このセクションでは、Kaspersky Security Network（KSN）というオンラインサービスのインフラストラクチャの使用方法を説明します。KSN の詳細、および KSN を有効にする方法、KSN へのアクセスの設定方法、KSN プロキシサーバーの使用の統計を表示する方法を説明します。

アップデート機能（ウイルス対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

KSN について

Kaspersky Security Network（KSN）は、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのナレッジベースへのオンラインアクセスを提供するオンラインサービスの基盤です。Kaspersky Security Network のデータを使用することにより、脅威に対するカスペルスキー製品の対応が迅速化され、一部の保護コンポーネントの効果が高まり、誤検知のリスクが低減されます。KSN によって、カスペルスキーの評価データベースを使用して、管理対象デバイスにインストールされたアプリケーションの情報を取得できます。

Kaspersky Security Center は、次のインフラストラクチャソリューションをサポートしています：

- *KSN*：Kaspersky Security Network との情報交換を可能にするソリューションです。KSN に参加すると、Kaspersky Security Center によって管理されるクライアントデバイス上にインストールされたカスペルスキー製品の動作に関する情報を、自動的にカスペルスキーに送信することに同意したことになります。情報は、現在の KSN アクセス設定に従って転送されます。カスペルスキーのアナリストは、受け取った情報をさらに分析し、Kaspersky Security Network の評価および統計データベースに追加します。Kaspersky Security Center は既定でこのソリューションを使用します。
- *Kaspersky Private Security Network（KPSN）*：カスペルスキー製品がインストールされたデバイスのユーザーが、自分のコンピューターからグローバル KSN にデータを送信することなく、Kaspersky Security

Network の定義データベースやその他の統計データにアクセスすることを可能にするソリューションです。KPSN は、次のいずれかの理由で Kaspersky Security Network にアクセスできない法人ユーザーの方を対象として開発されています：

- ユーザーデバイスがインターネットに接続されていない。
- 国外や企業 LAN の外へのデータの送信が、法律で禁止されているか社内のセキュリティポリシーで制限されている。

管理サーバーのプロパティウィンドウの［**KSN プロキシ設定**］セクションで、Kaspersky Private Security Network のアクセス設定をセットアップできます。

クイックスタートウィザードの実行時には、KSN に参加するよう促されます。アプリケーションの使用時であればいつでも、KSN の使用を開始または停止できます。

お客様は KSN を有効にする際に同意した KSN に関する声明に従って KSN を使用するものとします。KSN 声明が更新された場合は、管理サーバーのバージョンをアップグレードする際に更新された声明が表示されます。更新された KSN に関する声明に同意することも拒否することも可能です。拒否した場合は、以前に同意した KSN 声明の以前のバージョンの内容に従って KSN の使用が継続されます。

KSN が有効になっている場合、Kaspersky Security Center は KSN サーバーがアクセス可能であるかどうかを確認します。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。これは、管理対象デバイスのセキュリティレベルを確実に管理するために必要です。

管理サーバーが管理するクライアントデバイスは、KSN プロキシサーバーを使用して KSN と対話します。KSN プロキシサーバーは次の機能を提供します：

- クライアントデバイスは、インターネットに直接アクセスできない場合でも、KSN に要求を送信し、KSN から情報を取得し、KSN に情報を転送することができます。
- KSN プロキシサーバーでは処理データをキャッシュに保存するため、送信チャネルの負荷が軽減され、クライアントデバイスから要求された情報を待つ時間が短縮されます。

［管理サーバーのプロパティ］ウィンドウの［**KSN プロキシ設定**］セクションで、KSN プロキシサーバーを設定できます。

Kaspersky Security Network へのアクセスの設定

Kaspersky Security Network（KSN）へのアクセスを管理サーバーとディストリビューションポイントで設定できます。

Kaspersky Security Network（KSN）への管理サーバーのアクセスを設定するには：

1. コンソールツリーで、KSN へのアクセスを設定する管理サーバーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウの［**セクション**］ペインで、［**KSN プロキシ**］→［**KSN プロキシ設定**］の順に選択します。
4. 作業領域で、［**管理サーバーをプロキシサーバーとして使用する**］をオンにして、KSN プロキシサービスを使用します。

クライアントデバイスでアクティブな Kaspersky Endpoint Security のポリシーに従って、クライアントデバイスから KSN にデータが送信されます。このチェックボックスをオフにすると、管理サーバーおよびクライアントデバイスから Kaspersky Security Center を経由して KSN にデータが送信されることはありません。しかし、クライアントデバイスが、個々の設定に従って KSN に直接（Kaspersky Security Center を経由せずに）データを送信することがあります。クライアントデバイス上でアクティブな Kaspersky Endpoint Security for Windows ポリシーによって、それらのデバイスから直接（Kaspersky Security Center を経由せずに）KSN に送信するデータが決定されます。

5. ［**Kaspersky Security Network への参加に同意する**］をオンにします。

このオプションをオンにすると、クライアントデバイスがパッチのインストール結果をカスペルスキーに送信します。このオプションをオンにする際には、必ず KSN 声明の条項を読み、それに同意する必要があります。

Kaspersky Private Security Network を使用している場合、［**KPSN の設定**］をオンにし、［**KSN プロキシの設定ファイルを選択**］をクリックして、KPSN の設定をダウンロードします（拡張子 pkcs7、pem のファイル）。設定のダウンロード後、インターフェイスにはプロバイダー名と連絡先が表示されます。また、KPSN が設定されたファイルの作成日も表示されます。

KPSN を有効にする場合、以前の設定で KSN リクエストを直接 KSN クラウドに送信するように指定していたディストリビューションポイントに注意してください。バージョン 11 以前のネットワークエージェントをインストールしているディストリビューションポイントでは、引き続き KSN リクエストを KSN クラウドに送信します。これらのディストリビューションポイントで KSN リクエストを KPSN に送信するように設定を編集するには、［**KSN リクエストを管理サーバーに転送する**］をオンにします。このオプションは、ディストリビューションポイントのプロパティまたはネットワークエージェントのポリシーでオンにできます。

［**KPSN の設定**］をオンにすると、KPSN の詳細を説明したメッセージが表示されます。

Kaspersky Security Center で［**KPSN の設定**］をオンにすると、これらのカスペルスキー製品は KPSN の使用に関する通知を受け取ります。アプリケーション設定ウィンドウの［**先進の脅威対策**］セクションで、［**Kaspersky Security Network**］サブセクションに選択された KSN プロバイダーの情報が以下のように表示されています：KSN または KPSN。

KPSN を運用していて、Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 より前のバージョンまたは Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent より前のバージョンを使用する場合、KPSN の使用を無効にしたセカンダリ管理サーバーを使用してください。

管理サーバーのプロパティウィンドウの［**KSN プロキシ**］→［**KSN プロキシ設定**］セクションで KPSN が設定されている場合、Kaspersky Security Center は Kaspersky Security Network に統計データを送信しません。

管理サーバーのプロパティでプロキシサーバー設定を構成済みだけれどもネットワークアーキテクチャで KPSN を直接使用する必要がある場合は、［**KPSN への接続時に プロキシサーバーの設定を無視する**］をオンにします。このオプションをオンにしないと、管理対象アプリケーションからのリクエストが KPSN に到達できません。

6. 管理サーバーの KSN プロキシサービスへの接続を設定します：

- ［**接続設定**］の［**TCP ポート**］で、KSN プロキシサーバーへの接続に使用する TCP ポートの番号を指定します。KSN プロキシサーバーに接続する既定のポートは 13111 です。
- UDP ポートを経由して KSN プロキシサーバーと管理サーバーを接続する場合は、［**UDP ポートを使用**］をオンにして、［**UDP ポート**］でポート番号を指定します。既定では、このオプションはオフで、TCP ポートが使用されます。KSN プロキシサーバーに接続する既定の UDP ポートは 15111 です。

- 管理サーバーを HTTPS ポート経由で KSN プロキシサーバーに接続する場合は、［**HTTPS の使用時に経由するポート**］オプションを有効にしてポート番号を指定します。既定では、このオプションはオフで、TCP ポートが使用されます。このオプションがオンの場合、KSN プロキシサーバーに接続する既定の HTTPS ポートは 17111 です。

7. ［**KSN にセカンダリ管理サーバーをプライマリ管理サーバー経由で接続する**］をオンにします。

   このオプションをオンにすると、どの階層レベルのセカンダリ管理サーバーでもプライマリ管理サーバーを KSN プロキシサーバーとして使用します。このオプションをオフにすると、セカンダリ管理サーバーは直接 KSN に接続します。その場合、管理対象デバイスはセカンダリ管理サーバーを KSN プロキシサーバーとして使用します。

   > セカンダリ管理サーバーのプロパティの［**KSN プロキシ設定**］セクションの右側で［**管理サーバーをプロキシサーバーとして使用する**］がオンになっている場合、セカンダリ管理サーバーはプライマリ管理サーバーをプロキシサーバーとして使用します。

8. ［**OK**］をクリックします。

KSN のアクセス設定が保存されます。

管理サーバーの負荷を軽減したい場合などに、ディストリビューションポイントから KSN へのアクセスを設定できます。KSN プロキシサーバーとして動作しているディストリビューションポイントは、管理サーバーを使用せずに、管理対象デバイスからの KSN リクエストをカスペルスキーに直接送信します。

Kaspersky Security Network（KSN）へのディストリビューションポイントのアクセスを設定するには：

1. ディストリビューションポイントが手動で割り当てられていることを確認します。
2. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。
3. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
4. 管理サーバーのプロパティウィンドウで、［**ディストリビューションポイント**］セクションを選択します。
5. リスト内のディストリビューションポイントを選択し、［**プロパティ**］をクリックして、プロパティウィンドウを開きます。
6. ディストリビューションポイントのプロパティウィンドウの［**KSN プロキシ**］セクションで、［**インターネット経由で直接 KSN クラウド / KPSN にアクセスする**］を選択します。
7. ［**OK**］をクリックします。

ディストリビューションポイントが KSN プロキシサーバーとして動作します。

KSN の有効化および無効化

KSN を有効にするには：

1. コンソールツリーで、KSN を有効にする必要がある管理サーバーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。

3. 管理サーバーのプロパティウィンドウの［**KSN プロキシ**］セクションで、［**KSN プロキシ設定**］サブセクションを選択します。

4. ［**管理サーバーをプロキシサーバーとして使用する**］を選択します。

   KSN プロキシサーバーが有効になります。

5. ［**Kaspersky Security Network への参加に同意する**］を選択します。

   KSN が有効になります。

   このチェックボックスをオンにすると、クライアントデバイスがパッチのインストール結果をカスペルスキーに送信します。このチェックボックスをオンにした際には、KSN 声明の条項を読み、それに同意する必要があります。

6. ［**OK**］をクリックします。

KSN を無効にするには：

1. コンソールツリーで、KSN を有効にする必要がある管理サーバーを選択します。

2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。

3. 管理サーバーのプロパティウィンドウの［**KSN プロキシ**］セクションで、［**KSN プロキシ設定**］サブセクションを選択します。

4. ［**管理サーバーをプロキシサーバーとして使用する**］をオフにして、KSN プロキシサービスを無効にするか、［**Kaspersky Security Network への参加に同意する**］をオフにします。

   このチェックボックスをオフにすると、クライアントデバイスはパッチのインストール結果をカスペルスキーに送信しません。

   KPSN を使用している場合は、［**KPSN の設定**］をオフにします。

   KSN が無効になります。

5. ［**OK**］をクリックします。

同意した KSN に関する声明の表示

Kaspersky Security Network (KSN) を有効にする際には、KSN に関する声明を読み、同意する必要があります。同意した KSN に関する声明はいつでも表示できます。

同意した KSN に関する声明を表示するには：

1. コンソールツリーで、KSN を有効にした管理サーバーを選択します。

2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。

3. 管理サーバーのプロパティウィンドウの［**KSN プロキシ**］セクションで、［**KSN プロキシ設定**］サブセクションを選択します。

4. ［**同意した KSN 声明の表示**］をクリックします。

   表示されたウィンドウで、同意した KSN に関する声明の内容を表示できます。

KSN プロキシサーバーの統計の表示

*KSN プロキシサーバー*は、Kaspersky Security Network のインフラストラクチャと管理サーバーによって管理されるクライアントデバイスとのインタラクションを確保するサービスです。

KSN プロキシサーバーを使用すると、次の機能が提供されます：

- クライアントデバイスは、インターネットに直接アクセスできない場合でも、KSN に要求を送信し、情報を転送できます。
- KSN プロキシサーバーでは処理データをキャッシュに保存するため、送信チャネルの負荷が軽減され、クライアントデバイスから要求された情報を待つ時間が短縮されます。

管理サーバーのプロパティウィンドウで、KSN プロキシサーバーを設定し、KSN プロキシサーバーの使用統計情報を表示できます。

KSN プロキシサーバーの統計を表示するには：

1. コンソールツリーで、KSN 統計を表示する必要がある管理サーバーを選択します。
2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
3. 管理サーバーのプロパティウィンドウの［**KSN プロキシ**］セクションで、［**KSN プロキシの統計**］サブセクションを選択します。

   このセクションには、KSN プロキシサーバーの動作の実際の統計（キャッシュレコードの数、キャッシュで処理されたパッケージの数、受信されたパッケージの数）が表示されます。また、管理サーバーが KSN に接続されている場合は、対応する情報メッセージが表示されます。

   必要に応じて、次の操作を実行します：

   - ［**更新**］をクリックすると、KSN プロキシサーバーの使用に関する統計情報がアップデートされます。
   - ［**ファイルへのエクスポート**］をクリックすると、統計情報が CSV ファイルにエクスポートされます。
   - 管理サーバーが現在 KSN に接続されているかどうかを確認するには、［**KSN 接続を確認**］をクリックします。
4. ［**OK**］をクリックして、管理サーバーのプロパティウィンドウを閉じます。

更新された KSN に関する声明の同意

お客様は KSN を有効にする際に同意した KSN に関する声明に従って KSN を使用するものとします。KSN に関する声明が更新された場合は、管理サーバーをアップデートまたはアップグレードする際に更新された声明が表示されます。更新された KSN に関する声明に同意することも拒否することも可能です。拒否した場合は、以前に同意した KSN 声明の以前のバージョンの内容に従って KSN の使用が継続されます。

管理サーバーのアップデートまたはアップグレード中に、更新された KSN 声明が自動的に表示されます。更新された KSN 声明を拒否した場合、後で表示して同意することも可能です。

更新された KSN 声明を表示して同意するには：

1. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。

2. ［**監視**］セクションの［**監視**］タブで、［**同意した Kaspersky Security Network に関する声明が最新ではありません**］をクリックします。

   ［**KSN 声明**］ウィンドウが開きます。

3. KSN 声明を読み、対応を判断します。更新された KSN 声明に同意する場合は、［**使用許諾契約書の条項に同意する**］をクリックします。更新された KSN 声明に同意しない場合は、［**キャンセル**］をクリックします。

選択に応じて、KSN は更新前の、もしくは更新された KSN 声明の規約に従い動作します。管理サーバーのプロパティからいつでも同意した KSN 声明の本文を表示できます。

Kaspersky Security Network の強化された保護

Kaspersky Security Network は、ユーザーを高いレベルで保護します。保護の方法は、絶え間なく発生する高度な脅威やゼロデイ攻撃に対抗する目的で設計されています。クラウド技術と、カスペルスキーのウイルスアナリストの専門技術を統合することにより、ネットワーク上の最も高度な脅威に対する最高の保護が、本製品によって実現されます。

本製品の保護で強化された点の詳細は、カスペルスキーの Web サイトを参照してください。

ディストリビューションポイントが KSN プロキシサーバーとして機能するかどうかの確認

ディストリビューションポイントとして機能するように割り当てられた管理対象デバイスで、KSN プロキシサーバーを有効にできます。ksnproxy サービスがデバイスで実行されている場合、管理対象デバイスは KSN プロキシサーバーとして機能します。デバイスでこのサービスをローカルで確認し、オンまたはオフにできます。

Windows ベースまたは Linux ベースのデバイスをディストリビューションポイントとして割り当てることができます。ディストリビューションポイントのチェック方法は、このディストリビューションポイントのオペレーティングシステムによって異なります。

Windows ベースのディストリビューションポイントが KSN プロキシサーバーとして機能するかどうかを確認するには：

1. ディストリビューションポイントデバイスの Windows で、［**サービス**］（［**すべてのプログラム**］→［**管理ツール**］→［**サービス**］）を開きます。

2. サービスのリストで、ksnproxy サービスが実行されているかを確認します。

   ksnproxy サービスが実行されている場合、デバイス上のネットワークエージェントは Kaspersky Security Network に参加し、ディストリビューションポイントの範囲に含まれる管理対象デバイスの KSN プロキシサーバーとして機能します。

   必要に応じて ksnproxy サービスをオフにできます。この場合、ディストリビューションポイントのネットワークエージェントは Kaspersky Security Network への参加を停止します。この操作にはローカル管理者権限が必要です。

Linux ベースのディストリビューションポイントが KSN プロキシサーバーとして機能するかどうかを確認するには：

1. ディストリビューションポイントのデバイスで、実行中のプロセスの一覧を表示します。

2. 実行中のプロセスのリストで、 `/opt/kaspersky/ksc64/sbin/ksnproxy` プロセスが実行されているかどうかを確認します。

`/opt/kaspersky/ksc64/sbin/ksnproxy` プロセスが実行されている場合、デバイス上のネットワークエージェントは Kaspersky Security Network に参加し、ディストリビューションポイントの範囲に含まれる管理対象デバイスの KSN プロキシサーバーとして機能します。

オンラインヘルプとオフラインヘルプの切り替え

インターネットにアクセスできない場合は、オフラインヘルプを使用できます。

オンラインヘルプとオフラインヘルプを切り替えるには：

1. Kaspersky Security Center のメインウィンドウで、コンソールツリーの［**Kaspersky Security Center 15.1**］を選択します。
2. ［**グローバルインターフェイス設定**］をクリックします。
   設定ウィンドウが表示されます。
3. 設定ウィンドウで、［**オフラインヘルプを使用**］をクリックします。
4. ［**OK**］をクリックします。

設定が適用され保存されます。必要に応じて、いつでも設定を元に戻し、オンラインヘルプの使用を開始できます。

SIEM システムへのイベントのエクスポート

このセクションでは、Kaspersky Security Center によって登録されたイベントを外部 SIEM（Security Information and Event Management）システムにエクスポートする方法について説明します。

シナリオ：SIEM システムへのイベントのエクスポートの設定

Kaspersky Security Center で設定可能な方法は次のいずれかです：Syslog 形式を使用する任意の SIEM システムへのエクスポート、LEEF 形式と CEF 形式を使用する QRadar、Splunk、ArcSight SIEM システムへのエクスポート、Kaspersky Security Center データベースからイベントを直接 SIEM システムへエクスポート。このシナリオを完了すると、管理サーバーはイベントを SIEM システムに自動的に送信します。

必須条件

Kaspersky Security Center でイベントのエクスポートの設定を開始する前に：

- イベントのエクスポート方法の詳細を参照してください。
- システムの設定値を確認してください。

このシナリオのステップは、任意の順序で実行できます。

イベントを SIEM システムにエクスポートするプロセスは、次の手順で構成されます：

- **Kaspersky Security Center からイベントを受信するように SIEM システムを設定する**

  手順：SIEM システムへのイベントのエクスポートの設定

- **SIEM システムにエクスポートするイベントの選択：**

  実行手順の説明：

  - 管理コンソール：Syslog 形式でエクスポートするカスペルスキー製品のイベントのマーキング、Syslog 形式でエクスポートする一般的なイベントのマーキング
  - Kaspersky Security Center Web コンソール：Syslog 形式でエクスポートするカスペルスキー製品のイベントのマーキング、Syslog 形式でエクスポートする一般的なイベントのマーキング

- **次のいずれかの方法を使用した、SIEM システムへのイベントのエクスポートの設定：**

  - TCP / IP、UDP、または TLS over TCP プロトコルの使用。

    実行手順の説明：

    - 管理コンソール：SIEM システムへのイベントのエクスポートの設定
    - Kaspersky Security Center Web コンソール：SIEM システムへのイベントのエクスポートの設定

  - Kaspersky Security Center データベースからのイベントの直接エクスポートを使用（データベースでは定義済みのパブリックビューのセットを使用できます。これらのパブリックビューの詳細については、「klakdb.chm のドキュメント」を参照してください）。

結果

SIEM システムへのイベントのエクスポートを構成した後、表示できます 結果のエクスポート エクスポートするイベントを選択した場合。

事前準備

Kaspersky Security Center 管理コンソールでイベントの自動エクスポートを設定する場合は、SIEM システム設定の一部を指定する必要があります。Kaspersky Security Center の設定を準備できるように、SIEM システムの設定を事前に確認しておいてください。

SIEM システムへのイベントの自動送信を正しく設定するには、次の設定の値を把握する必要があります：

- **SIEM システムサーバーアドレス**

  現在使用している SIEM システムがインストールされているサーバーの IP アドレスです。SIEM システム設定でこの値を確認してください。

- **SIEM システムサーバーのポート**

  Kaspersky Security Center と SIEM システムサーバー間の接続を確立するために使用するポート番号。Kaspersky Security Center の設定と SIEM システムのレシーバ設定でこの値を指定します。

- **プロトコル**

  Kaspersky Security Center から SIEM システムへのメッセージの送信に使われるプロトコル。Kaspersky Security Center の設定と SIEM システムのレシーバ設定でこの値を指定します。

Kaspersky Security Center のイベントについて

Kaspersky Security Center では、管理サーバーと管理対象デバイスにインストールされた他のカスペルスキー製品の動作中に発生したイベントの情報を受信できます。イベントに関する情報は管理サーバーデータベースに保存されます。この情報は外部 SIEM システムにエクスポートできます。イベント情報を外部 SIEM システムにエクスポートすると、SIEM システムの管理者は、管理対象デバイスまたは管理グループで発生したセキュリティシステムイベントに迅速に対処できます。

イベント種別

Kaspersky Security Center には、次のイベント種別があります：

- 一般イベント：管理対象となるカスペルスキー製品すべてで共通して発生するイベントです。一般イベントの例としては「ウイルスアウトブレイク」があります。一般イベントでは、構文と形式が厳密に定義されています。一般イベントは、レポートやダッシュボードなどで使用されます。
- 管理対象のカスペルスキー製品それぞれに固有のイベント：管理対象となるカスペルスキーの各製品には、独自のイベントのセットがあります。

イベントソース

イベントは、次の製品で生成される可能性があります：

- Kaspersky Security Center のコンポーネント：
  - 管理サーバー
  - ネットワークエージェント
  - iOS MDM サーバー
- 管理対象のカスペルスキー製品

  管理対象のカスペルスキー製品によって生成されるイベントの詳細は、該当する製品のドキュメントを参照してください。

製品によって生成されるイベントの完全なリストは、アプリケーションポリシーの［**イベントの設定**］タブで確認できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示できます。

イベントの重要度

各イベントには固有の重要度があります。発生した状況に応じて、イベントには様々な重要度が割り当てることができます。イベントの重要度には次の 4 つがあります：

- *緊急イベント*は、データの損失、誤動作、または重大なエラーを招きかねない重大な問題が発生したことを示すイベントです。

- *機能エラー*は、アプリケーションの動作中または手順の実行中に重大な問題、エラー、または誤動作の発生を示すイベントです。

- *警告*は、必ずしも重大ではなくても、将来問題が発生する可能性があることを示すイベントです。こうしたイベントの発生後、データや機能を失わずにアプリケーションを復元できるのであれば、ほとんどのイベントは警告を意味します。

- *情報*イベントは、操作が適切に完了したこと、アプリケーションが適切に動作していること、手順が完了したことを伝えるために発生するイベントです。

各イベントには保管期間が定義されており、保管期間中、ユーザーは Kaspersky Security Center でイベントを表示または変更することができます。一部のイベントは既定により、管理サーバーデータベースに保管されません。保管期間がゼロと定義されているためです。管理サーバーデータベースに 1 日以上保管されるイベントだけを外部システムにエクスポートできます。

イベントのエクスポートについて

イベントのエクスポートは、組織および技術レベルでセキュリティ問題に対処し、セキュリティ監視サービスを提供し、各種ソリューションからの情報を統合できる、一元化されたシステム内で使用できます。これらは SIEM システムで、ネットワークのハードウェアとアプリケーション、またはセキュリティオペレーションセンター（SOC）によって生成されたセキュリティアラートとイベントをリアルタイムで分析します。

これらのシステムは、ネットワーク、セキュリティ、サーバー、データベース、アプリケーションなど多くのソースからのデータを受信します。SIEM システムは、重要なイベントを見逃すことがないように、監視対象データを統合する機能も提供します。さらに、緊急のセキュリティ問題を管理者に通知するために、相互に関連するイベントとアラートの分析を自動的に実行します。アラートはダッシュボードから発することも、メールなどのサードパーティのチャネルから送信することもできます。

Kaspersky Security Center から外部 SIEM システムにイベントをエクスポートするプロセスには、イベントの送信元である Kaspersky Security Center とイベントのレシーバである SIEM システムの 2 つが関係します。イベントを正常にエクスポートするには、SIEM システムと Kaspersky Security Center 管理コンソールの両方で設定する必要があります。どちらを先に設定してもかまいません。Kaspersky Security Center 管理コンソールからのイベントの送信を設定してから、SIEM システムによるイベントの受信を設定することも、逆の順序で設定することもできます。

Kaspersky Security Center からのイベントの送信方法

Kaspersky Security Center から外部システムにイベントを送信する方法は 3 つあります：

- Syslog 形式を使用して任意の SIEM システムにイベントを送信

  Syslog プロトコルを使用すると、Kaspersky Security Center 管理サーバーおよび管理対象デバイスにインストールされたカスペルスキー製品で発生したイベントはすべてリレーできます。Syslog プロトコルは、標準メッセージロギングプロトコルです。任意の SIEM システムへのイベントのエクスポートに使用可能です。

  この目的のために、SIEM システムに転送するイベントをマークする必要があります。イベントは、管理コンソールまたは Kaspersky Security Center Web コンソールでマークできます。マークされたイベントのみが SIEM システムに転送されます。何もマークしなかった場合、イベントは転送されません。

- CEF 形式と LEEF 形式を使用して、QRadar システム、Splunk システム、ArcSight システムにイベントを送信

CEF プロトコルと LEEF プロトコルを使用すると、一般イベントをエクスポートできます。CEF プロトコルと LEEF プロトコル経由でイベントをエクスポートする場合、エクスポートする特定のイベントを選択することはできません。代わりに、一般イベントがすべてエクスポートされます。Syslog プロトコルとは異なり、CEF プロトコルと LEEF プロトコルは汎用的なプロトコルではありません。CEF プロトコルと LEEF プロトコルは、対応する一部の SIEM システム（QRadar、Splunk、ArcSight）用です。そのため、これらの形式のいずれかを使用してイベントをエクスポートする場合は、必要なパーサーを SIEM システム内で使用します。

- Kaspersky Security Center のデータベースから直接、任意の SIEM システムにエクスポート

  このイベントのエクスポート方法では、SQL クエリを使用して、データベースのパブリックビューから直接イベントを受信できます。クエリの結果は XML ファイルに保存されるため、外部システムへの入力データとして使用できます。パブリックビューにあるイベントだけをデータベースから直接エクスポートできます。

SIEM システムによるイベントの受信

SIEM システムは、Kaspersky Security Center からイベントを受信して適切に解析する必要があります。これらの目的に対応できるように、SIEM システムを適切に設定する必要があります。設定は、利用する具体的な SIEM システムによります。ただし、レシーバとパーサーの設定など、すべての SIEM システムの設定で一般的なステップがいくつかあります。

SIEM システムでのイベントのエクスポートの設定について

Kaspersky Security Center から外部 SIEM システムにイベントをエクスポートするプロセスには、イベントの送信元である Kaspersky Security Center とイベントのレシーバである SIEM システムの 2 つが関係します。イベントのエクスポートは、SIEM システムと Kaspersky Security Center 管理コンソールの両方で設定する必要があります。

SIEM システムで指定する設定は、使用している個々のシステムにより異なります。一般に、すべての SIEM システムでレシーバを設定する必要があり、受信イベントを解析するためのメッセージパーサーを任意で設定します。

レシーバの設定

Kaspersky Security Center から送信されたイベントを受信するには、SIEM システムでレシーバを設定する必要があります。一般に、SIEM システムで次の設定を指定する必要があります：

- **エクスポートのプロトコルまたは入力の種別**

  これはメッセージ転送プロトコルで、TCP/IP または UDP のいずれかになります。このプロトコルは、Kaspersky Security Center で指定したプロトコルと同じにする必要があります。

- **ポート**

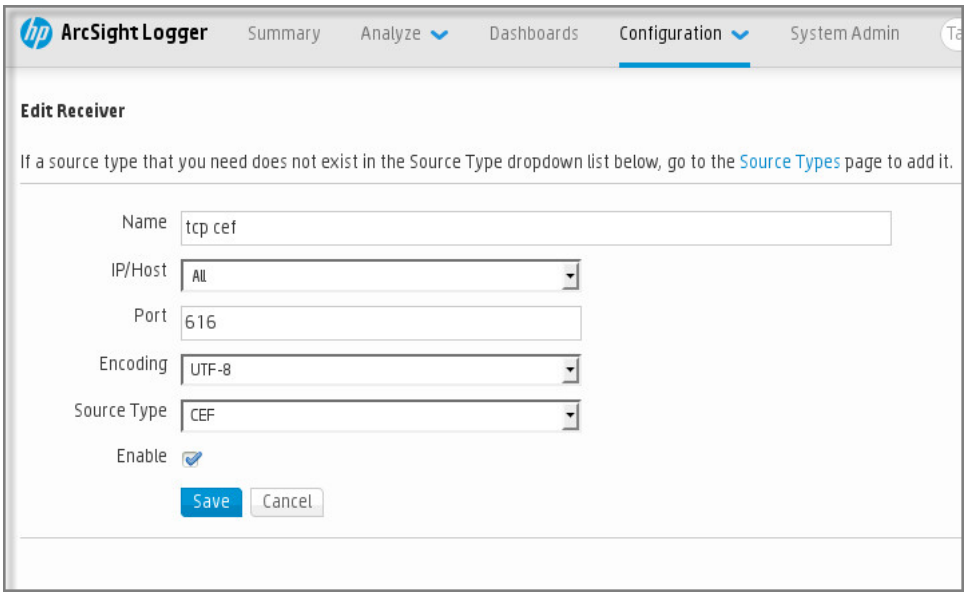
  Kaspersky Security Center に接続するポート番号。このポートは、Kaspersky Security Center で指定したポートと同じにする必要があります。

- **メッセージのプロトコルまたはソースの種別**

SIEM システムへのイベントのエクスポートに使われるプロトコル。標準プロトコルの Syslog、CEF、または LEEF のいずれかを指定できます。SIEM システムは、指定のプロトコルに従ってメッセージパーサーを選択します。

使用する SIEM システムによっては、受信者の設定を一部追加で指定する必要があります。

次の図は、ArcSight の受信者のセットアップ画面を示します。



ArcSight でのレシーバのセットアップ

メッセージパーサー

エクスポートされたイベントはメッセージとして SIEM システムに渡されます。SIEM システムでイベントに関する情報が利用できるように、これらのメッセージを適切に解析する必要があります。メッセージパーサーは SIEM システムの一部です。イベントの ID、深刻度、説明、パラメータなど関連フィールドにメッセージの内容を分けるために使用します。メッセージの内容を分けることで、SIEM システムは Kaspersky Security Center から受信したイベントを処理して、SIEM システムデータベースに保管することができます。

Syslog 形式で SIEM システムにエクスポートするイベントのマーキング

イベントの自動エクスポートを有効にしたら、外部 SIEM システムにエクスポートするイベントを選択する必要があります。

次の条件のいずれかに基づいて、外部システムへの Syslog 形式でのイベントのエクスポートを設定できます：

- 一般的なイベントのマーキング。イベントの設定または管理サーバーの設定でエクスポートするイベントをポリシー内でマークすると、特定のポリシーで管理されているすべてのアプリケーションで発生した選択済みのイベントが SIEM システムに送信されます。エクスポートされたイベントがポリシー内で選択されている場合、このポリシーで管理されている個別アプリケーションの当該イベントを再定義することはできません。

- 管理対象アプリケーションのイベントのマーキング。管理対象デバイスにインストールされた管理対象アプリケーションへエクスポートするイベントをマークすると、そのアプリケーションで発生したイベントのみが SIEM システムに送信されます。

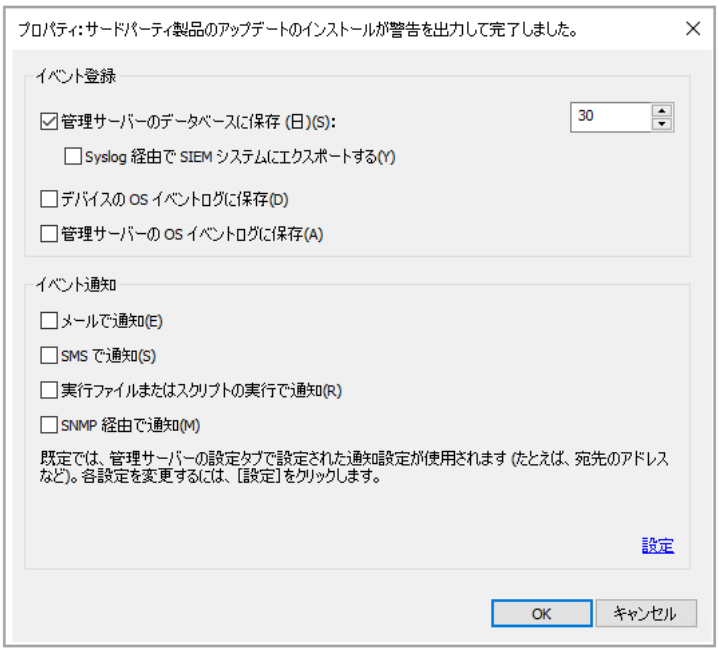
Syslog 形式でエクスポートするカスペルスキー製品のイベントのマーキング

管理対象デバイスにインストールされた管理対象アプリケーションで発生したイベントをエクスポートする場合は、そのアプリケーションのエクスポート対象のイベントをマークします。以前エクスポートしたイベントをポリシー内でマークした場合は、そのポリシーの管理対象である個別のアプリケーションのマークしたイベントを再定義することはできません。

個別の管理対象アプリケーションからエクスポートするイベントをマークするには：

1. Kaspersky Security Center のコンソールツリーで、［**管理対象デバイス**］フォルダーを選択して、［**デバイス**］タブに移動します。
2. 目的のデバイスを右クリックしてコンテキストメニューを開いて、［**プロパティ**］を選択します。
3. デバイスのプロパティウィンドウが開いたら、［**アプリケーション**］セクションを選択します。
4. アプリケーションのリストが表示されたら、イベントをエクスポートする必要があるアプリケーションを選択して、［**プロパティ**］をクリックします。
5. アプリケーションのプロパティウィンドウで［**イベントの設定**］セクションを選択します。
6. イベントのリストが表示されたら、SIEM システムにエクスポートする必要のあるイベントを 1 つ以上選択して、［**プロパティ**］をクリックします。
7. 表示されるイベントのプロパティウィンドウで、［**Syslog 経由で SIEM システムにエクスポートする**］をオンにして、Syslog 形式でエクスポートするために選択したイベントをマークします。Syslog 形式でエクスポートするために選択したイベントのマークを解除するには、［**Syslog 経由で SIEM システムにエクスポートする**］をオフにします。

イベントのプロパティがポリシーで定義されている場合、このウィンドウのフィールドを編集することはできません。



イベントのプロパティウィンドウ

8. ［**OK**］をクリックして変更内容を保存します。

9. アプリケーションのプロパティウィンドウとデバイスのプロパティウィンドウで［**OK**］をクリックします。

マークしたイベントが Syslog 形式で SIEM システムに送信されます。［**Syslog 経由で SIEM システムにエクスポートする**］をオフにしたイベントは、SIEM システムにエクスポートされません。自動エクスポートを有効にし、エクスポートするイベントを選択すると、エクスポートがすぐに開始されます。Kaspersky Security Center からイベントを確実に受信できるように SIEM システムを設定します。

Syslog 形式でエクスポートする一般的なイベントのマーキング

特定のポリシーによって管理されているすべてのアプリケーションで発生したイベントをエクスポートする場合は、エクスポートするイベントをポリシー内でマークします。その場合、個別の管理対象アプリケーションのイベントは選択できません。

SIEM システムにエクスポートする一般的なイベントをマークするには：

1. Kaspersky Security Center のコンソールツリーで、［**ポリシー**］フォルダーを選択します。

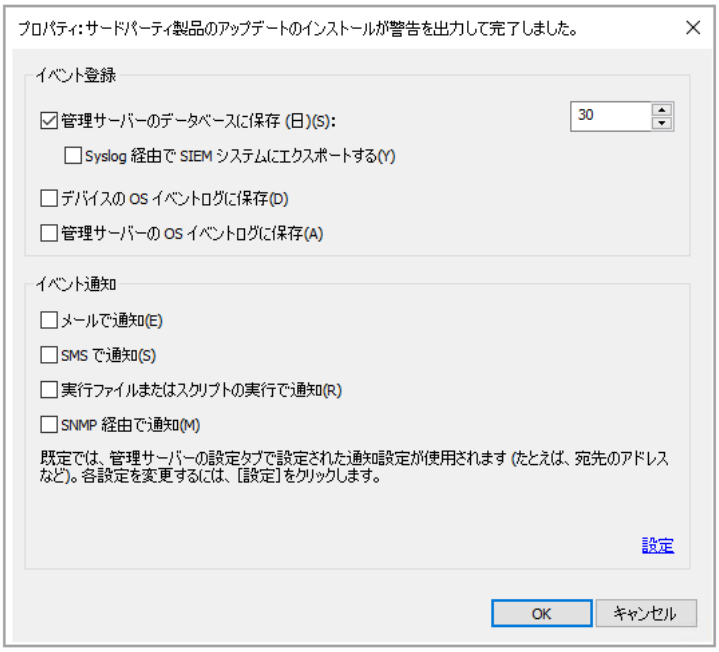
2. 目的のポリシーを右クリックしてコンテキストメニューを開いて、［**プロパティ**］を選択します。

3. ポリシーのプロパティウィンドウが開いたら、［**イベントの設定**］セクションを選択します。

4. イベントのリストが表示されたら、SIEM システムにエクスポートする必要のあるイベントを 1 つ以上選択して、［**プロパティ**］をクリックします。

   すべてのイベントを選択する必要がある場合は、［**すべて選択**］をクリックします。

5. 表示されるイベントのプロパティウィンドウで、［**Syslog 経由で SIEM システムにエクスポートする**］をオンにして、Syslog 形式でエクスポートするために選択したイベントをマークします。Syslog 形式でエクスポートするために選択したイベントのマークを解除するには、［**Syslog 経由で SIEM システムにエクスポートする**］をオフにします。



管理サーバーのイベントのプロパティウィンドウ

6. ［**OK**］をクリックして変更内容を保存します。

7. ポリシーのプロパティウィンドウで［**OK**］をクリックします。

マークしたイベントが Syslog 形式で SIEM システムに送信されます。［**Syslog 経由で SIEM システムにエクスポートする**］をオフにしたイベントは、SIEM システムにエクスポートされません。自動エクスポートを有効にし、エクスポートするイベントを選択すると、エクスポートがすぐに開始されます。Kaspersky Security Center からイベントを確実に受信できるように SIEM システムを設定します。

Syslog 形式を使用したイベントのエクスポートについて

Syslog 形式を使用すると、管理サーバー、管理対象デバイスにインストールされた他のカスペルスキー製品で発生したイベントを SIEM システムにエクスポートできます。

Syslog は標準メッセージロギングプロトコルです。メッセージを生成するソフトウェア、メッセージを保管するシステム、メッセージを報告、分析するソフトウェアを分けることができます。各メッセージには、メッセージを生成したソフトウェアの種別を示す機能コードのラベルが付けられ、重要度が割り当てられます。

Syslog 形式は、インターネット技術タスクフォース（インターネット標準）によって公開されている RFC（Request for Comments）の文書で定義されています。Kaspersky Security Center から外部システムへのイベントのエクスポートには、RFC 5424 標準が使用されます。

Kaspersky Security Center で、Syslog 形式を使用して外部システムにイベントがエクスポートされるように設定できます。

エクスポートのプロセスは次の 2 つのステップで構成されます：

1. イベントの自動エクスポートの有効化。このステップでは、イベントを SIEM システムに送信するように Kaspersky Security Center を設定します。自動エクスポートを有効にすると、Kaspersky Security Center は即座にイベントの送信を開始します。

2. 外部システムにエクスポートするイベントの選択。このステップでは、SIEM システムにエクスポートするイベントを選択します。

CEF 形式および LEEF 形式を使用したイベントのエクスポート

CEF プロトコルと LEEF プロトコルを使用すると、一般イベントおよびカスペルスキー製品から管理サーバーに送信されたイベントを SIEM システムにエクスポートできます。エクスポートするイベントのセットは事前定義されており、エクスポートするイベントを選択することはできません。

使用している SIEM システムを基にエクスポート形式を選択します。次の表は、SIEM システムおよび対応するエクスポート形式を示します。

SIEM システムへのイベントのエクスポートに使用する形式

SIEM システム	エクスポート形式
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF（ログイベント拡張フォーマット） - IBM Security QRadar SIEM 用にカスタマイズされたイベント形式。QRadar は LEEF イベントを統合、識別、処理できます。LEEF イベントは UTF-8 文字コードを使用する必要があります。LEEF プロトコルの詳細については、IBM Knowledge Center を参照してください。

- CEF（Common Event Format） - 様々なセキュリティとネットワークのデバイス、アプリケーションからのセキュリティ関連情報の相互運用性を改善するオープンログ管理標準。CEF により、共通のイベントログ形式を使用できるため、データを容易に統合して集約し、企業用管理システムで分析できます。CEF イベントは UTF-8 文字コードを使用する必要があります。

自動エクスポートを使用する場合、Kaspersky Security Center から SIEM システムに一般イベントが送信されます。イベントの自動エクスポートは、有効にすると即座に開始されます。このセクションでは、イベントの自動エクスポートを有効にする方法について詳細に説明します。

イベントを SIEM システムにエクスポートするための Kaspersky Security Center の設定

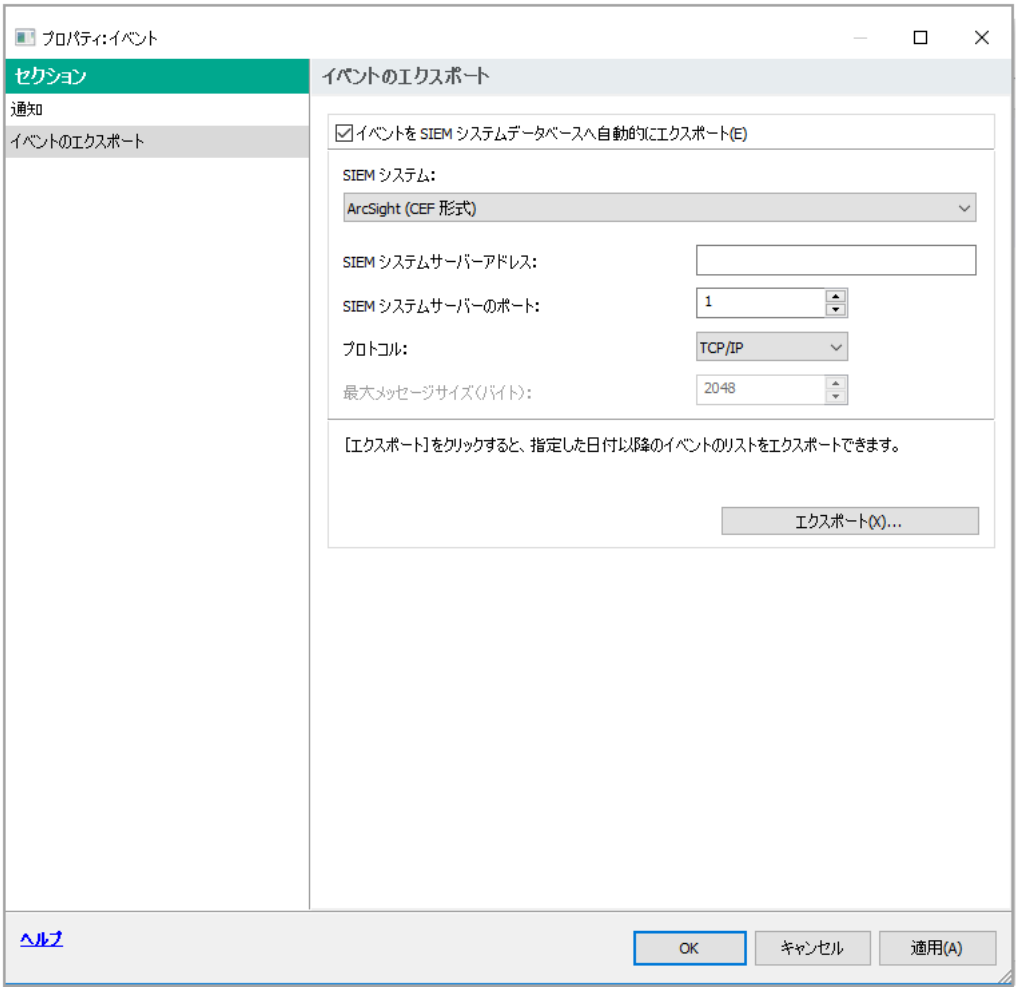
Kaspersky Security Center でイベントの自動的なエクスポートを有効にできます。

管理対象アプリケーションから CEF 形式および LEEF 形式でエクスポート可能なイベントは一般イベントのみです。アプリケーション固有のイベントは、管理対象アプリケーションから CEF 形式および LEEF 形式でエクスポートできません。管理対象アプリケーションのイベントまたは管理対象アプリケーションのポリシーを使用して設定されたカスタムイベントをエクスポートするには、イベントを Syslog 形式でエクスポートする必要があります。

イベントの自動的なエクスポートを有効にするには：

1. Kaspersky Security Center のコンソールツリーで、イベントをエクスポートする管理サーバーを選択します。
2. 選択した管理サーバーの作業領域で、［**イベント**］タブを選択します。
3. ［**通知とイベントのエクスポートの設定**］に隣接するドロップダウン矢印をクリックして、ドロップダウンリストから［**SIEM システムへのエクスポートの設定**］を選択します。

   イベントのプロパティウィンドウが開き、［**イベントのエクスポート**］セクションが表示されます。
4. ［**イベントのエクスポート**］セクションで、次のエクスポート設定を指定します：



イベントのプロパティウィンドウの［イベントのエクスポート］セクション

- **イベントを SIEM システムデータベースへ自動的にエクスポート**

  このチェックボックスをオンにすると、SIEM システムへのイベントの自動エクスポートが有効になります。このチェックボックスをオンにすると、［**イベントのエクスポート**］セクションのすべてのフィールドが有効になります。

- **SIEM システム**

  イベントをエクスポートする SIEM システムを選択します：QRadar®（LEEF 形式）、ArcSight（CEF 形式）、Splunk®（CEF 形式）、Syslog 形式（RFC 5424）。

- **SIEM システムサーバーアドレス**

  SIEM システムサーバーアドレスを指定します。アドレスは、DNS または NetBIOS 名または IP アドレスとして指定できます。

- **SIEM システムサーバーのポート**

  SIEM システムサーバーへの接続用のポート番号を指定します。このポート番号は、SIEM システムがイベントの受信に使用するポートと同じにする必要があります（詳細については、「SIEM システムの設定」のセクションを参照）。

- **プロトコル**

メッセージを SIEM システムに送信するために使用するプロトコルを選択します。TCP/IP、UDP、TCP プロトコルのいずれかを選択できます。

TLS over TCP プロトコルを選択した場合は、次の TLS 設定を指定します：

- **SIEM サーバー認証**

  次のいずれかの方法を選択して、SIEM システムサーバーを認証します：

  - **CA 証明書を使用**：信頼できる証明書認証局（CA）から証明書のリストを含むファイルを受け取り、ファイルを Kaspersky Security Center にアップロードできます。Kaspersky Security Center は、SIEM システムサーバーの証明書も CA によって署名されているかどうかを確認します。

    信頼できる証明書を追加するには、［**参照**］をクリックして、証明書をアップロードします。

    ［**CA 証明書を使用**］をオンにする場合、［**サーバー証明書の発行先（任意）**］にサブジェクト名を指定できます。*サブジェクト名*は、証明書を受け取るドメインの名前です。SIEM システムサーバーのドメイン名が SIEM システムサーバー証明書のサブジェクト名と一致しない場合、Kaspersky Security Center は SIEM システムサーバーに接続できません。ただし、証明書内でサブジェクト名を変更すると、SIEM システムサーバーによりドメイン名が変更されることがあります。これを行うには、サブジェクト名を［**サーバー証明書の発行先（任意）**］に指定します。指定されたサブジェクト名のいずれかが SIEM システム証明書のサブジェクト名と一致する場合、Kaspersky Security Center は SIEM システムサーバー証明書を検証します。

  - **サーバー証明書の SHA1 サムプリントを使用**：SIEM システム証明書の SHA-1 サムプリントを Kaspersky Security Center で指定できます。SHA-1 サムプリントを追加するには、オプションの下のフィールドに入力します。

- **クライアント認証**

  クライアント認証用に、自身の証明書を挿入するか、Kaspersky Security Center で生成することができます。

  - **Insert certificate**：CA など、任意の発行元から受け取った証明書を使用できます。既存の証明書を挿入するには、［**証明書の参照**］をクリックします。表示された［**証明書**］ウィンドウで、次のいずれかの証明書の種別を選択して、証明書と秘密鍵を指定します：

    - **X.509 証明書**：秘密鍵が含まれるファイルを［**秘密鍵 (*.prk, *.pem)**］にアップロードし、証明書が含まれるファイルを［**証明書 (*.cer)**］にアップロードします。これを行うには、対応するフィールドの右側にある［**参照**］をクリックし、必要なファイルを追加します。両方のファイルは相互に依存せず、ファイルを読み込む順序は重要ではありません。両方のファイルをアップロードしたら、秘密鍵をデコードするためのパスワードを［**パスワード**］に指定します。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

    - **PKCS #12 コンテナー**：証明書と秘密鍵を含む単一のファイルを［**証明書ファイル**］にアップロードします。これを行うには、フィールドの右側にある［**参照**］をクリックし、必要なファイルを追加します。ファイルをアップロードしたら、秘密鍵をデコードするためのパスワードを［**パスワード**］に指定します。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

  - **Generate key**：Kaspersky Security Center で自己署名証明書を生成できます。［**証明書の生成**］をクリックし、［**発行先**］にサブジェクト名を入力します。このサブジェクト名に対してクライアント証明書が生成され、この証明書のSHA-1サムプリントが［**クライアント証明書の SHA1 サムプリント**］に表示されます。Kaspersky Security Center は生成された自己署名証明書を保存し、証明書の公開部分または SHA-1 サムプリントを SIEM システムに渡すことができます。

Syslog 形式を選択する場合は、次を指定する必要があります：

- **最大メッセージサイズ（バイト）**

  SIEM システムにリレーされた 1 つのメッセージの最大サイズ（バイト）を指定します。各イベントは 1 つのメッセージでリレーされます。メッセージの実際の長さが指定の値を上回る場合、メッセージは切り捨てられて、データが失われる可能性があります。既定のサイズは 2048 バイトです。［**SIEM システム**］で Syslog 形式を選択した場合にだけ、このフィールドを使用できます。

5. 過去の指定した日付を経過した後に発生したイベントを SIEM システムデータベースにエクスポートする場合は、［**エクスポート**］をクリックして、イベントをエクスポートする開始日を指定します。既定では、イベントのエクスポートは、エクスポートを有効にするとすぐに開始されます。

6. ［**OK**］をクリックします。

イベントの自動エクスポートが有効になります。

イベントの自動エクスポートを有効にしたら、SIEM システムにエクスポートするイベントを選択します。

データベースからのイベントの直接エクスポート

Kaspersky Security Center インターフェイスを使わなくても、Kaspersky Security Center のデータベースから直接イベントを取得できます。パブリックビューに対して直接クエリを実行してイベントデータを取得することも、既存のパブリックビューを基に独自のビューを作成して、必要なデータを取得するようにアドレス指定することもできます。

パブリックビュー

Kaspersky Security Center のデータベースには、パブリックビューの便利なセットをご用意しています。これらのパブリックビューの詳細は、klakdb.chm のドキュメントを参照してください。

v_akpub_ev_event パブリックビューには、データベース内のイベントパラメータを表す一連のフィールドが含まれています。klakdb.chm ドキュメントには、デバイス、アプリケーション、ユーザーなど、他の Kaspersky Security Center のエンティティに対応するパブリックビューに関する情報も含まれています。この情報はクエリに使用できます。

このセクションでは、klsql2 ユーティリティを使って SQL クエリを作成する手順について説明し、クエリの例を示します。

SQL クエリまたはデータベースビューを作成する時には、データベースと連携する他のプログラムも使用できます。Kaspersky Security Center のデータベースへの接続に必要なインスタンス名やデータベース名などのパラメータの表示方法についても、該当セクションを参照してください。

klsql2 ユーティリティを使用した SQL クエリの作成

この記事では、klsql2 ユーティリティをダウンロードして使用する方法、このユーティリティを使用して SQL クエリを作成する方法について説明します。

klsql2 ユーティリティを使用するには：

1. Kaspersky Security Center のインストールフォルダーから klsql2 ユーティリティを配置します。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。Kaspersky Security Center の古いバージョン向けの klsql2 ユーティリティバージョンは使用しないでください。

2. 任意のテキストエディターで src.sql ファイルを作成し、そのファイルをユーティリティと同じフォルダーに配置します。

3. 必要な SQL クエリを src.sql ファイルに入力して、ファイルを保存します。

4. Kaspersky Security Center 管理サーバーがインストールされたデバイスで、次のコマンドをコマンドラインに入力して、src.sql ファイルから SQL クエリを実行し、結果を result.xml ファイルに保存します：
   `klsql2 -i src.sql -u <ユーザー名> -p <パスワード> -o result.xml`
   <ユーザー名>と<パスワード>は、定義データベースにアクセスできるユーザーアカウントの資格情報です。

5. 必要に応じて、データベースにアクセスできるユーザーアカウントのログインとパスワードを入力してください。

6. 新しく作成されたファイル result.xml を開いて、SQL クエリ結果を確認します。

ファイル src.sql を編集して、パブリックビューに対する任意の SQL クエリを作成することができます。次に、コマンドラインから SQL クエリを実行して、結果をファイルに保存します。

klsql2 ユーティリティでの SQL クエリの例

このセクションでは、klsql2 ユーティリティによって作成された SQL クエリの例を示します。

次の例では、過去 7 日間にデバイスで発生したイベントを取得し、発生した順にイベントを表示します。イベントは新しい順から表示されます。

例：

```
SELECT
e.nId, /* イベントの識別子 */
e.tmRiseTime, /* イベントが発生した時間 */
e.strEventType, /* イベント種別の内部名 */
e.wstrEventTypeDisplayName, /* イベント種別の表示名 */
e.wstrDescription, /* イベントについて表示される説明 */
e.wstrGroupName, /* デバイスが配置されているグループの名前 */
h.wstrDisplayName, /* イベントが発生したデバイスの表示名 */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* イベントが発生したデバイスの IP アドレス */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Kaspersky Security Center データベース名の表示

たとえば、SQL クエリを送信し、SQL スクリプトエディターからデータベースに接続する必要がある場合は、データベース名を知っておくと役立ちます。

Kaspersky Security Center のデータベースの名前を表示するには：

1. Kaspersky Security Center のコンソールツリーで、［**管理サーバー**］フォルダーのコンテキストメニューを開いて、［**プロパティ**］を選択します。

2. 管理サーバーのプロパティウィンドウにある［セクション］ペインで、［**詳細**］→［**現在のデータベースの詳細**］の順に選択します。

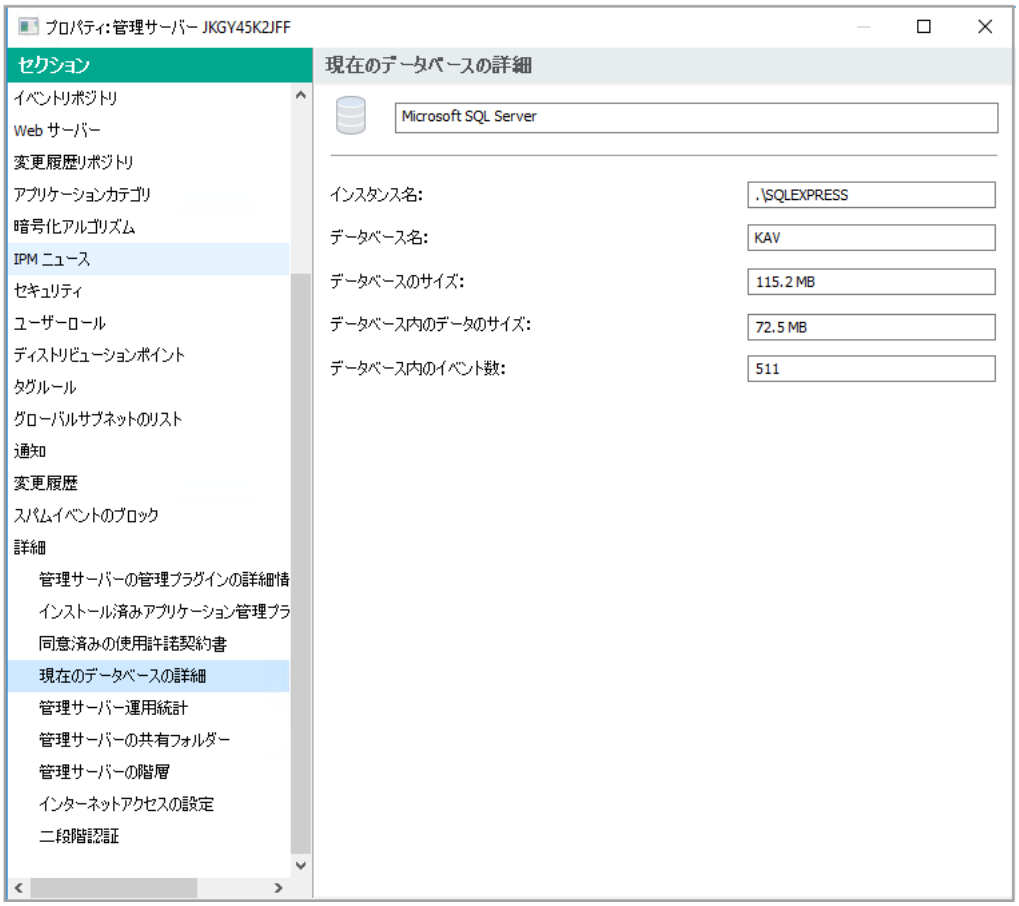
3. ［**現在のデータベースの詳細**］セクションで、次のデータベースプロパティを確認します（次の図を参照）：

   - **インスタンス名**

     現在の Kaspersky Security Center のデータベースのインスタンスの名前。既定値は *.\KAV_CS_ADMIN_KIT* です。

   - **データベース名**

     Kaspersky Security Center の SQL データベースの名前。既定値は *KAV* です。



現在の管理サーバーデータベースに関する情報があるセクション。

4. ［**OK**］をクリックして、管理サーバーのプロパティウィンドウを閉じます。

このデータベース名を使用して、SQL クエリ内のデータベースのアドレスを指定します。

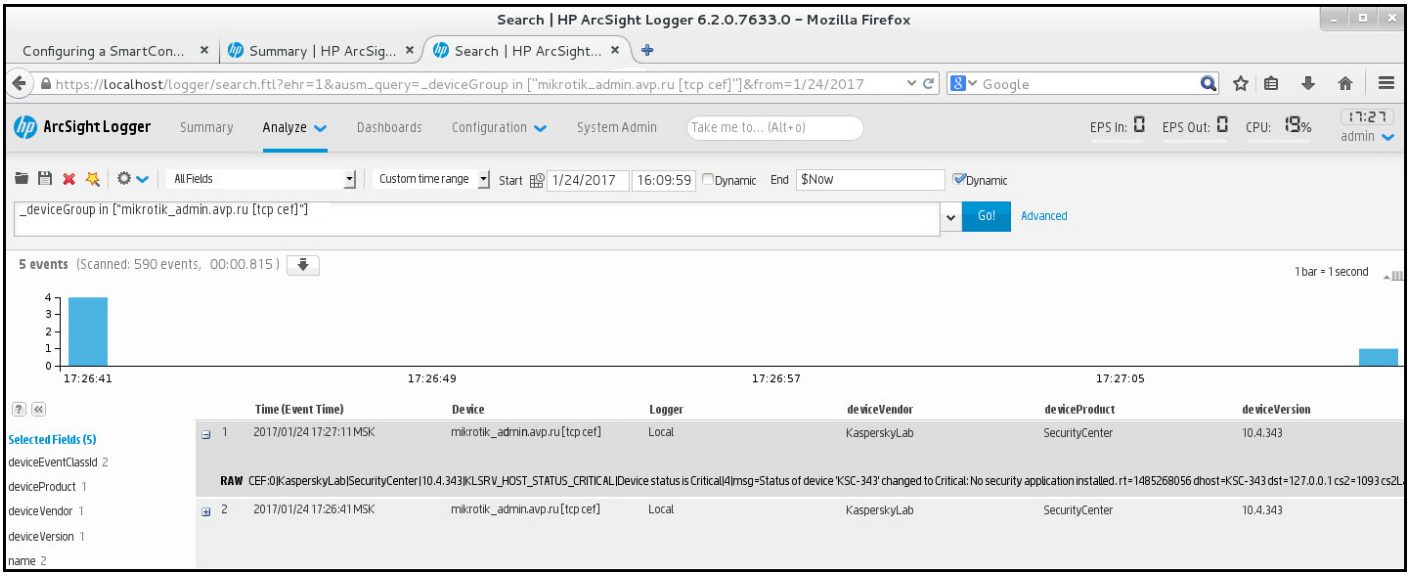
エクスポート結果の表示

イベントのエクスポート手順が正常に完了するようにコントロールすることができます。それには、イベントのエクスポートとともにメッセージが SIEM システムで受信されているかどうかを確認します。

Kaspersky Security Center から送信されたイベントが SIEM システムで受信され、適切に解析されている場合、設定は両者で適切に行われています。イベントが受信されない場合は、Kaspersky Security Center で指定した設定を SIEM システムの設定と比べて確認してください。

次の図は、ArcSight にエクスポートされたイベントを示します。たとえば、最初のイベントは重大な管理サーバーイベントです：「*デバイスのステータスが「緊急」です。*」

エクスポートされたイベントの SIEM システムでの表示は、使用している SIEM システムによって異なります。



イベントの例

サードパーティ製品への統計の送信を目的とした SNMP の使用

このセクションでは、Windows で SNMP（Simple Network Management Protocol）を使用して管理サーバーから情報を取得する方法について説明します。Kaspersky Security Center には、OID を使用して管理サーバーのパフォーマンスに関する統計情報をサイドアプリケーションに転送する SNMP エージェントが含まれています。

このセクションでは、Kaspersky Security Center で SNMP の使用中に発生する可能性のある問題の解決に関する情報も提供します。

Kaspersky Security Center で使用するための SNMP サービスの設定

このセクションでは、SNMP（Simple Network Management Protocol）を使用して管理サーバーから情報を取得するために、Windows 上で SNMP サービスを設定する方法について説明します。

Windows では、SNMP のサポートは既定で無効です。

Windows で SNMP サポートを有効にするには：

1. **コントロールパネル**に移動します。
2. ［**プログラムの追加と削除**］メニューを開きます。
3. ［**Windows の機能の有効化または無効化**］をクリックします。
4. Windows の機能リストで、SNMP 機能に移動し、［**OK**］をクリックします。
5. ［**コントロールパネル**］→［**管理ツール**］→［**サービス**］の順に選択します。
6. **SNMP サービス**を選択して実行します。
7. 標準の UDP ポートについて、`netstat` でテストしてリスニングが機能するかどうかを確認します。

SNMP サポートは Windows で有効になっています。

Windows で SNMP サービスを設定するには：

1. Kaspersky Security Center の［**SNMP エージェント**］コンポーネントが、通常のインストールまたはサイレントインストール中にインストールされていることを確認してください。
2. **SNMP サービス**および **SNMP トラップ** Windows サービスが実行されていることを確認してください。
3. システムに ManageEngine MIB ブラウザーがインストールされていることを確認してください。
4. **SNMP サービス**のプロパティの［**セキュリティ**］タブで、次の権限を持つ 2 つのコミュニティを追加します：

コミュニティ	権限
カスペルスキー	通知する
`public`	読み取り / 書き込み

5. ［**これらのホストからの SNMP パケットを受け入れる**］フィールドに、ManageEngine MIB ブラウザーがインストールされているデバイスの IP アドレスを追加します。たとえば、10.10.10.105 です。
6. ［**トラップ**］タブの［**コミュニティ名**］フィールドに「`kaspersky`」と入力します。
7. ［**OK**］をクリックして、変更内容を保存し、サービスのプロパティウィンドウを閉じます。
8. ManageEngine MIB ブラウザーで、Kaspersky Security Center のインストールフォルダーから adminkit.mib ファイルをロードします。既定では、ファイル adminkit.mib は <ディスク>:\Program Files\Kaspersky Lab\Kaspersky Security Center\snmp フォルダーにあります。
9. ManageEngine MIB ブラウザーウィンドウの［**ホスト**］フィールドに、Kaspersky Security Center 管理サーバーがインストールされているデバイスの IP アドレスを追加します。

SNMP サービスは、SNMP（Simple Network Management Protocol）を使用して管理サーバーから情報を取得するように設定されています。

SNMP エージェントとオブジェクト識別子

Kaspersky Security Center では、SNMP エージェントはダイナミックライブラリ `klsnmpag.dll` として実装されます。これは、管理サーバーのインストール中にインストーラーによって登録されます。SNMP エージェントは、`snmp.exe` プロセス（つまり Windows サービス）内で機能します。サードパーティ製品は、SNMP を使用して、管理サーバーのパフォーマンスに関する統計情報（カウンターの形式で提供されます）を受信します。

各カウンターには、一意の*オブジェクト識別子*（「OID」とも表記）があります。オブジェクト識別子とは、ドットで区切られた一連の数値です。管理サーバーのオブジェクト識別子は、1.3.6.1.4.1.23668.1093 プレフィックスで始まります。カウンターの OID は、このプレフィックスにカウンターを記述するサフィックスをつなげたものです。たとえば、OID の値 1.3.6.1.4.1.23668.1093.1.1.4 のカウンターは 1.1.4 のサフィックスを持ちます。

システムの状態を監視するために Zabbix のような SNMP クライアントを使用できます。情報を取得するには、情報に対応する OID の値を検索して SNMP クライアントにその値を入力できます。そうすると SNMP クライアントはシステムの状態を示す別の値を返します。

カウンターとカウンタータイプのリストは、管理サーバーの `adminkit.mib` ファイルにあります。*MIB* は Management Information Base の略です。カウンター値の要求および表示を目的として設計されている MIB ビューアーアプリケーションを介して、`.mib` ファイルをインポートおよび解析できます。

オブジェクト識別子からの文字列カウンター名の取得

サードパーティ製品への情報の転送にオブジェクト識別子（OID）を使用するには、その OID から文字列カウンター名を取得する必要があります。

OID から文字列カウンター名を取得するには：

1. 管理サーバーにある `adminkit.mib` ファイルをテキストエディターで開きます。
2. 最初の値を説明するネームスペースを（左から右に）特定します。

   たとえば、サフィックス 1.1.4 の OID の場合、`"counters" (::= { kladminkit 1 })` の可能性があります。
3. 2 番目の値を説明するネームスペースを探します。

   たとえば、サフィックス 1.1.4 の OID の場合、`counters 1` の可能性があります。これは `deployment` を意味します。
4. 3 番目の値を説明するネームスペースを探します。

   たとえば、サフィックス 1.1.4 の OID の場合、`deployment 4` の可能性があります。これは `hostsWithAntivirus` を意味します。

文字列カウンター名はこれらの値を連結したもので、たとえば `<MIB base namespace>.counters.deployment.hostsWithAntivirus` となり、値は 1.3.6.1.4.1.23668.1093.1.1.4 の OID に対応します。

SNMP 用のオブジェクト識別子の値

次の表は、管理サーバーのパフォーマンスに関する情報をサードパーティ製品に転送するために使用されるオブジェクト識別子（「OID」とも表記）の値と説明を示しています。

SNMP 用のオブジェクト識別子の値と説明

オブジェクト識別子の値	数値のデータ型	OID	説明

DeploymentStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.1.1	展開ステータス。ステータスは次のいずれかです： • **情報**：N 台のデバイスのライセンスが有効ではなくなった。 • **警告**：次のいずれか： 管理サーバーグループのデバイス合計 N 台のうち、カスペルスキー製品がインストールされたデバイスが M 台ある（N > M）。 ライセンス L が N 台のデバイスで M 日以内に有効期限が終了する。 N 台のデバイスでアプリケーションのインストールのタスク T が正常に完了し、M 台のデバイスで再起動が必要である。 • **緊急**：N 台のデバイスのライセンスの有効期限が終了した。 • **OK**：上記のどれでもない。
noAntivirusSoftware	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.1	理由 deploymentStatus は、管理対象製品がインストールされていないデバイスが管理サーバーグループに多すぎることを示しています。 管理対象製品がインストールされていないデバイスがいくつか見つかった場合は値が 1 になり、それ以外の場合は 0 になります。
remoteInstallTaskFailed	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.2	理由 deploymentStatus は、リモートインストールのタスクが一部のデバイスで失敗したことを示しています。これらのデバイスの数は hostsRemoteInstallFailed を介して取得できます。
licenceExpiring	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.3	理由 deploymentStatus は、7 日以内にライセンスの有効期限が終了するデバイスがいくつかあることを示しています。これらのデバイスの数は hostsLicenseExpiring を介して取得できます。
licenceExpired	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.4	理由 deploymentStatus は、ライセンスの有効期限が終了したデバイスがいくつかあることを示しています。これらのデバイスの数は hostsLicenseExpired を介して取得できます。
hostsInGroups	Counter32	.1.3.6.1.4.1.23668.1093.1.1.3	管理サーバーグループ内のデバイスの数。
hostsWithAntivirus	Counter32	.1.3.6.1.4.1.23668.1093.1.1.4	管理対象製品がインストールされている管理サーバーグループ内のデバイスの数。
hostsRemoteInstallFailed	Counter32	.1.3.6.1.4.1.23668.1093.1.1.5	リモートインストールのタスクが失敗したデバイスの数。
licenceExpiringSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.6	まもなく（7日以内に）有効期限が終了するライセンスの ID。
licenceExpiredSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.7	有効期限が終了したライセンスの ID。
licenceExpiringDays	Unsigned32	.1.3.6.1.4.1.23668.1093.1.1.8	ライセンスの有効期限が終了するまでの日数。このパラメータでは、有効期限までの残り日数が 7 日未満の場合、ライセンス期間は期限切れと判断されます。 有効期限までの残り日数が 7 日を超えている場合、値は 0 になります。
hostsLicenceExpiring	Counter32	.1.3.6.1.4.1.23668.1093.1.1.9	まもなく（7日以内に）ライセンスの有効期限が終了するデバイスの数。
hostsLicenceExpired	Counter32	.1.3.6.1.4.1.23668.1093.1.1.10	ライセンスの有効期限が終了したデバイスの数。
updateStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	定義データベースの現在のアップデートステータス。ステータスは次のいずれかです： • **情報**：管理サーバーまたはデバイス上の定義データベースが 1 日以上アップデートされておらず、アプリケーションのインストールから 1 日未満が経過しています。 • **警告**：管理サーバーまたはデバイス上の定義データベースが 3 日以上アップデートされていません。この値はグループ設定で変更できます。

			• **緊急**：管理サーバーまたはデバイス上の定義データベースが 7 日以上アップデートされていません。この値はグループ設定で変更できます。 • **OK**：上記のどれでもない。
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	この理由は、管理サーバーが長期間にわたって更新されなかったことを示しています。長期間と判断される時間は updatesStatus に指定されています。
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	この理由は、一部のデバイスが長期間にわたって（既定で**緊急**の場合は 7 日以上、**警告**の場合は 3 日）更新されなかったことを示しています。これらのデバイスの数は hostsNotUpdated を介して取得できます。
lastServerUpdateTime	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.2.3	管理サーバーでの定義データベースの最終更新日時。
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	長期間アップデートされていないアンチウイルスベースを含むデバイスの数（既定で**緊急**場合は 7 日以上、**警告**の場合は 3 日）。更新ステータスが**緊急**のデバイスがある場合は、それらのデバイスのみがカウントされます。更新ステータスは、 updatesStatus から取得できます。
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	リアルタイム保護のステータス。次のいずれか： • **警告**：次のいずれか： 管理サーバーグループに属するデバイスでセキュリティ侵害が検出された。 暗号化のエラーにより、一部のデバイスで保護ステータスが変更された。 フルスキャンを長期間実行していない。 • **緊急**：管理サーバーグループの一部のデバイスでアンチウイルスによる保護が機能していない。 • **OK**：上記のどれでもない。
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	この理由は、一部のデバイスでセキュリティ製品が実行されていないことを示しています。これらのデバイスの数は hostsAntivirusNotRunning を介して取得できます。
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	この理由は、一部のデバイスでリアルタイム保護が実行されていないことを示しています。これらのデバイスの数は hostsRealtimeNotRunning を介して取得できます。
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	この理由は、駆除されていないオブジェクトが含まれているデバイスがあることを示しています。これらのデバイスの数は hostsNotCuredObject を介して取得できます。
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	この理由は、一部のデバイスで脅威が見つかったことを示しています。これらのデバイスの数は hostsTooManyThreats を介して取得できます。
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	この理由は、システムのウイルスアウトブレイクステータスを示しています。 特定の期間内に特定の数のウイルスが検知された場合は値が 1 になり、それ以外の場合は 0 になります。ウイルスの数と期間の長さは、管理サーバーで ウイルス攻撃の設定を使用して指定します。
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	セキュリティ製品が実行されていないデバイスの数。
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	リアルタイム保護が実行されていないデバイスの数。
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	リアルタイム保護が許容されるレベルではないデバイスの数。
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	駆除されていないオブジェクトが含まれるデバイスの数。
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	脅威が含まれるデバイスの数。
fullscanStatus	INTEGER { ok(0),	.1.3.6.1.4.1.23668.1093.1.4.1	アンチウイルスのフルスキャンのステータス。次のいずれか：

	info(1), warning(2), critical(3) }		• **情報**：アプリケーションのインストールから 7 日未満。 • **警告**：アプリケーションのインストールから 7 日以上にわたってアンチウイルスフルスキャンが実行されていない。 • **緊急**：アプリケーションのインストールから 14 日以上にわたってアンチウイルスフルスキャンが実行されていない。 • **OK**：上記のどれでもない。
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	この理由は、一部のデバイスが一定期間スキャンされていないことを示しています。これらのデバイスの数は hostsNotScannedLately を介して取得できます。期間の長さは fullScanStatus に指定されています。
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	一定期間にわたってスキャンされていないデバイスの数。期間の長さは fullScanStatus に指定されています。
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	管理サーバーの論理ネットワークのステータス。次のいずれか： • **警告**：アクセスできない警告ステータスのデバイスがある場合、またはどの管理サーバーグループにも属していないデバイスがある場合。 • **緊急**：管理サーバーによる制御が失われたデバイスがある場合、または緊急ステータスのデバイスがあり、アクセスできない場合。 • **OK**：上記のどれでもない。
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	この理由は、一部のデバイスが長期間にわたって（**警告**ステータスのデバイスの場合は 7 日以上、**緊急**ステータスのデバイスの場合は 4 日）管理サーバーに接続されていないことを示しています。これらのデバイスの数は hostsNotConnectedLongTime を介して取得できます。
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	この理由は、管理サーバーによる制御が失われたデバイスがあることを示しています。これらのデバイスの数は hostsControlLost を介して取得できます。
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	管理サーバーによって検出され、どの管理サーバーグループにも属していないデバイスの数。
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	管理サーバーのグループの数。
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	長期間にわたって管理サーバーに接続されていないデバイスの数。長期間と判断される時間は notConnectedLongTime に指定されています。
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	管理サーバーによって制御されていないデバイスの数。
eventsStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.6.1	イベントサブシステムのステータス。次のいずれか： • **警告**：次のいずれか： 管理サーバーグループのデバイスが長期間にわたって Windows Update を検索していない。 ステータスに問題のあるデバイスがある。 • **緊急**：次のいずれか： 少なくとも 1 つのデバイスに重要度が「緊急」のイベントがある。 少なくとも 1 つのデバイスに重要度が「エラー」のイベントがある。 少なくとも 1 つのデバイスに、タスクが正常に完了していないイベントがある。 管理サーバーグループのデバイスが長期間にわたって Windows Update を検索していない。 ステータスに問題のあるデバイスがある。 • **OK**：上記のどれでもない。

criticalEventOccured	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.6.2.1	理由 eventsStatus は、管理サーバーにいくつかの緊急イベントがあることを示しています。これらのイベントの数は criticalEventsCount を介して取得できます。 いずれかのデバイスに少なくとも 1 つの緊急イベントがある場合は値が 1 になり、それ以外の場合は 0 になります。
criticalEventsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.6.3	管理サーバーでの緊急イベントの数。

トラブルシューティング

このセクションでは、SNMP サービスの使用中に発生する可能性がある一般的な問題の一部について解決策を説明します。

サードパーティ製品が SNMP サービスに接続できない

SNMP サービスがインストールされ、［Kaspersky Security Center で使用するための SNMP サービスの設定］セクションの説明に従って設定されていることを確認してください。

SNMP サービスは機能していますが、サードパーティ製品が値を取得できません

SNMP エージェントのトレースを許可し、空ではないファイルが作成されていることを確認します。これは、SNMP エージェントが適切に登録され、機能していることを意味します。その後、サイドサービスの設定で、SNMP サービスからの接続を許可します。サイドサービスが SNMP エージェントと同じホストで動作する場合、IP アドレスのリストに、そのホストの IP アドレスまたは `loopback 127.0.0.1` のいずれかが含まれている必要があります。

エージェントと通信する SNMP サービスは、Windows で実行されている必要があります。regedit を使用して、Windows レジストリで SNMP エージェントのパスを指定できます。

- Windows 10の場合：
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
- WindowsVista および Windows Server 2008 の場合：
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

regedit を介して SNMP エージェントのトレースを許可することもできます。

- 32 ビットシステム：
  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug
- 64 ビットシステム：
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Deb
  "TraceLevel"=dword:00000004
  "TraceDir"="C:\\"

値が管理コンソールのステータスと一致しない

管理サーバーでの負荷を軽減するために、SNMP エージェントに値のキャッシュが実装されています。実現されるキャッシュと管理サーバーで変更される値の間のレイテンシーにより、SNMP エージェントによって返される値と実際の値の間に不一致が生じる可能性があります。サードパーティ製品を使用する場合は、レイテンシーが発生する可能性を考慮に入れる必要があります。

クラウド環境での利用

このセクションでは、Amazon Web Services、Microsoft Azure、および Google Cloud のクラウド環境での Kaspersky Security Center の導入とメンテナンスについて説明しています。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

アップデート機能（ウイルス対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

クラウド環境での利用について

Kaspersky Security 15.1 はオンプレミスのデバイスに対して使用できるだけでなく、クラウド環境で使用できる特別な機能を備えています。Kaspersky Security Center は次の仮想マシンと連携します：

- Amazon EC2 インスタンス（以降、*インスタンス*とも表記）。Amazon EC2 インスタンスとは、AWS（Amazon Web Services）プラットフォームで作成された仮想マシンを指します。Kaspersky Security Center は AWS *API*（アプリケーションプログラミングインターフェイス）を使用します。
- Microsoft Azure 仮想マシン。Kaspersky Security Center は Azure API を使用します。
- Google Cloud 仮想マシンインスタンス。Kaspersky Security Center は Google API を使用します。

Kaspersky Security Center をインスタンスまたは仮想マシンに導入して、クラウド環境内のデバイスの保護を管理し、Kaspersky Security Center の特別な機能をクラウド環境での作業に使用できます。次のような機能があります：

- API ツールを使用して、クラウド環境のデバイスをポーリングする
- API ツールを使用して、ネットワークエージェントとセキュリティ製品をクラウド環境のデバイスにインストールする
- 特定のクラウドセグメントに属しているかどうかに応じてデバイスを検索する

Kaspersky Security Center 管理サーバーが導入されたインスタンスまたは仮想マシンを使用して、オンプレミスのデバイスを保護することもできます（たとえば、クラウドサーバーの方が物理サーバーよりも維持やメンテナンスがしやすいことが判明した場合）。そのような場合は、管理サーバーがオンプレミスのデバイスにインストールされている場合と同じように管理サーバーで作業を行います。

AWS の有料 AMI（Amazon Machine Image）または Azure の月単位の従量課金 SKU から導入された Kaspersky Security Center では、脆弱性とパッチ管理（SIEM システムとの連携を含む）は自動的にアクティベートされますが、モバイルデバイス管理はアクティベートできません。

管理サーバーは、管理コンソールと一緒にインストールされます。管理サーバーのインストール先のデバイスに Kaspersky Security for Windows Server も自動的にインストールされます。

クラウド環境での作業の詳細を考慮して、クラウド環境設定ウィザードで Kaspersky Security Center を設定できます。

シナリオ：クラウド環境への導入

このセクションでは、Amazon Web Services、Microsoft Azure、Google Cloud などのクラウド環境での稼働を目的として Kaspersky Security Center を導入することについて説明します。

この導入シナリオが完了すると、Kaspersky Security Center 管理サーバーと管理コンソールが起動し、既定のパラメータが指定されます。Kaspersky Security Center で管理されるアンチウイルスによる保護が、選択した Amazon EC2 インスタンスまたは Microsoft Azure 仮想マシンに導入されます。その後、Kaspersky Security Center の設定の微調整、管理グループの複雑な構造の作成、各種のポリシーやタスクの作成などが可能です。

クラウド環境での稼働を目的として Kaspersky Security Center を導入する際の手順は次の通りです：

1. 準備作業
2. 管理サーバーの導入
3. 保護が必要な仮想マシンにカスペルスキー製品をインストールする
4. アップデートのダウンロードの設定
5. デバイスの保護ステータスに関するレポートの管理の設定

クラウド環境設定ウィザードは、初期設定を実行するためのものです。Kaspersky Security Center が初めて設定済みのイメージから展開されると、自動的に開始します。このウィザードは、いつでも手動で開始できます。さらに、このウィザードが実行するすべての操作を、手動で実行することができます。

クラウド環境への Kaspersky Security Center 管理サーバーの導入には、少なくとも 1 時間を、クラウド環境への保護の導入には、少なくとも 1 営業日を割り当てることを推奨します。

クラウド環境への Kaspersky Security Center の導入は、以下の手順で進みます：

1 クラウドセグメントの構成の計画

Kaspersky Security Center がクラウド環境でどのように動作するかを資料で確認します。管理サーバーの導入先（クラウド環境の内外）を決定します。また、保護するクラウドセグメントの数を決定します。管理サーバーをクラウド環境の外に導入する場合、または 5,000 台を超えるデバイスを保護する場合は、管理サーバーを手動でインストールする必要があります。

Google Cloud を使用する場合、管理サーバーのインストールは手動でのみ実行できます。

2 リソース計画

導入に必要な項目をすべて準備できていることを確認します。

3 設定済みイメージとして提供されている Kaspersky Security Center の利用登録を行う

AWS Marketplace で設定済み AMI の 1 つを選択するか Azure Marketplace で月単位の従量課金の SKU を選択し、必要な場合は各マーケットプレイスの規則に従って支払いを行います（BYOL 方式の使用時には支払いは不要です）。イメージを使用して、Kaspersky Security Center がインストールされた状態の Amazon EC2 インスタンスまたは Microsoft Azure 仮想マシンを導入します。

このステップは、管理サーバーをクラウド環境内のインスタンスまたは仮想マシンに導入し、5000 台以下のデバイスを保護する場合にのみ必要です。それ以外の場合、このステップは必要ありません。代わりに、管理サーバー、管理コンソール、DBMS を手動でインストールする必要があります。

この手順は Google Cloud の場合は実行できません。

4 DBMS の配置場所の選定

DBMS の配置場所を決定します。

クラウド環境外のデータベースを使用する場合は、使用可能なデータベースが準備されていることを確認します。

Amazon Relational Database Service（RDS）を使用する場合は、AWS クラウド環境で RDS を使用してデータベースを作成します。

Microsoft Azure SQL DBMS を使用する場合は、Microsoft Azure クラウド環境で Azure Database サービスを使用してデータベースを作成します。

Google MySQL を使用する場合は、Google Cloud にデータベースを作成します（詳細は、https://cloud.google.com/sql/docs/mysql を参照してください）。

5 管理サーバー、管理コンソール（Microsoft 管理コンソールベース、Web ベースの管理コンソール、またはその両方）を指定したデバイスに手動でインストール

Kaspersky Security Center の主要なインストールシナリオに従って、管理サーバー、管理コンソール、DBMS を指定したデバイスにインストールします。

このステップは、管理サーバーをクラウド環境外に導入する場合、または 5,000 台を超えるデバイスを保護する場合に必要です。次に、管理サーバーがハードウェア要件を満たしていることを確認します。それ以外の場合、このステップは必要ありません。AWS Marketplace、Azure Marketplace または Google Cloud で設定済みイメージとして提供されている Kaspersky Security Center の利用登録を行うだけで十分です。

6 管理サーバーがクラウド API を使用する権限を持っていることの確認

AWS で AWS 管理コンソールに移動し、IAM ロールまたは IAM ユーザーアカウントを作成します。作成した IAM ロール（または IAM ユーザーアカウント）によって、Kaspersky Security Center が AWS API を使用してクラウドセグメントのポーリングと保護の導入を実行します。

Azure を使用する場合、サブスクリプション、アプリケーション ID、パスワードを作成します。Kaspersky Security Center がこれらの認証情報で Azure API を使用してクラウドセグメントのポーリングと保護の導入を実行します。

Google Cloud で、プロジェクトを登録し、プロジェクト ID と秘密鍵を取得します。Kaspersky Security Center が Google API でこれらの認証情報を使用してクラウドセグメントのポーリングを実行します。

7 保護対象インスタンス用の IAM ロールの作成（AWS のみ）

AWS 管理コンソールで、AWS へのリクエストを実行するための一連の権限を定義する IAM ロールを作成します。このロールは、後で新規インスタンスに割り当てます。アプリケーションのインスタンスへのインストールに Kaspersky Security Center を使用するには、IAM ロールが必要です。

8 Amazon RDS（リレーショナルデータベースサービス）または Microsoft Azure SQL を使用したデータベースの準備

Amazon RDS の使用を計画している場合は、Amazon RDS データベースと、データベースのバックアップを保存する S3 バケットを作成します。管理サーバーをインストールするのと同じ EC2 インスタンス上にデータベースを配置する場合、またはデータベースを AWS 以外の場所に配置する場合は、この手順をスキップできます。

Microsoft Azure SQL の使用を計画している場合は、Microsoft Azure でストレージアカウントとデータベースを作成します。

Google MySQL を使用する場合は、Google Cloud にデータベースを作成します（詳細は、https://cloud.google.com/sql/docs/mysql を参照してください）。

9 クラウド環境を使用するための Kaspersky Security Center ライセンス

Kaspersky Security Center をクラウド環境で使用するためのライセンスを保有していることを確認し、アクティベーションコードまたはライセンス情報ファイルを確実に製品のライセンス保管領域に追加します。この段階はクラウド環境の設定で完了させることができます。

このステップは、BYOL モデルに基づく無料の設定済み AMI からインストールされた Kaspersky Security Center を使用する場合、または AMI を使用せず手動で Kaspersky Security Center をインストールする場合に必要です。これらの場合、Kaspersky Security Center をアクティベートするには、Kaspersky Security for Virtualization または Kaspersky Hybrid Cloud Security のライセンスが必要です。

使用準備済みイメージからインストールした Kaspersky Security Center を使用している場合は、この段階は必要なく、クラウド環境設定ウィザードの該当ウィンドウは表示されません。

⑩ クラウド環境での認証

Kaspersky Security Center に AWS、Azure または Google Cloud の認証情報を入力し、Kaspersky Security Center が必要な権限を付与された状態で動作できるようにします。この段階は、クラウド環境での認証中に完了することができます。

⑪ 管理サーバーがクラウドセグメントのデバイスに関する情報を受信できるように、クラウドセグメントをポーリングする

クラウドセグメントのポーリングを開始します。AWS 環境では、Kaspersky Security Center は、IAM ロールまたは IAM ユーザーの権限に基づいてアクセス可能なすべてのインスタンスのアドレスと名前を受信します。Microsoft Azure 環境では、Kaspersky Security Center は、「Reader」ロールの権限に基づいてアクセス可能なすべての仮想マシンのアドレスと名前を受信します。

その後、Kaspersky Security Center を使用してカスペルスキー製品と他社製ソフトウェアを、検出されたインスタンスまたは仮想マシンにインストールできます。

Kaspersky Security Center によって定期的にポーリングが開始されるため、新しいインスタンスまたは仮想マシンが自動的に検出されます。

⑫ すべてのネットワークデバイスをクラウド管理グループにまとめる

検出されたインスタンスまたは仮想マシンを［**管理対象デバイス**］の［**クラウド**］管理グループに移動し、一元管理できるようにします。たとえば、インストールされているオペレーティングシステムに応じてデバイスをサブグループに割り当てる場合は、［**管理対象デバイス**］の［**クラウド**］グループ内に複数の管理グループを作成できます。定期ポーリング中に検出されるすべてのデバイスの［**管理対象デバイス**］の［**クラウド**］グループへの自動移動を有効にすることができます。

⑬ ネットワークエージェントを使用しネットワークデバイスを管理サーバーに接続する

クラウド環境のデバイスにネットワークエージェントをインストールします。ネットワークエージェントは、デバイスと管理サーバー間の通信を確立する Kaspersky Security Center コンポーネントです。ネットワークエージェントは自動的に設定されるようになっています。

ネットワークエージェントを各デバイスのローカルにインストールすることができます。Kaspersky Security Center を使用して、ネットワークエージェントをリモートでデバイスにインストールすることもできます。または、この手順をスキップして、最新バージョンのセキュリティ製品と一緒にネットワークエージェントをインストールすることもできます。

⑭ 最新バージョンのセキュリティ製品をネットワークデバイスへインストールする

セキュリティ製品をインストールするデバイスを選択し、対象デバイスに最新バージョンのセキュリティ製品をインストールします。インストールは、管理サーバー上の Kaspersky Security Center を使用してリモートで、またはローカルで実行できます。

これらのプログラム用のインストールパッケージを手動で作成する必要がある場合があります。

Kaspersky Endpoint Security for Linux は、Linux を実行するインスタンスおよび仮想マシン用です。

Kaspersky Security for Windows Server は、Windows を実行するインスタンスおよび仮想マシン用です。

⑮ アップデートを設定する

［**脆弱性と必要なアップデートの検出**］タスクは、クラウド環境の設定の実行時に自動作成されます。タスクの手動作成もできます。このタスクによって、必要なアプリケーションのアップデートが検出およびダウンロードされ、続いて Kaspersky Security Center ツールを使用してネットワークデバイスにインストールされます。

クラウド環境設定が完了したら、次のステップを完了させることを推奨します：

1. **レポート管理の設定**

   ［**監視**］タブ（［**管理サーバー**］フォルダーの作業領域にある）でレポートを表示できます。メールでレポートを受信することもできます。レポートは［**監視**］タブであらかじめ表示できるようになっています。メールでのレポート受信を設定するには、レポートを受信するメールアドレスを指定し、レポートの形式を設定します。

結果

シナリオの手順が完了したら、初期設定が正常に完了して次の状況が実現していることを確認してください：

- 管理コンソールまたは Kaspersky Security Center Web コンソールを使用して管理サーバーに接続できる。
- 最新バージョンのカスペルスキー製品が管理対象デバイスにインストールされ、動作している。
- すべての管理対象デバイスに対して、Kaspersky Security Center で既定のポリシーとタスクが作成されている。

Kaspersky Security Center をクラウド環境に導入する場合の前提条件

Amazon Web Services または Microsoft Azure のクラウド環境への Kaspersky Security Center の導入を開始する前に、次の項目が準備できていることを確認します。

- インターネットアクセス
- 次のアカウントのいずれか：
  - Amazon Web Services アカウント（AWS で使用する場合）
  - Microsoft アカウント（Azure で使用する場合）
  - Google アカウント（Google Cloud で使用する場合）
- 次のいずれか：
  - Kaspersky Security for Virtualization のライセンス
  - Kaspersky Hybrid Cloud Security のライセンス
  - 該当のライセンスを購入する予算（Kaspersky Security for Virtualization または Kaspersky Hybrid Cloud Security）
  - 月額制サービスを利用する予算
- Kaspersky Endpoint Security for Linux と Kaspersky Security for Windows Server の最新バージョンのガイド

クラウド環境での管理サーバーのハードウェア要件

クラウド環境での導入の場合、管理サーバーとデータベースサーバーの要件は、物理管理サーバーの要件と同じです（管理するデバイスの数によって異なります）。詳細については、クラウド環境のドキュメントを参照してください。

クラウド環境で利用できるライセンスオプションについて

クラウド環境での使用は、Kaspersky Security Center の基本機能の範囲外なので、専用のライセンスが必要です。

クラウド環境で利用できる Kaspersky Security Center のライセンスオプションとして次の 2 種類が提供されています。

- 有料 AMI（Amazon Web Services） / 月単位の従量課金の SKU（Microsoft Azure）

  このオプションでは、Kaspersky Security Center のライセンスだけでなく Kaspersky Endpoint Security for Linux と Kaspersky Security for Windows Server のライセンスも提供されます。使用するクラウド環境の規則に従って料金を支払う必要があります。

  この方式では、管理サーバー 1 台で 200 台以内のクライアントデバイスを管理できます。

- 無料の設定済みイメージを BYOL（Bring Your Own License：ライセンス持ち込み）方式で専用ライセンスを使用して導入

  AWS または Azure 環境での Kaspersky Security Center のライセンス使用には、次のいずれかの製品のライセンスが必要です：

  - Kaspersky Security for Virtualization
  - Kaspersky Hybrid Cloud Security

  BYOL 方式では、管理サーバー 1 台で 100,000 台までのクライアントデバイスを管理できます。また、この方式では AWS、Azure または Google のクラウド環境外のデバイスも管理できます。

  次のような状況では、BYOL 方式の利用を選択できます：

  - Kaspersky Security for Virtualization の有効なライセンスを既に保有している。
  - Kaspersky Hybrid Cloud Security の有効なライセンスを既に保有している。
  - Kaspersky Security Center の導入直前にライセンスを購入予定である。

  初期セットアップの段階でアクティベーションコードまたはライセンス情報ファイルの提供を要求されます。

  BYOL を選択する場合は、Kaspersky Security Center の料金を Azure Marketplace または AWS Marketplace で支払う必要はありません。

どちらの場合も、脆弱性とパッチ管理は自動的にアクティベートされますが、モバイルデバイスサポートはアクティベートできません。

Kaspersky Hybrid Cloud Security のライセンスを使用して、クラウド環境のサポート機能をアクティベートしようとすると、エラーが発生する場合があります。

Kaspersky Security Center の定額制サービスでの利用を開始すると、Kaspersky Security Center 管理サーバーがインストールされた Amazon EC2（Amazon Elastic Compute Cloud）インスタンスまたは Microsoft Azure 仮想マシンが利用できます。Kaspersky Security for Windows Server と Kaspersky Endpoint Security for Linux のインストールパッケージは管理サーバーで利用できます。これらの製品をクラウド環境のデバイスへインストールできます。ライセンス情報ファイルやアクティベーションコードの利用は必要ありません。

管理対象デバイスが管理サーバーの側から 1 週間以上可視でない場合、デバイス上のアプリケーション（Kaspersky Security for Windows Server または Kaspersky Endpoint Security for Linux）は、機能制限モードに移行します。アプリケーションを再度アクティベートするには、アプリケーションがインストールされたデバイスを管理サーバーの側でもう一度可視になるようにする必要があります。

クラウド環境で利用できるデータベースの構成

Kaspersky Security Center で使用できるデータベースが必要です。AWS、Microsoft Azure、または Google Cloud に Kaspersky Security Center を導入する場合は、3 つの選択肢があります。

- 管理サーバーと同じデバイスにローカルデータベースを作成する。Kaspersky Security Center には SQL Server Express が付属し、最大で 5000 台の管理対象デバイスをサポートできます。SQL Server Express Edition で必要を満たせる場合は、このオプションを選択します。
- AWS クラウド環境の RDS（Relational Database Service）または Microsoft Azure クラウド環境の Azure データベースサービスを使用して、データベースを作成する。SQL Express 以外の DBMS を使用したい場合はこのオプションを選択します。データはクラウド環境に転送されて保存され、そこでの追加費用は発生しません。Kaspersky Security Center をオンプレミスで使用しており、データベースにデータが保存されている場合、新しいデータベースにデータを移すことができます。

  Google Cloud Platform で動作させる場合は、Cloud SQL for MySQL のみを使用できます。
- 既存のデータベースサーバーを使用する。既に使用しているデータベースサーバーがあり、Kaspersky Security Center でこれを使用する場合はこのオプションを選択します。このデータベースサーバーがクラウド環境外にある場合、データはインターネット経由で転送されるため、追加費用が発生する可能性があります。

Kaspersky Security Center のクラウド環境への導入手順では、データベースの作成または選択を行うステップが設けられています。

Amazon Web Services クラウド環境での利用

このセクションでは、Amazon Web Services で Kaspersky Security Center を使用するための準備について説明します。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

Amazon Web Services クラウド環境での使用について

Kaspersky Security Center は AWS Marketplace で AMI（Amazon Machine Image）の形で購入できます。AMI は、事前設定された仮想マシンの使用準備済みイメージです。有料 AMI またはライセンス持ち込みの BYOL AMI を登録することができ、そのイメージを基に、Kaspersky Security Center 管理サーバーがインストールされた状態の Amazon EC2 インスタンスを作成できます。

AWS プラットフォームを使用し、特に AWS Marketplace でアプリを購入してインスタンスを作成するには、Amazon Web Services のアカウントが必要です。無料のアカウントを https://aws.amazon.com/jp/ で作成できます。既存の Amazon アカウントも使用できます。

AWS Marketplace にある AMI を登録する場合は、すぐに使用できる Kaspersky Security Center とともにインスタンスが届きます。自分でアプリケーションをインストールする必要はありません。その場合、Kaspersky Security Center 管理サーバーは、ユーザーが何もしなくてもインスタンスにインストールされます。インストール後、管理コンソールを起動して管理サーバーに接続し、Kaspersky Security Center の操作を開始できます。

AMI、および AWS Marketplace の仕組みの詳細については、AWS Marketplace Help ページにアクセスしてください。AWS プラットフォームでの作業、インスタンスの使用、関連する概念の詳細については、Amazon Web Services のドキュメントを参照してください。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

Amazon EC2 インスタンスで IAM ロールと IAM ユーザーアカウントを作成する

このセクションでは管理サーバーを正常に動作させるために必要な手順について説明します。具体的な操作としては、AWS IAM（ID およびアクセス管理）ロールとユーザーアカウントの操作が含まれます。また、クライアントデバイスにネットワークエージェントをインストールしてから、Kaspersky Security for Windows Server や Kaspersky Endpoint Security for Linux をインストールするために必要なクライアントデバイスでの手順についても説明します。

Kaspersky Security Center 管理サーバーが AWS を使用する権限を持っているかどうかの確認

Amazon Web Services クラウド環境の標準的な運用方法は、規定により、特別な IAM ロールが管理サーバーのインスタンスに割り当てられ、AWS サービスを使用します。IAM ロールは、IAM のエンティティであり、AWS サービスに対する実行リクエストに必要な権限を定義しています。IAM ロールには、クラウドのセグメントへのポーリング、およびインスタンスへのアプリケーションのインストールの権限があります。

IAM ロールを作成し、管理サーバーに割り当てた後、このロールを使用してインスタンスの保護を導入できるようになります。その他の追加の情報は Kaspersky Security Center に提供されません。

しかしながら、以下の場合は、管理サーバー用の IAM ロールを作成しないことを推奨します：

- 保護の管理を計画しているデバイスが、Amazon Web Services クラウド環境内にある EC2 インスタンスであるが、管理サーバーはその環境の外にある場合。

- 自分のクラウドのセグメント内だけではなく、AWS の他のアカウントで作成された別のクラウドのセグメント内でも保護の管理を計画している場合。この場合、IAM ロールは、自分のクラウド環境に対してのみ必要となります。別のクラウドのセグメントに対しては、IAM ロールは不要です。

これらの場合、IAM ロールの作成ではなく、Kaspersky Security Center で使用する *IAM ユーザーアカウント*を作成し、AWS サービスを使用する必要があります。管理サーバーでの作業開始前に、IAM ユーザーアカウントおよび対応する *AWS IAM アクセスキー*（以降、*IAM アクセスキー*とも表記）を作成します。

IAM ロールまたは IAM ユーザーアカウントの作成には、AWS 管理コンソールが必要です。AWS 管理コンソールを使用するには、AWS のアカウントのユーザー名とパスワードが必要です。

管理サーバー用の IAM ロールの作成

管理サーバーの導入前に、AWS 管理コンソール内で、インスタンスへのアプリケーションのインストールに必要な権限を持った IAM ロールを作成します。詳細については、IAM ロールに関する AWS ヘルプを参照してください。

管理サーバー用の IAM ロールを作成するには：

1. AWS 管理コンソールを開いて、AWS アカウントでログインします。
2. ［**ロール**］セクションで、次の権限を持つロールを作成します：
   - **AmazonEC2ReadOnlyAccess**（クラウドセグメントのポーリングのみを実行し、AWS API を使用して EC2 インスタンスにアプリケーションをインストールしない場合）。
   - **AmazonEC2ReadOnlyAccess**、**AmazonSSMFullAccess**（クラウドセグメントのポーリングを実行し、AWS API を使用して EC2 インスタンスにアプリケーションをインストールする場合）。この場合、AmazonEC2RoleforSSM 権限を持つ IAM ロールを保護対象の EC2 インスタンスに割り当てることも必要になります。

このロールを、管理サーバーとして使用する EC2 インスタンスに割り当てる必要があります。

新しく作成されたロールは、管理サーバー上のすべてのアプリケーションに適用されます。そのため、管理サーバー上で実行されるどのアプリケーションも、クラウドセグメントへのポーリング、またはクラウドセグメント内の EC2 インスタンスへのアプリケーションのインストールが実行可能です。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

Kaspersky Security Center で使用する IAM ユーザーアカウントの作成

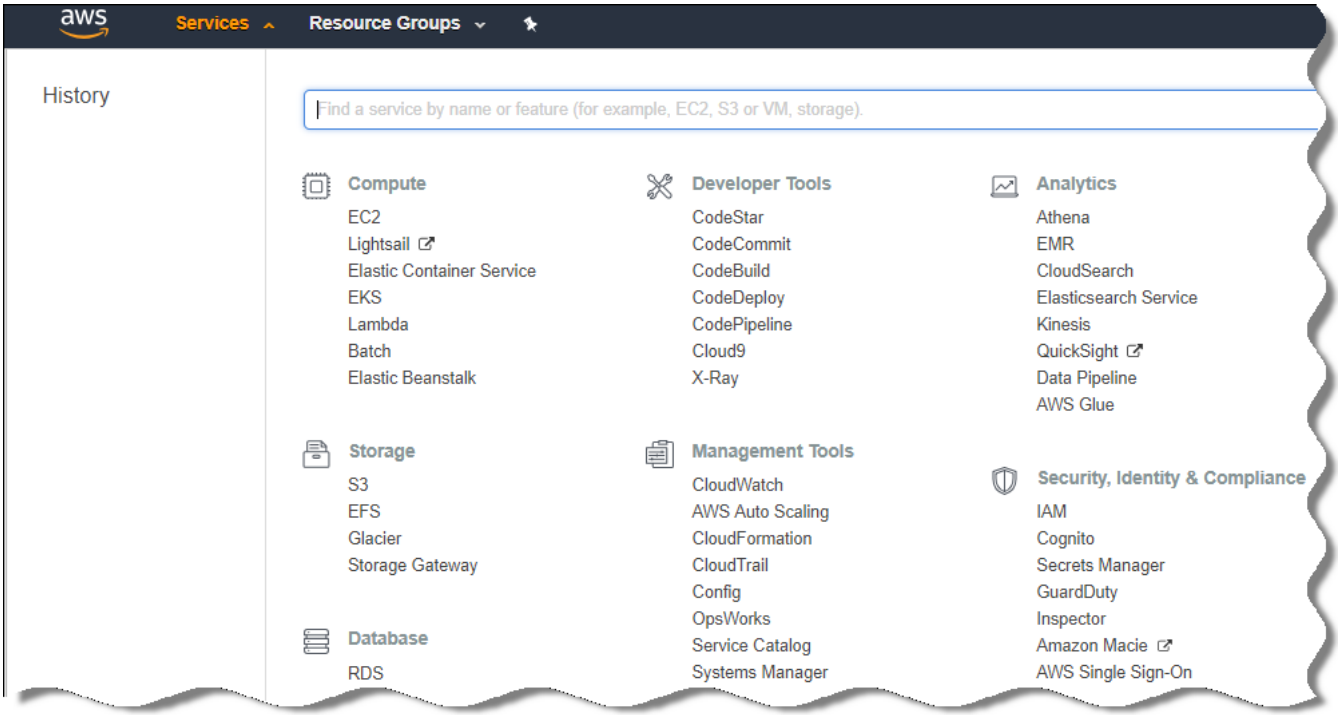
デバイスの検索とインスタンス上へのアプリケーションのインストールの権限が付与された IAM ロールが管理サーバーに割り当てられていない場合、Kaspersky Security Center の動作には IAM ユーザーアカウントが必要です。S3 バケットを使用する場合も、管理サーバーのデータのバックアップタスクで、前述の IAM ユーザーアカウントまたは別個の IAM ユーザーアカウントが必要です。すべての必要な権限を付与した IAM ユーザーアカウントを 1 個作成することも、ユーザーアカウントを 2 個作成することもできます。

IAM ユーザーには、Kaspersky Security Center の初期設定時に指定する必要のある *IAM アクセスキー*が自動的に作成されます。IAM アクセスキーは、アクセスキー ID と秘密鍵で構成されますIAM サービスの詳細については、AWS の次のリファレンスページを参照してください：

- http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/introduction.html
- http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2

必要な権限を持つIAMユーザーアカウントを作成するには：

1. AWS 管理コンソールを開き、正しいアカウントでログインします。
2. AWS のサービスのリストから［**IAM**］を選択します（下図を参照）。



AWS 管理コンソールで表示されるサービスのリスト

ユーザー名のリストとツールの操作メニューを含むウィンドウが表示されます。

3. ユーザーアカウントに関するメニューを選択して、ユーザー名を追加します。
4. 追加するユーザーについては、次の AWS プロパティを指定します：
   - アクセスの種類：**プログラムによるアクセス**
   - アクセス権限の境界は設定しない
   - アクセス権限：
     - ［**ReadOnlyAccess**］：クラウドセグメントのポーリングのみを実行し、AWS API を使用して EC2 インスタンスにアプリケーションをインストールしない場合。
     - ［**ReadOnlyAccess**］と［**AmazonSSMFullAccess**］：クラウドセグメントのポーリングを実行し、AWS API を使用して EC2 インスタンスにアプリケーションをインストールする場合。この場合、AmazonEC2RoleforSSM 権限を持つ IAM ロールを保護対象の EC2 インスタンスに割り当てる必要があります。

   アクセス権限の追加後、正しい権限を追加したかを確認します。選択が誤っている場合は前の画面に戻って再度選択します。
5. ユーザーアカウントの作成後、新しい IAM ユーザーの IAM アクセスキーを含む表が表示されます。アクセスキーの ID が［**アクセスキー ID**］列に表示されます。秘密鍵は［**シークレットアクセスキー**］列にアスタ

リスクとして表示されます。秘密鍵を表示するには、［**表示**］をクリックします。

新しく作成されたアカウントが、AWS アカウントに対応する IAM ユーザーアカウントの一覧に表示されます。

クラウドセグメントに Kaspersky Security Center を導入する際、IAM ユーザーアカウントの使用を指定し、アクセスキー ID とシークレットアクセスキーを Kaspersky Security Center に入力する必要があります。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

Amazon EC2 インスタンスにアプリケーションをインストールするための IAM ロールを作成する

Kaspersky Security Center を使用して EC2 インスタンスに保護を導入する前に、インスタンスにアプリケーションをインストールする権限を持つ IAM ロールを AWS 管理コンソール内に作成してください。詳細は、AWS ヘルプ内の IAM ロールに関する AWS ヘルプを参照してください。

Kaspersky Security Center を使用してセキュリティ製品をインストールする予定がある EC2 インスタンスに IAM ロールを割り当てるために、IAM ロールが必要になります。必要な権限を持つ IAM ロールを IAM ロールに割り当てない場合、AWS API ツールを使用したインスタンスでのアプリケーションのインストールでエラーが発生します。

AWS 管理コンソールを使用するには、AWS のアカウントのユーザー名とパスワードが必要です。

インスタンスへのアプリケーションのインストールに使用する IAM ロールを作成するには：

1. AWS 管理コンソールを開いて、AWS アカウントでログインします。
2. 左側のメニューで［**ロール**］を選択します。
3. ［**ロールの作成**］をクリックします。
4. 表示されるサービスのリストから［**EC2**］を選択します。その後、［**ユースケースの選択**］リストで［**EC2**］を再度選択します。
5. ［**次のステップ：アクセス権限**］をクリックします。
6. 表示されるリストで、［**AmazonEC2RoleforSSM**］の横にあるチェックボックスをオンにします。
7. ［**次のステップ：確認**］をクリックします。
8. IAM ロールの名前と説明を入力して、［**ロールの作成**］をクリックします。
   作成したロールの名前と説明がロールのリストに表示されます。

これ以降、新しく作成された IAM ロールを使用して、Kaspersky Security Center を使用して保護できる新しい EC2 インスタンスを作成できます。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

Amazon RDS の利用

このセクションでは、Kaspersky Security Center 用の Amazon RDS データベースの準備、RDS データベースのオプショングループへの配置、RDS データベースを使用するための IAM ロールの作成、ストレージとして使用する S3 バケットの準備、既存データベースの RDS への移行で必要となる手順を説明します。

Amazon RDS（Relational Database Service）とは、AWS クラウド環境で AWS ユーザーがリレーショナルデータベースの設定、運用、規模の調整を行うための Web サービスです。必要に応じて、Kaspersky Security Center で Amazon RDS データベースを使用できます。

次のデータベースを使用できます：

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

Amazon RDS インスタンスの作成

DBMS として Amazon RDS を使用する場合は、Amazon RDS データベースインスタンスを作成する必要があります。このセクションでは、SQL Express Edition の選択方法を説明します。Aurora MySQL または Standard MySQL（バージョン 5.7、8.0）を使用する場合は、これらのエンジンのうち 1 つを選択する必要があります。

Amazon RDS データベースインスタンスを作成するには：

1. https://console.aws.amazon.com にアクセスして AWS 管理コンソールを開き、正しいアカウントでログインします。
2. AWS インターフェイスを使用して、次の設定でデータベースを作成します。
   - エンジン：Microsoft SQL Server の Express Edition
   - DB エンジンのバージョン：SQL Server 2014 12.00.5546.0v1
   - DB インスタンスのクラス：db.t2.medium
   - ストレージタイプ：汎用
   - ストレージ割り当て：50 GiB 以上
   - セキュリティグループ：Kaspersky Security Center 管理サーバーをインストールする EC2 インスタンスと同じグループ

   RDS インスタンスの識別子、ユーザー名、パスワードを作成します。

   その他の設定は既定のまま利用できます。Amazon RDS インスタンスをカスタマイズしたい場合は、既定の設定を変更できます。ヘルプが必要な場合は、AWS の情報ページを参照してください。

3. 手順を終えると、AWS にプロセスの結果が表示されます。Amazon RDS インスタンスの詳細を確認したい場合は、［**DB インスタンスの詳細の表示**］をクリックします。次の操作として、Amazon RDS インスタンスのオプショングループの作成を開始できます。

Amazon RDS インスタンスの新規作成には数分かかる場合があります。作成したインスタンスは Kaspersky Security Center のデータ運用に利用できます。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

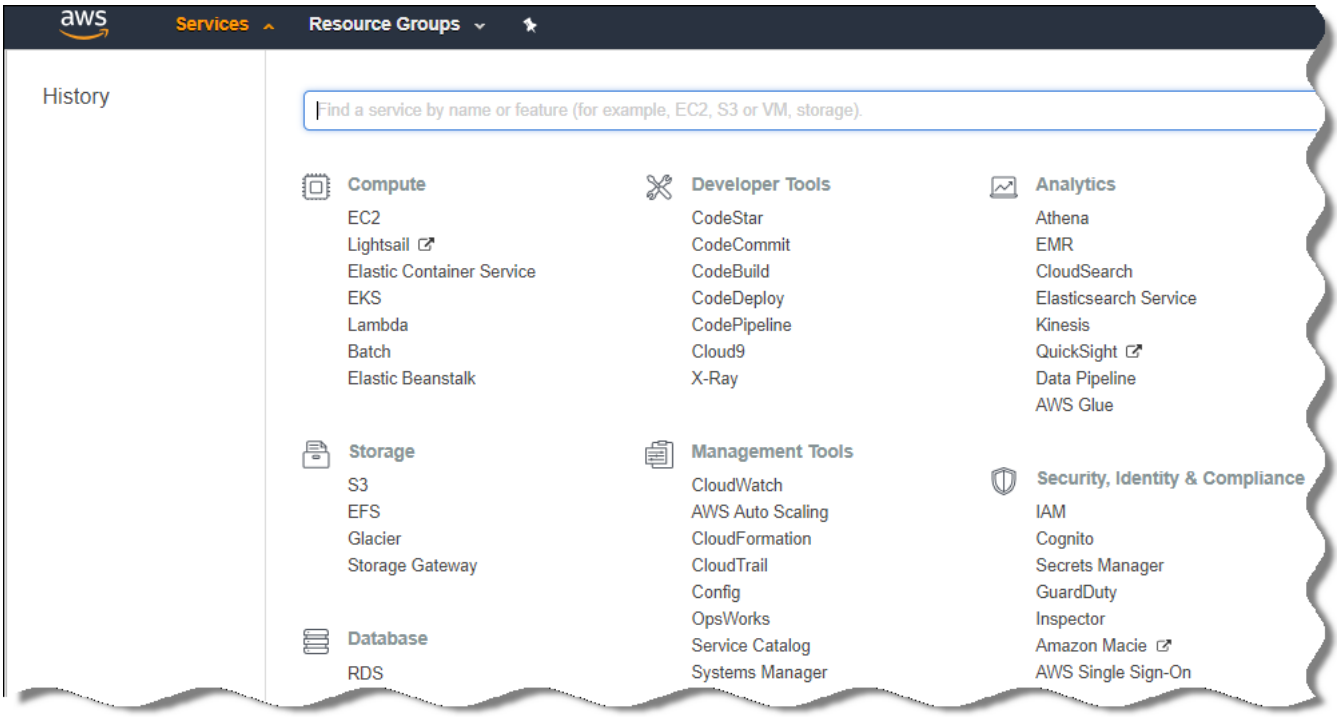
Amazon RDS インスタンス用のオプショングループの作成

Amazon RDS インスタンスをオプショングループに配置する必要があります。

Amazon RDS インスタンス用のオプショングループを作成するには：

1. https://console.aws.amazon.com にアクセスして AWS 管理コンソールを開き、正しいアカウントでサインインしていることを確認します。

2. メニューのリストから［**サービス**］を選択します。
使用可能なサービスのリストが表示されます（下図）。



AWS 管理コンソールで表示されるサービスのリスト

3. リストの中で［**RDS**］をクリックします。

4. 左側のペインで［**オプショングループ**］を選択します。

5. ［**グループの作成**］をクリックします。

6. Amazon RDS インスタンスの作成時に SQL Server を選択した場合、次の設定でオプショングループを作成します。

- エンジン：SQLserver-ex
- メジャーエンジンのバージョン：12.00

Amazon RDS インスタンスの作成時に異なる SQL データベースを選択した場合は、該当するエンジンを選択します。

グループが作成され、グループのリストに表示されます。

オプショングループの作成後、Amazon RDS インスタンスをオプショングループに配置します。

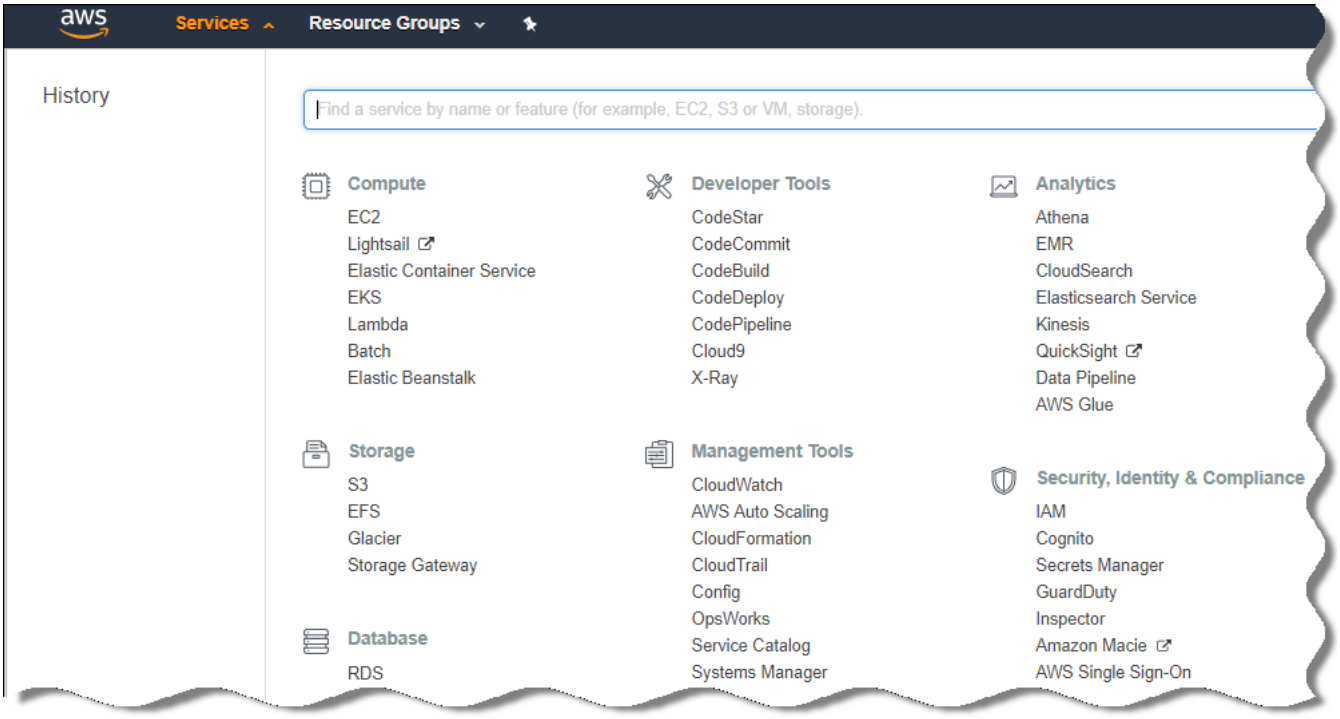
文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

オプショングループの変更

Amazon RDS インスタンスを配置したオプショングループの既定の設定では、Kaspersky Security Center データベースを使用するために十分ではありません。オプショングループにオプションを追加し、データベースを使用するための新しい IAM ロールを作成する必要があります。

オプショングループを変更し新しい IAM ロールを作成するには：

1. https://console.aws.amazon.com にアクセスして AWS 管理コンソールを開き、正しいアカウントでサインインしていることを確認します。
2. メニューのリストから［**サービス**］を選択します。
   使用可能なサービスのリストが表示されます（下図）。



AWS 管理コンソールで表示されるサービスのリスト

3. リストの中で［RDS］を選択します。
4. 左側のペインで［**オプショングループ**］を選択します。

オプショングループのリストが表示されます。

5. Amazon RDS インスタンスを配置したオプショングループを選択し、［**オプションの追加**］をクリックします。

   ［**オプションの追加**］ウィンドウが表示されます。

6. ［IAM ロール］セクションで［**新規ロールの作成**］を選択し、新しい IAM ロールの名前を入力します。

   既定の権限セットが付与された状態でロールが作成されます。以降の手順で、権限を変更する必要があります。

7. ［S3 バケット］セクションで、次のいずれかを実行します：

   - Amazon S3 バケットをまだ作成していない場合は、［**新規 S3 バケットの作成**］を選択し、AWS のインターフェイスを使用して新規 S3 バケットを作成します。
   - 管理サーバーデータのバックアップタスク用に Amazon S3 バケットインスタンスを作成済みの場合は、ドロップダウンリストから該当する S3 バケットを選択します。

8. ページの一番下にある［**オプションの追加**］をクリックして、オプションの追加を完了します。

オプショングループが変更され、RDS データベースを使用するための新しい IAM ロールが作成されます。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

Amazon RDS データベースのインスタンスを使用するための IAM ロールの権限の変更

オプショングループへのオプションの追加が完了したら、Amazon RDS データベースインスタンスを使用するために作成した IAM ロールに、必要な権限を割り当てる必要があります。

Amazon RDS データベースインスタンスを使用するために作成した IAM ロールに、必要な権限を割り当てるには：

1. https://console.aws.amazon.com にアクセスして AWS 管理コンソールを開き、正しいアカウントでサインインしていることを確認します。

2. サービスのリストから、［**IAM**］を選択します。

   ユーザー名のリストとツールの操作メニューを含むウィンドウが表示されます。

3. メニューで［**ロール**］を選択します。

4. 表示される IAM ロールのリストから、オプショングループへのオプションの追加時に作成したロールを選択します。

5. AWS のインターフェイスを使用して、**sqlNativeBackup-<日付>** ポリシーを削除します。

6. AWS のインターフェイスを使用して、ロールに「**AmazonS3FullAccess**」ポリシーを追加します。

IAM ロールに、Amazon RDS を使用するために必要な権限が割り当てられます。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

データベース用に使用する Amazon S3 バケットの準備

Amazon RDS（Amazon Relational Database System）のデータベースを使用する場合、データベースの定期的なバックアップが保存される Amazon S3（Amazon Simple Storage Service）バケットインスタンスを作成する必要があります。Amazon S3 と S3 バケットの概要については、Amazon のヘルプページを参照してください。Amazon S3 インスタンスの作成については、Amazon S3 のヘルプページを参照してください。

Amazon S3 バケットを作成するには：

1. AWS 管理コンソールを開き、正しいアカウントでサインインしていることを確認します。
2. AWS のサービスのリストから、S3 を選択します。
3. ウィザードの指示に従って管理コンソールを移動し、バケットを作成します。
4. 管理サーバーが置かれている（または配置が予定されている）のと同じリージョンを選択します。
5. ウィザードが完了したら、バケットのリストに新しいバケットが表示されていることを確認します。

新しい S3 バケットが作成され、バケットのリストに表示されます。オプショングループへのオプションの追加時に、このバケットを指定する必要があります。Kaspersky Security Center で*管理サーバーデータのバックアップタスクを作成*する場合も、S3 バケットのアドレスを指定する必要があります。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

Amazon RDS へのデータベースの移行

Kaspersky Security Center データベースをオンプレミスのデバイスから Amazon RDS をサポートする Amazon S3 インスタンスに移行できます。この操作には、RDS データベース用の S3 バケットとこの S3 バケットの AmazonS3FullAccess 権限が付与された IAM ユーザーアカウントが必要になります。

データベースの移行を実行するには：

1. RDS インスタンスを作成済みであることを確認します（詳細については、Amazon RDS のリファレンスページを参照）。
2. 物理管理サーバー（オンプレミス）で、カスペルスキーのバックアップユーティリティを実行して、管理サーバーのデータのバックアップを作成します。

   ファイルが backup.zip という名前になっていることを確認してください。
3. この backup.zip を管理サーバーがインストールされている EC2 インスタンスにコピーします。

管理サーバーがインストールされている EC2 インスタンスには十分な空き容量を確保してください。AWS 環境では、データベースの移行プロセスに対応できるように、インスタンスにディスク容量を追加できます。

4. AWS 環境の管理サーバーで、カスペルスキーのバックアップユーティリティを対話モードで起動します。バックアップと復元ウィザードが開始します。
5. ［**処理の選択**］ステップで、［**管理サーバーデータを復元**］を選択し、［**次へ**］を選択します。
6. ［**設定の復元**］ステップで、［**バックアップ保存先フォルダー**］の横の［**参照**］をクリックします。
7. 表示される［**オンラインストレージへサインイン**］ウィンドウで、次の情報を入力し［**OK**］をクリックします：
   - **S3 バケット名**

     S3 バケットの名前。
   - **バックアップフォルダー**

     バックアップ用の保管領域のフォルダーの場所を指定します。
   - **アクセスキーの ID**

     S3 バケットを使用する権限（AmazonS3FullAccess 権限）を付与された IAM ユーザーの AWS IAM アクセスキー ID を入力します。
   - **秘密鍵**

     S3 バケットを使用する権限（AmazonS3FullAccess 権限）を付与された IAM ユーザーの AWS IAM シークレットキーを入力します。
8. ［**ローカルバックアップから移行**］を選択します。［**参照**］を選択できるようになります。
9. ［**参照**］をクリックし、backup.zip をコピーした AWS 環境の管理サーバー上のフォルダーを選択します。
10. ［**次へ**］をクリックして、手順を完了します。

S3 バケットを使用している RDS データベースにデータが復元されます。AWS 環境での以降の Kaspersky Security Center の利用にこのデータベースを使用できます。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

Microsoft Azure クラウド環境での利用

このセクションでは、Microsoft Azure により提供されるクラウド環境での Kaspersky Security Center の導入とメンテナンスについての情報、およびこのクラウド環境での仮想マシンへの製品導入の詳細を説明します。

月単位の従量課金の SKU から導入された Kaspersky Security Center では、脆弱性とパッチ管理は自動的にアクティベートされますが、モバイルデバイス管理はアクティベートできません。

Microsoft Azure の使用について

Microsoft Azure プラットフォームを使用し、特に Azure Marketplace でアプリを購入して仮想マシンを作成するには、Azure サブスクリプションが必要です。管理サーバーの導入前に、仮想マシンへのアプリケーションのインストールに必要な権限を持った Azure アプリケーション ID を作成します。

Azure Marketplace で Kaspersky Security Center のイメージを購入する場合は、Kaspersky Security Center 管理サーバーが設定済みの状態で仮想マシンを導入できます。仮想マシンの設定を選択する必要はありますが、製品の導入を自分自身で行う必要はありません。インストール後、管理コンソールを起動して管理サーバーに接続し、Kaspersky Security Center の操作を開始できます。

Kaspersky Security Center 管理サーバーが導入された Azure 仮想マシンを使って、オンプレミスのデバイスを保護することもできます（たとえば、クラウドサーバーの方が物理サーバーよりも維持やメンテナンスがしやすいことが判明した場合）。そのような場合は、管理サーバーがオンプレミスのデバイスにインストールされている場合と同じように管理サーバーで作業を行います。Azure API ツールを使用する計画がない場合は、Azure アプリケーション ID は必要ありません。この場合、Azure サブスクリプションのみで要件を満たします。

サブスクリプション、アプリケーション ID およびパスワードの作成

Microsoft Azure 環境で Kaspersky Security Center を使用するには、Azure サブスクリプション、Azure アプリケーション ID および Azure アプリケーションパスワードが必要です。既にサブスクリプションを保有している場合は、既存のサブスクリプションを使用できます。

Azure サブスクリプションを保有していると、Microsoft Azure プラットフォーム管理ポータルと Microsoft Azure サービスへのアクセスが許可されます。サブスクリプションの保有者は、Windows Azure プラットフォームを使用して Azure SQL、Azure ストレージなどのサービスを管理できます。

Microsoft Azure サブスクリプションを作成するには：

https://learn.microsoft.com/ja-jp/azure/cost-management-billing/manage/create-subscription に移動します。そこにある指示に従ってください。

サブスクリプションの作成の詳細については、Microsoft の Web サイトを参照してください。サブスクリプション ID を取得できます。後程、このサブスクリプション ID とアプリケーション ID およびパスワードを、Kaspersky Security Center に入力します。

Azure アプリケーション ID とパスワードを作成するには：

1. https://portal.azure.com に移動し、ログインしていることを確認します。
2. リファレンスページの指示に従って、アプリケーション ID を作成します。
3. アプリケーション設定の［**キー**］セクションに移動します。

4. ［**キー**］セクションで、［**説明**］と［**有効期限**］を入力し、［**値**］は空白のままにしておきます。

5. ［**保存**］をクリックします。

   ［**保存**］をクリックすると、［**値**］フィールドにシステムが自動的に生成した長い文字列が表示されます。この文字列が Azure アプリケーションパスワードとなります（例：yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU= など）。説明は入力した通りに表示されます。

6. パスワードをコピーして保管し、後程 Kaspersky Security Center でアプリケーション ID とパスワードを入力できるようにしておきます。

   パスワードはこの作成画面でのみコピーできます。この機会を逃すと、パスワードは表示されなくなり復元できません。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

Azure アプリケーション ID へのロールの割り当て

デバイスの検索を使用した仮想マシンの検出のみが目的の場合、Azure アプリケーション ID に「Reader」ロールを割り当てる必要があります。仮想マシンの検出だけでなく仮想マシンへの保護の導入も行う場合、Azure アプリケーション ID に「Virtual Machine Contributor」ロールを割り当てる必要があります。

マイクロソフト社の Web サイトの説明に従って、Azure アプリケーション ID にロールを割り当てます。

Microsoft Azure での管理サーバーの導入とデータベースの選択

Microsoft Azure 環境に管理サーバーを導入するには：

1. 正しいアカウントを使用して Microsoft Azure にサインインします。

2. Azure ポータルに移動します。

3. 左側のペインで、緑色のプラス記号をクリックします。

4. メニューの検索フィールドで「Kaspersky Hybrid Cloud Security」と入力します。

   Kaspersky Hybrid Cloud Security では、Kaspersky Security Center と次の 2 つのセキュリティ製品を組み合わせて提供します： Kaspersky Endpoint Security for Linux および Kaspersky Security for Windows Server

5. 検索結果のリストから Kaspersky Hybrid Cloud Security または Kaspersky Hybrid Cloud Security（BYOL）を選択します。

   画面の右側に情報ウィンドウが表示されます。

6. 情報を読み、情報ボックスの下部に表示されている［作成］をクリックします。

7. すべての必須フィールドに値を入力します。必要に応じて、ツールチップから情報やヘルプを参照してください。

8. サイズの選択時は、星マークで推奨されている 3 つのオプションのいずれかを選択します。

通常、RAM のサイズは 8 GB で十分です。また、Azure では仮想マシンの RAM や他のリソースのサイズをいつでも増やすことができます。

9. データベースの選択時は、配備計画に応じて次のいずれかを選択します：

   - ローカル：管理サーバーを導入先と同じ仮想マシンにデータベースを配置したい場合。Kaspersky Security Center には SQL Server Express が付属します。SQL Server Express で必要を満たせる場合は、このオプションを選択します。

   - 新規：Azure 環境で新しい RDS データベースが必要な場合。SQL Server Express 以外の DBMS を使用したい場合はこのオプションを選択します。データはクラウド環境に転送されて保存され、そこでの追加費用は発生しません。

   - 既存：既存のデータベースサーバーを使用する場合。この場合、データベースサーバーの場所を指定する必要があります。このデータベースサーバーが Azure 環境外にある場合、データはインターネット経由で転送されるため、追加費用が発生する可能性があります。

10. サブスクリプション ID の入力時には、事前に作成したサブスクリプションを使用します。

導入後、RDP を使用して管理サーバーに接続できます。管理コンソールを使用して管理サーバーを操作できます。

Azure SQL の利用

このセクションでは、Kaspersky Security Center 用の Microsoft Azure のデータベースの準備、Azure ストレージアカウントの準備、既存のデータベースの Azure SQL への移行で必要となる手順を説明します。

SQL Database は Microsoft Azure の汎用的なリレーショナルデータベース管理サービスです。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

Azure ストレージアカウントの作成

Azure SQL データベースと導入スクリプトを使用するためには Microsoft Azure のストレージアカウントを作成する必要があります。

ストレージアカウントを作成するには：

1. Azure ポータルにサインインします。

2. 左側のペインで、［**ストレージアカウント**］を選択して［**ストレージアカウント**］ウィンドウを開きます。

3. ［**ストレージアカウント**］ウィンドウで［**追加**］をクリックして［**ストレージアカウントの作成**］ウィンドウを開きます。

4. すべての必須フィールドに値を入力してストレージアカウントを作成します：

   - 場所：管理サーバーと同じ場所を選択してください。

- その他の入力フィールド：既定値のまま設定できます。

各フィールドの詳細については、必要に応じてツールチップの情報を参照してください。

ストレージアカウントの作成が完了すると、ストレージアカウントのリストが表示されます。

5. ストレージアカウントのリストで新規に作成されたアカウント名をクリックすると、このアカウントの情報が表示されます。

6. ストレージアカウントのアカウント名、リソースグループ、アクセスキーは確実に把握しておいてください。Kaspersky Security Center の使用時にこれらの情報が必要になります。

サポート情報が必要な場合は、Azure の Web サイトを参照してください。

ストレージアカウントを既に保有している場合、これを使用して Kaspersky Security Center を使用できます。

Azure SQL データベースと SQL サーバーの作成

Azure 環境で SQL データベースと SQL サーバーが必要です。

Azure SQL データベースと SQL サーバーを作成するには：

1. Azure の Web サイトに記載されている手順を参照してください。

   Microsoft Azure で新しい SQL サーバーを作成するかどうか確認された時、新しい SQL サーバーを作成できます。使用できる Azure SQL サーバーがある場合、新規作成せずに既存の SQL サーバーを Kaspersky Security Center で使用できます。

2. SQL データベースと SQL サーバーの作成後、リソース名とリソースグループを確実に把握しておくようにしてください：

   a. https://portal.azure.com に移動し、ログインしていることを確認します。

   b. 左側のペインで、［**SQL データベース**］を選択します。

   c. データベースのリストから目的のデータベースの名前をクリックします。

   プロパティウィンドウが表示されます。

   d. データベースの名前がリソース名です。リソースグループ名はプロパティウィンドウの［**概要**］セクションに表示されます。

Azure SQL へのデータベースの移行を行うために、データベースのリソース名とリソースグループが必要です。

Azure SQL へのデータベースの移行

Azure 環境への管理サーバーの導入の完了後、オンプレミスのデバイスから Azure SQL へ Kaspersky Security Center のデータベースを移行できます。Azure SQL データベース用の Azure ストレージアカウントが必要です。管理サーバーに Microsoft SQL Server データ層アプリケーションフレームワーク（DacFx）と SQLSysCLRTypes が必要です。

データベースの移行を実行するには：

1. Azure ストレージアカウントを作成していることを確認します。

2. 管理サーバーに SQLSysCLRTypes と DacFx が存在することを確認します。

   Microsoft SQL Server Data-Tier Application Framework(17.0.1 DacFx) と SQLSysCLRTypes（使用する SQL Server のバージョンに対応するバージョンを選択してください）を Microsoft の公式 Web サイトからダウンロードできます。

3. 物理管理サーバー（オンプレミス）で、［**Azure 形式へ移行**］をオンにしてカスペルスキーのバックアップユーティリティを実行し、管理サーバーのデータのバックアップを作成します。

4. バックアップファイルを Azure 環境の管理サーバーにコピーします。

   管理サーバーがインストールされている Azure 仮想マシンには十分な空き容量があるようにしてください。Azure 環境では、データベースの移行プロセスに対応できるように、仮想マシンにディスク容量を追加できます。

5. Microsoft Azure 環境の管理サーバーで、カスペルスキーのバックアップユーティリティを対話モードで起動します。

   バックアップと復元ウィザードが開始します。

6. ［**処理の選択**］ステップで、［**管理サーバーデータを復元**］を選択し、［**次へ**］を選択します。

7. ［**設定の復元**］ステップで、［**バックアップ保存先フォルダー**］の横の［**参照**］をクリックします。

8. 表示される［**オンラインストレージへサインイン**］ウィンドウで、次の情報を入力し［**OK**］をクリックします：

   - **Azure ストレージアカウント名**

     Kaspersky Security Center で使用するために作成した Azure ストレージアカウントの名前です。

   - **バックアップフォルダー**

     バックアップ用の保管領域のフォルダーの場所を指定します。

   - **Azure サブスクリプション ID**

     Azure ポータルで作成したサブスクリプションです。

   - **Azure アプリケーションパスワード**

     アプリケーション ID の作成時に取得したアプリケーション ID のパスワードです。

     パスワードの文字はアスタリスクで表示されます。パスワードの入力を開始すると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを押し続けます。

   - **Azure ストレージのアクセスキー**

情報はストレージアカウントのプロパティの［アクセスキー］セクションで確認できます。いずれのキー（key1 または key2）も使用できます。

- **Azure SQL サーバー名**

  情報は Azure SQL サーバーのプロパティで確認できます。

- **Azure SQL サーバーリソースグループ**

  情報は Azure SQL サーバーのプロパティで確認できます。

- **Azure アプリケーション ID**

  Azure ポータルで作成したアプリケーション ID です。

  ポーリングやその他の目的で使用する Azure アプリケーション ID を 1 つだけ指定できます。別の Azure セグメントでポーリングを実行する場合は、既存の Azure 接続を事前に削除する必要があります。

9. ［**ローカルバックアップから移行**］を選択します。

   ［**参照**］を選択できるようになります。

10. ［**参照**］をクリックし、バックアップファイルをコピーした Azure 環境の管理サーバー上のフォルダーを選択します。

11. ［**次へ**］をクリックして、手順を完了します。

Azure ストレージを使用している Azure SQL データベースにデータが復元されます。Azure 環境での以降の Kaspersky Security Center の利用にこのデータベースを使用できます。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center のリリース日時点のものです。

Google Cloud での利用

このセクションでは、Google が提供するクラウド環境での Kaspersky Security Center の使用に関する情報を提供します。

クライアントのメールアドレス、プロジェクトID、秘密鍵の作成

Google API を使用して、Google Cloud Platform で Kaspersky Security Center を操作できます。Google アカウントが必要です。詳細については、https://cloud.google.com にある Google のドキュメントを参照してください。

次の認証情報を作成し Kaspersky Security Center に提供する必要があります：

- **クライアントのメール**

  クライアントのメールアドレスは、Google Cloud でプロジェクトの登録に使用したメールアドレスです。

- **プロジェクト ID**

  プロジェクト ID は、Google Cloud でプロジェクトの登録時に取得した ID です。

- **秘密鍵**

  秘密鍵は、Google Cloud でプロジェクトの登録時に秘密鍵として取得した文字列です。間違えないように、この文字列をコピーして貼り付けることを検討してください。

Google Cloud SQL for MySQL インスタンスの操作

Google Cloud でデータベースを作成し、このデータベースを Kaspersky Security Center に使用できます。

Kaspersky Security Center は MySQL 5.7 と 5.6 で動作します。MySQL の他のバージョンはテストされていません。

MySQL データベースを作成して設定するには：

ブラウザーで https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen ページを開き、表示される指示に従います。

MySQL データベースを設定する際は、次のフラグを使用します：

- **sort_buffer_size** 10000000
- **join_buffer_size** 20000000
- **innodb_lock_wait_timeout** 300
- **max_allowed_packet** 32000000
- **innodb_thread_concurrency** 20
- **max_connections** 151
- **tmp_table_size** 67108864
- **max_heap_table_size** 67108864
- **lower_case_table_names** 1

Kaspersky Security Center で管理するクラウド環境のクライアントデバイスの必須条件

管理サーバーやネットワークエージェント、カスペルスキーのセキュリティ製品をインストールするデバイスは、次の条件を満たす必要があります：

- セキュリティグループの設定により、管理サーバーの次のポート（導入に最低限必要な一連のポート）を使用できる：
  - 8060 HTTP（ネットワークエージェントのインストールパッケージおよびセキュリティ製品のインストールパッケージの、管理サーバーから保護対象インスタンスへの転送で使用します）
  - 8061 HTTPS（ネットワークエージェントのインストールパッケージおよびセキュリティ製品のインストールパッケージの、管理サーバーから保護対象インスタンスへの転送で使用します）
  - 13000 TCP（SSL を使用した、保護対象インスタンスおよびセカンダリ管理サーバーからプライマリ管理サーバーへのデータ転送で使用します）
  - 13000 UDP（管理サーバーへのインスタンスのシャットダウンに関する情報の転送で使用します）
  - 14000 TCP（SSL を使用しない、保護対象インスタンスおよびセカンダリ管理サーバーからプライマリ管理サーバーへのデータ転送で使用します）
  - 13291（管理コンソールから管理サーバーへの接続で使用します）
  - 40080（導入スクリプトの動作に使用します）

  セキュリティグループは AWS 管理コンソールまたは Azure ポータルで設定できます。既定以外の構成で Kaspersky Security Center を使用する場合は、ナレッジベース参照してください。既定以外の構成としては、たとえば管理サーバーの端末に管理コンソールをインストールせずにワークステーションにインストールしたり、KSN プロキシサーバーを使用する構成が当てはまります。
- ポート 15000 UDP はクライアントデバイスで利用可能です（管理サーバーとの通信の要求の受け取りに使用します）。
- AWS クラウド環境：
  - AWS API を使用する場合、本製品をインスタンスにインストールする際に使用する IAM ロールが設定されている。
  - 各 Amazon EC2 インスタンスに Systems Manager Agent （SSM エージェント）がインストールされ、実行されている。
  - Kaspersky Security Center は SSM エージェントによって、管理者に毎回確認しなくても、デバイスおよびデバイスのグループに自動的にアプリケーションをインストールできます。
  - Windows オペレーティングシステムを実行していて、2016 年 11 月以降に AMI から導入されたインスタンスでは、SSM エージェントがインストールされ、実行されている。他のすべてのデバイスでは、SSM エージェントを手動でインストールする必要があります。Windows と Linux のオペレーティングシステムを実行しているデバイスに SSM エージェントをインストールする方法については、AWS のヘルプページを参照してください。
- Microsoft Azure クラウド環境：

- 各 Azure 仮想マシンに Azure 仮想マシンエージェントがインストールされ、実行されている。

  既定では、新規仮想マシンと合わせて Azure 仮想マシンエージェントも作成されるため、エージェントを手動で作成したり有効にする必要はありません。Windows デバイスと Linux デバイス用の Azure 仮想マシンエージェントの詳細については、Microsoft のヘルプページを参照してください。

- Azure アプリケーション ID に次のロールが付与されている。

  - Reader（ポーリングを使用して仮想マシンを検出するために必要）
  - Virtual Machine Contributor（仮想マシンに保護を導入するために必要）
  - SQL Server Contributor（Microsoft Azure 環境で SQL データベースを使用するために必要）

  これらすべての処理を実行する場合は、Azure アプリケーション ID に 3 つすべてのロールを割り当ててください。

クラウド環境の設定に必要なインストールパッケージの作成

次のプログラム用のインストールパッケージと管理プラグインがある場合は Kaspersky Security Center の［クラウド環境設定ウィザード］が使用可能です：

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

  クラウド環境での Kaspersky Endpoint Security for Windows の導入は、 カスペルスキー Endpoint Security 12.0 for Windows の次期リリース後に使用可能になります。

- Kaspersky Security for Windows Server

これらのインストールパッケージは、保護するインスタンスまたは仮想マシンにアプリケーションをインストールするために必要です。これらのインストールパッケージがない場合は作成する必要があります。そうしないと、クラウド環境設定ウィザードが機能しません。

インストールパッケージを作成するには：

1. カスペルスキーの Web サイトから最新版のアプリケーションとプラグインをダウンロードします：

   - Kaspersky Security for Windows Server のインストーラーと管理プラグイン。
   - Kaspersky Security Center 経由のリモートインストール用のインストーラー、ファイル、Kaspersky Endpoint Security for Linux 管理プラグイン。

2. 管理サーバーがインストールされているインスタンス（または仮想マシン）のすべてのファイルを保存します。
3. すべてのパッケージからファイルを展開します。
4. Kaspersky Security Center を開始します。
5. コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］の順に選択して、［**インストールパッケージの作成**］をクリックします。

6. ［**カスペルスキーのインストールパッケージの作成**］をクリックします。

7. パッケージ名と製品インストーラーのパスを「<フォルダー>\<ファイル名>.kud」のように指定して、［**次へ**］をクリックします。

8. 使用許諾契約書を読み、規約に同意することを確認するチェックボックスを選択し、［**次へ**］をクリックします。

管理サーバーにインストールパッケージがアップロードされ、インストールパッケージのリストで利用できるようになります。

インストールパッケージを作成し、管理プラグインを管理サーバーにインストールするとすぐに、クラウド環境の設定が使用可能になります。

クラウド環境の設定

クラウド環境設定ウィザードを使用して Kaspersky Security Center を構成する場合に必要な項目は次の通りです：

- クラウド環境用の特定の資格情報：
  - クラウドセグメントをポーリングする権限が付与された IAM ロールまたはクラウドセグメントをポーリングする権限が付与された IAM ユーザーアカウント（Amazon Web Services で使用する場合）
  - Azure アプリケーション ID パスワードとサブスクリプション（Microsoft Azure で使用する場合）
  - Google クライアントのメールアドレス、プロジェクト ID、秘密鍵（Google Cloud で使用する場合）
- インストールパッケージ：
  - Windows 用のネットワークエージェント
  - Linux 用のネットワークエージェント
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux の Web プラグイン
- 次のうち少なくとも 1 つ：
  - Kaspersky Endpoint Security for Windows のインストールパッケージと Web プラグイン（推奨）
  - Kaspersky Security for Windows Server のインストールパッケージと Web プラグイン

クラウド環境の機能を使用しない場合（たとえば、物理クライアントデバイスの保護のみを管理する場合など）、クラウド環境設定ウィザードを終了し、標準の管理サーバークイックスタートウィザードを手動で実行することができます。

すぐに使えるイメージから Kaspersky Security Center を導入している場合、クラウド環境の設定は、管理コンソールからの管理サーバーへの初回接続時に自動的に開始されます。また、クラウド環境設定ウィザードは手動でいつでも起動することができます。

クラウド環境設定ウィザードを手動で起動するには：

1. コンソールツリーで、［**管理サーバー**］フォルダーを選択します。

2. ノードのコンテキストメニューで、［**すべてのタスク**］→［**クラウド環境の設定**］の順にオンにします。

平均作業時間は約 15 分です。

クラウド環境設定ウィザードについて

クラウド環境設定ウィザードを使用すると、クラウド環境での使用の詳細を考慮しながら、Kaspersky Security Center を設定することができます。

ウィザードでは、次のオブジェクトを作成します：

- 既定の設定が指定されたネットワークエージェントポリシー
- Kaspersky Endpoint Security for Linux のポリシー
- Kaspersky Security for Windows Server のポリシー
- インスタンス用の管理グループとインスタンスを自動的に管理グループに移動するためのルール
- 管理サーバーデータのデータバックアップタスク
- Linux と Windows を実行しているデバイスに保護をインストールするためのタスク
- 各管理対象デバイスに対するタスク：
  - 簡易マルウェアスキャン
  - アップデートのダウンロード

BYOL ライセンスオプションを選択した場合は、クラウド環境の設定もライセンス情報ファイルまたはアクティベーションコードを使用して Kaspersky Security Center をアクティベートし、ライセンス情報ファイルまたはアクティベーションコードをライセンスストレージに格納します。

ステップ 1：アプリケーションのアクティベート方法の選択

すぐに使用できる AMI の 1 つ（AWS Marketplace）または利用ベースで月額請求される　SKU（Azure Marketplace）を契約している場合、このステップは表示されません。この場合、ウィザードはすぐに次のステップに進みます。Google Cloud ですぐに使用できる AMI を購入することはできません。

Kaspersky Security Center の BYOL ライセンスオプションを選択した場合、ウィザードでアプリケーションのアクティベーション方法を選択するウィンドウが表示されます。

Kaspersky Security for Virtualization または Kaspersky Hybrid Cloud Security のアクティベーションコードまたはライセンス情報ファイルでアプリケーションをアクティベートする必要があります。

次のいずれかの方法でアプリケーションをアクティベートすることができます：

- アクティベーションコードを入力します。

  オンラインアクティベーションが起動します。このプロセスでは、指定したアクティベーションコード、およびライセンス情報ファイルの発行とアクティベーションが検証されます。

- ライセンス情報ファイルを指定します。

  ライセンス情報ファイルの確認が行われ、正しい情報が含まれている場合はアクティベートされます。あるいは、別のライセンス情報ファイルを指定するように指示されます。

Kaspersky Security Center によって、ライセンス保管領域にライセンスが格納され、管理対象デバイス上で自動的に配信されたライセンスとしてマークされます。

Microsoft Windows の標準リモートデスクトップ接続のようなアプリケーションを使用してインスタンスに接続する場合は、接続に使用している物理デバイスのドライブをリモート接続のプロパティで指定する必要があります。ドライブを指定することで、インスタンスから物理デバイス上のファイルまで確実にアクセスでき、ライセンス情報ファイルを選択、指定することができます。

有料 AMI または月単位の従量課金の SKU から導入した Kaspersky Security Center で作業を行う場合は、ライセンス情報ファイルとアクティベーションコードをライセンス保管領域に追加することはできません。

ステップ 2：クラウド環境の選択

Kaspersky Security Center を導入するクラウド環境を選択します：AWS、Azure、または Google Cloud。

ステップ 3：クラウド環境での認証

AWS

AWS を選択した場合は、必要な権限がある IAM ロールの使用を指定するか、AWS IAM アクセスキーを Kaspersky Security Center に入力します。IAM ロールまたは AWS IAM アクセスキーがない場合、クラウドセグメントのポーリングはできません。

クラウドセグメントのポーリングに使用する接続について、以下の設定を指定します：

- **接続名**

  接続の名前を入力します。名前を 256 文字以上にすることはできません。Unicode 文字のみを使用できます。

  この名前はクラウドデバイスの管理グループの名前としても使用されます。

  複数のクラウド環境を使用する予定の場合は、たとえば「Azure Segment」「AWS Segment」「Google Segment」のように、環境の名前を接続名に含めることを検討してください。

- **AWS IAM ロールを使用**

既に AWS サービスで使用する管理サーバー用 IAM ロールを作成している場合、このオプションを選択します。

- **AWS IAM ユーザーアカウントを使用**

  必要な権限がある IAM ユーザーアカウントがある場合、このオプションを選択し、キーの ID と秘密鍵を入力します。

  - **アクセスキーの ID**

    IAM アクセスキーの ID（英数字の並び）：IAM ユーザーアカウント作成時に受け取ったキーの ID です。

    このフィールドは、IAM ロールではなく AWS IAM アクセスキーを認証のために選択した場合に使用できます。

  - **秘密鍵**

    IAM ユーザーアカウント作成時にアクセスキーの ID と一緒に受け取った秘密鍵です。

    秘密鍵の文字はアスタリスクで表示されます。秘密鍵を入力し始めると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを必要な間だけ押し続けます。

    このフィールドは、IAM ロールではなく AWS IAM アクセスキーを認証のために選択した場合に使用できます。

この接続は本製品の設定に保存されます。クラウド環境の設定で作成できる AWS IAM アクセス キーは 1 つだけです。その後で、追加の接続を指定して、他のクラウドセグメントを管理することもできます。

Kaspersky Security Center からインスタンスにアプリケーションをインストールするには、IAM ロール（または入力中のキーにアカウントが関連付けられている IAM ユーザー）にすべての必要な権限があることを確認する必要があります。

Azure

Azure を選択した場合は、クラウドセグメントのポーリングに使用する接続について、以下の設定を指定します：

- **接続名**

  接続の名前を入力します。名前を 256 文字以上にすることはできません。Unicode 文字のみを使用できます。

  この名前はクラウドデバイスの管理グループの名前としても使用されます。

  複数のクラウド環境を使用する予定の場合は、たとえば「Azure Segment」「AWS Segment」「Google Segment」のように、環境の名前を接続名に含めることを検討してください。

- **Azure アプリケーション ID**

Azure ポータルで作成したアプリケーション ID です。

ポーリングやその他の目的で使用する Azure アプリケーション ID を 1 つだけ指定できます。別の Azure セグメントでポーリングを実行する場合は、既存の Azure 接続を事前に削除する必要があります。

- **Azure サブスクリプション ID**

  Azure ポータルで作成したサブスクリプションです。

- **Azure アプリケーションパスワード**

  アプリケーション ID の作成時に取得したアプリケーション ID のパスワードです。

  パスワードの文字はアスタリスクで表示されます。パスワードの入力を開始すると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを押し続けます。

- **Azure ストレージアカウント名**

  Kaspersky Security Center で使用するために作成した Azure ストレージアカウントの名前です。

- **Azure ストレージのアクセスキー**

  パスワード（アクセスキー）は Kaspersky Security Center で使用する Azure ストレージアカウントを作成した時に取得したものです。

  キーは、Azure ストレージアカウントの概要セクションのアクセスキーに関するサブセクションで確認できます。

この接続は本製品の設定に保存されます。

Google Cloud

Google Cloud を選択した場合は、クラウドセグメントのポーリングに使用する接続について、以下の設定を指定します：

- **接続名**

  接続の名前を入力します。名前を 256 文字以上にすることはできません。Unicode 文字のみを使用できます。

  この名前はクラウドデバイスの管理グループの名前としても使用されます。

  複数のクラウド環境を使用する予定の場合は、たとえば「Azure Segment」「AWS Segment」「Google Segment」のように、環境の名前を接続名に含めることを検討してください。

- **クライアントのメール**

  クライアントのメールアドレスは、Google Cloud でプロジェクトの登録に使用したメールアドレスです。

- **プロジェクト ID**

プロジェクト ID は、Google Cloud でプロジェクトの登録時に取得した ID です。

- **秘密鍵**

  秘密鍵は、Google Cloud でプロジェクトの登録時に秘密鍵として取得した文字列です。間違えないように、この文字列をコピーして貼り付けることを検討してください。

この接続は本製品の設定に保存されます。

ステップ 4：クラウドとの同期設定および次に実行される処理の選択

このステップでは、クラウドセグメントのポーリングが開始し、インスタンス専用の管理グループが作成されます。ポーリング中に検出されたインスタンスはこのグループに配置されます。クラウドセグメントのポーリングスケジュールが設定されます（既定では 5 分間隔）。

未割り当てデバイスを自動的に移動する［**クラウドと同期**］ルールも作成されます。以降、クラウドネットワークがスキャンされるたびに、検出された仮想デバイスは［**管理対象デバイス**］の［**クラウド**］グループ内の対応するサブグループに移動されます。

［**クラウドセグメントとの同期**］ウィンドウで、次の設定を指定できます：

- **管理グループ構造をクラウドセグメントと同期する**

  このオプションをオンにすると、［**クラウド**］グループが自動的に［**管理対象デバイス**］グループ内に作成され、クラウドデバイスの検索が開始されます。クラウドネットワークの各スキャンによって検出されたインスタンスと仮想マシンは、クラウドグループ内に配置されます。このグループ内の管理サブグループの構造は、クラウドセグメントの構造に対応します（AWS では、アベイラビリティーゾーンとプレイスメントグループは構造に反映されません。Azure では、サブネットは構造に反映されません）。クラウド環境のインスタンスとして識別されていないデバイスは**未割り当てデバイス**グループに分類されます。このグループ構造を使用して、インストールタスクをグループ化してアンチウイルス製品をインスタンスにインストールし、グループごとに異なるポリシーを設定することができます。

  このチェックボックスをオフにしても、**クラウド**グループは作成され、デバイスの検索も開始されます。ただし、クラウドセグメントの構造に対応するサブグループはグループ内で作成されません。検出されたすべてのインスタンスは**クラウド**管理グループに属しているため、1つのリストに表示されます。同期を必要とする Kaspersky Security Center を使用している場合、［**クラウドと同期**］ルールのプロパティを編集し、このルールを強制的に実行することもできます。このルールを強制的に適用すると、クラウドセグメントの構造と一致するようにクラウドグループ内のサブグループの構造が変更されます。

  既定では、このオプションはオフです。

- **保護の導入**

このオプションをオンにすると、セキュリティ製品をインスタンスにインストールするためのタスクをウィザードで作成します。ウィザードが終了すると、製品導入ウィザードが自動的にクラウドセグメント内のデバイス上で起動するため、ユーザーはネットワークエージェントとセキュリティ製品をこれらのデバイスにインストールできます。

Kaspersky Security Center にはこれらの導入時に利用できるネイティブツールが用意されています。EC2 インスタンスまたは Azure 仮想マシンにアプリケーションにインストールに必要な権限が付与されていない場合、**リモートインストール**タスクを手動で構成し、必要な権限が付与されたアカウントを指定できます。この場合、AWS API または Azure API を使用して検出されたデバイスではリモートインストールタスクを利用できません。このタスクは Active Directory、Windows ドメイン、IP アドレス範囲のいずれかのポーリングを使用して検出されたデバイスで利用できます。

このオプションをオフにすると、製品導入ウィザードは起動せず、セキュリティ製品をインスタンスにインストールするタスクは作成されません。これらの操作は両方とも、後で手動で実行することができます。

Google Cloud では、製品の導入は Kaspersky Security Center ネイティブツールを使用してのみ行うことができます。Google Cloud を選択した場合、［**保護の導入**］は使用できません。

ステップ 5：クラウド環境での Kaspersky Security Network の設定

Kaspersky Security Center の動作に関する情報を Kaspersky Security Network ナレッジベースに転送する設定を指定します。次のいずれかのオプションをオンにします：

- **Kaspersky Security Network への参加に同意する**

  Kaspersky Security Center とクライアントデバイスにインストールされている管理対象製品は、自動的に動作情報を Kaspersky Security Network に送信します。Kaspersky Security Network への参加により、ウイルスなどの脅威に関する情報を含んだデータベースのアップデートをより迅速に入手できるため、セキュリティへの緊急の脅威にすぐに対応できます。

- **Kaspersky Security Network への参加に同意しない**

  Kaspersky Security Center と管理対象製品は、Kaspersky Security Network に対して情報を提供しません。

  このオプションをオンにすると、Kaspersky Security Network の使用がオフになります。

カスペルスキーは、Kaspersky Security Network への参加を推奨しています。

ステップ 6：クラウド環境でのメール通知の設定

仮想クライアントデバイス上のカスペルスキー製品の実行中に登録されたイベントに関する通知の配信方法を設定します。この設定は、アプリケーションポリシーの既定の設定として使用されます。

カスペルスキー製品で発生したイベントに関する通知の配信を設定するには、次の設定を使用します：

- **宛先（メールアドレス）**

通知が送られるユーザーのメールアドレスです。1つ以上のアドレスを入力できます。複数のアドレスを入力する場合はセミコロンで区切ってください。

- **SMTP サーバー**

  組織のメールサーバーのアドレスです。

  複数のアドレスを入力する場合はセミコロンで区切ってください。次の値を使用できます：

  - IPv4 / IPv6 アドレス
  - デバイスの Windows ネットワーク名（NetBIOS 名）
  - SMTP サーバーの DNS 名

- **SMTP サーバーのポート**

  SMTP サーバーの通信ポート番号。複数の SMTP サーバーを使用する場合、それらサーバーへの接続は指定された通信ポートを介して確立されます。既定のポート番号は 25 です。

- **ESMTP 認証を使用する**

  ESMTP 認証のサポートを有効にします。チェックボックスをオンにすると、［**ユーザー名**］と［**パスワード**］で ESMTP 認証を設定できます。既定では、このチェックボックスはオフです。

［**テストメッセージの送信**］をクリックして、新しいメール通知設定をテストできます。［**宛先（メールアドレス）**］で指定したアドレスにテストメッセージが問題なく届いた場合、設定は正しく行われています。

ステップ 7：クラウド環境の保護の初期設定の作成

このステップでは、Kaspersky Security Center によってポリシーとタスクが自動的に作成されます。［**初期プロテクションの設定**］ウィンドウには、アプリケーションによって作成されたポリシーとタスクのリストが表示されます。

AWS クラウド環境で RDS データベースを使用する場合は、管理サーバーのバックアップタスクの作成時に Kaspersky Security Center に IAM アクセスキーペアの情報を指定する必要があります。この場合、次のフィールドに値を入力します：

- **S3 バケット名**

  バックアップ用に作成した S3 バケットの名前です。

- **アクセスキーの ID**

  S3 バケットストレージインスタンスを使用するために IAM ユーザーアカウントを作成した時に受け取ったキーの ID（英数字の並び）です。

  このフィールドは、S3 バケット上の RDS データベースを選択した場合に使用可能になります。

- **秘密鍵**

  IAM ユーザーアカウント作成時にアクセスキーの ID と一緒に受け取った秘密鍵です。

  秘密鍵の文字はアスタリスクで表示されます。秘密鍵を入力し始めると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを必要な間だけ押し続けます。

  このフィールドは、IAM ロールではなく AWS IAM アクセスキーを認証のために選択した場合に使用できます。

Azure クラウド環境で Azure SQL データベースを使用する場合は、管理サーバーのバックアップタスクの作成時に Kaspersky Security Center に Azure SQL サーバーに関する情報を指定する必要があります。この場合、次のフィールドに値を入力します：

- **Azure ストレージアカウント名**

  Kaspersky Security Center で使用するために作成した Azure ストレージアカウントの名前です。

- **Azure サブスクリプション ID**

  Azure ポータルで作成したサブスクリプションです。

- **Azure アプリケーションパスワード**

  アプリケーション ID の作成時に取得したアプリケーション ID のパスワードです。

  パスワードの文字はアスタリスクで表示されます。パスワードの入力を開始すると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを押し続けます。

- **Azure アプリケーション ID**

  Azure ポータルで作成したアプリケーション ID です。

  ポーリングやその他の目的で使用する Azure アプリケーション ID を 1 つだけ指定できます。別の Azure セグメントでポーリングを実行する場合は、既存の Azure 接続を事前に削除する必要があります。

- **Azure SQL サーバー名**

  この名前とリソースグループは Azure SQL サーバーのプロパティで確認できます。

- **Azure SQL サーバーリソースグループ**

  この名前とリソースグループは Azure SQL サーバーのプロパティで確認できます。

- **Azure ストレージのアクセスキー**

  情報はストレージアカウントのプロパティの［アクセスキー］セクションで確認できます。いずれのキー（key1 または key2）も使用できます。

管理サーバーを Google Cloud 内に導入する場合、バックアップコピーの保管先となるフォルダーを選択する必要があります。ローカルデバイスのフォルダーまたは仮想マシンインスタンスのフォルダーを選択します。

最小の保護の設定に必要なポリシーとタスクをすべて作成すると、［**次へ**］が使用可能になります。

タスクを実行するはずのデバイスが管理サーバー上で可視でない場合、デバイスが可視になるまでタスクは開始しません。EC2 インスタンスまたは Azure 仮想マシンの新規作成時には、管理サーバー上でインスタンスが認識されるまで時間がかかることがあります。新規作成したすべてのデバイスにできるだけ早くネットワークエージェントとセキュリティ製品をインストールしたい場合は、**アプリケーションのリモートインストール**タスクの設定で［**未実行のタスクを実行する**］がオンになっていることを確認してください。このオプションがオフだと、タスクがスケジュールに従って始まるまで、新規作成されたインスタンスまたは仮想マシンにネットワークエージェントとセキュリティ製品は導入されません。

ステップ 8：インストール中にオペレーティングシステムを再起動する必要がある場合の操作の選択（クラウド環境）

これまでの手順で［**保護の導入**］をオンにした場合、対象デバイスのオペレーティングシステムを再起動しなければならない状況での処理を選択する必要があります。［**保護の導入**］をオンにしていない場合は、このステップは省略します。

アプリケーションのインストール中に、デバイスのオペレーティングシステムを再起動する場合の処理を選択します：

- **デバイスを再起動しない**

  このオプションをオンにすると、セキュリティ製品のインストール後にデバイスが再起動されません。

- **デバイスを再起動する**

  このオプションをオンにすると、セキュリティ製品のインストール後にデバイスが再起動されます。

再起動の前にインスタンス上でセッションがブロックされたすべてのアプリケーションを強制的に終了する場合は、［**セッションがブロックされたアプリケーションを強制終了する**］を選択してください。このチェックボックスがオフの場合は、セッションがブロックされた状態で実行されているすべてのアプリケーションを手動で終了する必要があります。

ステップ 9：管理サーバーによるアップデートの受信

このステップでは、管理サーバーの適切な動作に必要なアップデートをダウンロードする際の進捗状況を表示できます。［**次へ**］をクリックすると、ダウンロードの完了を待たずに、ウィザードの最後のウィンドウに進むことができます。

ウィザードが終了します。

設定の確認

クラウド環境内での利用のために Kaspersky Security Center 15.1 が適切に設定されているか確認するには：

1. Kaspersky Security Center を起動し、管理コンソールを使用して管理サーバーに接続できることを確認します。
2. コンソールツリーで、［**管理対象デバイス**］の［**クラウド**］を選択します。
3. ［**管理対象デバイス**］の［**クラウド**］グループ内の任意のサブグループを表示する時は、そのサブグループの［**デバイス**］タブにすべてのデバイスが表示されていることを確認します。

   デバイスが表示されない場合、手動で対応するクラウドセグメントのポーリングを行ってデバイスを検出できます。
4. ［**ポリシー**］タブに、以下のアプリケーションに対するアクティブなポリシーがあることを確認してください：

   - Kaspersky Security Center ネットワークエージェント
   - Kaspersky Security for Windows Server
   - Kaspersky Endpoint Security for Linux

   リストに表示されていない場合、手動で作成できます。
5. ［**タスク**］タブに次のタスクが表示されていることを確認します：

   - **管理サーバーデータのバックアップ**
   - **Windows Server のアップデートタスク**
   - **管理サーバーのメンテナンス**
   - **管理サーバーのリポジトリへのアップデートのダウンロード**
   - **脆弱性とアプリケーションのアップデートの検索**
   - **Windows の保護をインストール**
   - **Linux の保護をインストール**
   - **Windows Server 簡易スキャンタスク**
   - **簡易スキャン**
   - **Linux 向けアップデートのインストール**

   リストに表示されていない場合、手動で作成できます。

クラウド環境内での利用のために Kaspersky Security Center 15.1 が適切に設定されています。

クラウドデバイスグループ

クラウドデバイスをグループ化して管理することができます。Kaspersky Security Center の初期設定段階で、［**管理対象デバイス**］内に［**クラウド**］管理グループが既定で作成され、ポーリング中に検出されたクラウドデバイスがグループに配置されます。

同期の設定時に［**管理グループ構造をクラウドセグメントと同期する**］チェックボックスをオンにした場合、この管理グループ内のサブグループの構造はクラウドセグメントの構造と同じになります（ただし、AWS では、アベイラビリティーゾーンとプレイスメントグループは構造に反映されません。Azure では、サブネットは構造に反映されません）。ポーリング中に検出された、グループ内の空のサブグループは自動的に削除されます。

すべてのまたは特定のインスタンスをまとめて管理グループを手動で作成することもできます。

既定では、［**管理対象デバイス**］内の［**クラウド**］グループは［**管理対象デバイス**］グループからポリシーとタスクを継承します。該当するポリシーとタスクの設定のプロパティで［**編集を許可**］がオンの場合、設定を変更できます。

ネットワークセグメントのポーリング

管理サーバーでは、AWS API ツール、Azure API ツールまたは Google API ツールを使ったクラウドセグメントに対する定期的なポーリングによって、ネットワーク構造とそのネットワーク上のデバイスに関する情報を受信します。Kaspersky Security Center は、この情報を使用して、［**未割り当てデバイス**］フォルダーと［**管理対象デバイス**］フォルダーの内容を更新します。デバイスが管理グループに自動的に移動するように設定している場合、検出されたデバイスは管理グループに含まれます。

管理サーバーにクラウドセグメントのポーリングを許可するには、IAM ロールまたは IAM ユーザーアカウント（AWS の場合）、アプリケーション ID とパスワード（Azure の場合）、または Google クライアントのメールアドレス、Google プロジェクト ID および秘密鍵によって権限を付与されている必要があります。

各クラウドセグメント用に接続を追加したり削除したりできます。また、各クラウドセグメントのポーリングスケジュールを設定することもできます。

クラウドセグメントのポーリングに使用する接続を追加する

利用可能な接続のリストにクラウドセグメントのポーリングに使用する接続を追加するには：

1. コンソールツリーで、［**デバイスの検索**］→［**クラウド**］フォルダーの順に選択します。
2. このウィンドウの作業領域で［**ポーリングの設定**］をクリックします。
   クラウドセグメントのポーリングに使用できる接続の一覧を含むプロパティウィンドウが開きます。
3. ［**追加**］をクリックします。
   ［**接続**］ウィンドウが表示されます。
4. クラウドセグメントのポーリングに使用する接続について、クラウド環境の名前を指定します：

   クラウド環境

   EC2 インスタンスまたは仮想マシンを配置する環境は、Amazon Web Services （AWS）、Microsoft Azure、または Google Cloud から選択できます。

   AWS を選択した場合は、次の設定を指定してください：

- **接続名**

  接続の名前を入力します。名前を 256 文字以上にすることはできません。Unicode 文字のみを使用できます。

  この名前はクラウドデバイスの管理グループの名前としても使用されます。

  複数のクラウド環境を使用する予定の場合は、たとえば「Azure Segment」「AWS Segment」「Google Segment」のように、環境の名前を接続名に含めることを検討してください。

- **AWS IAM ロールを使用**

  既に AWS サービスで使用する管理サーバー用 IAM ロールを作成している場合、このオプションを選択します。

- **AWS IAM ユーザーアカウントを使用**

  必要な権限がある IAM ユーザーアカウントがある場合、このオプションを選択し、キーの ID と秘密鍵を入力します。

  - **アクセスキーの ID**

    IAM アクセスキーの ID（英数字の並び）：IAM ユーザーアカウント作成時に受け取ったキーの ID です。

    このフィールドは、IAM ロールではなく AWS IAM アクセスキーを認証のために選択した場合に使用できます。

  - **秘密鍵**

    IAM ユーザーアカウント作成時にアクセスキーの ID と一緒に受け取った秘密鍵です。

    秘密鍵の文字はアスタリスクで表示されます。秘密鍵を入力し始めると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを必要な間だけ押し続けます。

    このフィールドは、IAM ロールではなく AWS IAM アクセスキーを認証のために選択した場合に使用できます。

クラウド環境設定ウィザードでは、AWS IAM のアクセスキーを 1 つだけ指定することができます。その後で、追加の接続を指定して、他のクラウドセグメントを管理することもできます。

Azure を選択した場合は、次の設定を指定してください：

- **接続名**

  接続の名前を入力します。名前を 256 文字以上にすることはできません。Unicode 文字のみを使用できます。

  この名前はクラウドデバイスの管理グループの名前としても使用されます。

  複数のクラウド環境を使用する予定の場合は、たとえば「Azure Segment」「AWS Segment」「Google Segment」のように、環境の名前を接続名に含めることを検討してください。

- **Azure アプリケーション ID**

Azure ポータルで作成したアプリケーション ID です。

ポーリングやその他の目的で使用する Azure アプリケーション ID を 1 つだけ指定できます。別の Azure セグメントでポーリングを実行する場合は、既存の Azure 接続を事前に削除する必要があります。

- **Azure サブスクリプション ID**

  Azure ポータルで作成したサブスクリプションです。

- **Azure アプリケーションパスワード**

  アプリケーション ID の作成時に取得したアプリケーション ID のパスワードです。

  パスワードの文字はアスタリスクで表示されます。パスワードの入力を開始すると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを押し続けます。

- **Azure ストレージアカウント名**

  Kaspersky Security Center で使用するために作成した Azure ストレージアカウントの名前です。

- **Azure ストレージのアクセスキー**

  パスワード（アクセスキー）は Kaspersky Security Center で使用する Azure ストレージアカウントを作成した時に取得したものです。

  キーは、Azure ストレージアカウントの概要セクションのアクセスキーに関するサブセクションで確認できます。

Google Cloud を選択した場合は、次の設定を指定してください：

- **接続名**

  接続の名前を入力します。名前を 256 文字以上にすることはできません。Unicode 文字のみを使用できます。

  この名前はクラウドデバイスの管理グループの名前としても使用されます。

  複数のクラウド環境を使用する予定の場合は、たとえば「Azure Segment」「AWS Segment」「Google Segment」のように、環境の名前を接続名に含めることを検討してください。

- **クライアントのメール**

  クライアントのメールアドレスは、Google Cloud でプロジェクトの登録に使用したメールアドレスです。

- **プロジェクト ID**

  プロジェクト ID は、Google Cloud でプロジェクトの登録時に取得した ID です。

- **秘密鍵**

  秘密鍵は、Google Cloud でプロジェクトの登録時に秘密鍵として取得した文字列です。間違えないように、この文字列をコピーして貼り付けることを検討してください。

5. 必要に応じて、［**ポーリングのスケジュールを設定する**］を選択し既定の設定を変更します。

   この接続は本製品の設定に保存されます。

追加したクラウドセグメントの初回ポーリング後、このセグメントに対応するサブグループが［**管理対象デバイス**］の［**クラウド**］管理グループに表示されます。

誤った資格情報を指定した場合、クラウドセグメントのポーリング中、インスタンスは検出されず、新しいサブグループは［**管理対象デバイス**］の［**クラウド**］管理グループに表示されません。

クラウドセグメントのポーリングに使用した接続を削除する

特定のクラウドセグメントをポーリングする必要がなくなった場合、使用可能な接続リストから、そのセグメントに対応する接続を削除できます。また、クラウドセグメントをポーリングするための権限が別のライセンスを使用している AWS IAM ユーザーに移された場合にも、接続を削除できます。

接続を削除するには：

1. コンソールツリーで、［**デバイスの検索**］→［**クラウド**］フォルダーの順に選択します。
2. ウィンドウの作業領域で、［**ポーリングの設定**］を選択します。
   クラウドセグメントのポーリングに使用できる接続の一覧を含むウィンドウが開きます。
3. 削除する接続を選択して、ウィンドウ右側の［**削除**］をクリックします。
4. 表示されたウィンドウで、［OK］をクリックして処理を確定します。

使用可能な接続のリストから接続を削除する場合、対応するセグメント内のデバイスも、対応する管理グループから自動的に削除されます。

ポーリングスケジュールの設定

クラウドセグメントのポーリングは、スケジュールに従って実行されます。ポーリングの頻度が設定可能です。

ポーリング頻度は、クラウド環境の設定で自動的に 5 分に設定されています。この値はいつでも変更でき、別のスケジュールを設定することができます。ポーリングの実行を 5 分間隔より多い頻度に設定しないでください。AWS API 操作にエラーが生じる可能性があります。

クラウドセグメントのポーリングスケジュールを設定するには：

1. コンソールツリーで、［**デバイスの検索**］→［**クラウド**］フォルダーの順に選択します。

2. 作業領域で［**ポーリングの設定**］をクリックします。
   クラウドのプロパティウィンドウが開きます。

3. リストから目的の接続を選択し、［**プロパティ**］をクリックします。
   接続のプロパティウィンドウが開きます。

4. プロパティウィンドウで［**ポーリングのスケジュールを設定する**］をクリックします。
   ［**スケジュール**］ウィンドウが表示されます。

5. 次の設定を定義します：

   - **実行予定**
     ポーリングスケジュールのオプション：

     - **N 日ごと**

       指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。
       既定では、現在のシステム日時から、1 日ごとにポーリングが実行されます。

     - **N 分ごと**

       指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。
       既定では、現在のシステム時刻から、5 分ごとにポーリングが実行されます。

     - **曜日ごと**

       指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。
       既定では、毎週金曜日の午後 6 時にポーリングが実行されます。

     - **毎月、選択した週の指定日**

       毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。
       既定では、月内のいかなる日付も選択されておらず、開始時刻は午後 6 時です。

   - **未実行のタスクを実行する**

     ポーリングの実行がスケジュールされていた時刻に管理サーバーがオフまたは接続できなかった場合は、管理サーバーがオンになった時に即座にポーリングを実行させるか、ポーリングの次回のスケジュールまで待機するかを選択できます。
     このオプションをオンにすると、管理サーバーがオンになるとすぐにポーリングを開始します。
     このオプションをオフにすると、管理サーバーはポーリングの次回のスケジュールまでポーリングの実行を待機します。
     既定では、このオプションはオンです。

6. ［**OK**］をクリックして変更内容を保存します。

ポーリングのスケジュールが設定され保存されます。

クラウド環境のデバイスへのアプリケーションのインストール

クラウド環境のデバイスには、カスペルスキー製品の Kaspersky Security for Windows Server（Windows デバイス用）と Kaspersky Endpoint Security for Linux（Linux デバイス用）をインストールできます。

保護機能をインストールする予定のクライアントデバイスは、クラウド環境での Kaspersky Security Center の動作のための要件を満たしていなければなりません。AWS インスタンス、Microsoft Azure 仮想マシン、または Google 仮想マシンインスタンスへの製品のインストールには、有効なライセンスが必要です。

Kaspersky Security Center 15.1 では次の利用シナリオがサポートされます。

- クライアントデバイスが API によって検出され、製品のインストールも API によって実行される。AWS と Azure のクラウド環境では、このシナリオがサポートされます。
- クライアントデバイスが Active Directory のポーリング、Windows ドメインのポーリング、IP アドレス範囲のポーリングのいずれかで検出され、製品のインストールが Kaspersky Security Center によって実行される。
- クライアントデバイスが Google API によって検出され、製品のインストールが Kaspersky Security Center によって実行される。Google Cloud では、このシナリオのみがサポートされます。

その他の製品インストール方法はサポートされていません。

仮想デバイスにアプリケーションをインストールするには、インストールパッケージを使用します。

AWS API または Azure API を使用してインスタンスにアプリケーションのリモートインストール用のタスクを作成するには：

1. コンソールツリーで、［**タスク**］フォルダーを選択します。
2. ［**新規タスク**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. ［**タスク種別の選択**］ウィンドウで、タスク種別として［**アプリケーションのリモートインストール**］を選択します。
4. ［**デバイスの選択**］ウィンドウで、［**管理対象デバイス**］の［**クラウド**］グループから目的のデバイスを選択します。
5. アプリケーションをインストールする予定のデバイスにまだネットワークエージェントがインストールされていない場合、［**タスクを実行するアカウントの選択**］ウィンドウで［**アカウントが必要（ネットワークエージェントの使用なし）**］を選択し、ウィンドウの右側にある［**追加**］をクリックします。表示されるメニューで、次のいずれかを選択します：
   - **クラウドアカウント**

AWS 環境のインスタンスにアプリケーションをインストール予定で、必要な権限が設定された AWS IAM アクセスキーを保有しているが IAM ロールがない場合、このオプションを選択します。Azure 環境のデバイスにアプリケーションをインストールしたい場合にもこのオプションを選択します。

表示されたウィンドウで、目的のデバイスにアプリケーションをインストールする権限を付与する認証情報を入力します。

クラウド環境を選択します：AWS または Azure。

［**アカウント名**］に、これらの認証情報の名前を入力します。タスクを実行するアカウントのリストにこの名前が表示されます。

AWS を選択した場合、［**アクセスキーの ID**］と［**秘密鍵**］に、指定したデバイスにアプリケーションをインストールする権限のある IAM ユーザーアカウントの認証情報を入力します。

Azure を選択した場合、［**Azure サブスクリプション ID**］と［**Azure アプリケーションパスワード**］に、指定したデバイスにアプリケーションをインストールする権限のある Azure アカウントの認証情報を入力します。

誤った認証情報を入力した場合、リモートインストールタスクをスケジュール設定したデバイス上で、タスクはエラー終了します。

- **アカウント**

  Windows を実行しているインスタンスでは、AWS または Azure の API ツールを使用してアプリケーションをインストールする予定がない場合は、このオプションを選択します。この場合、クラウドセグメントのデバイスが、要件を満たすことを確認してください。AWS API と Azure API のどちらも使用せずに Kaspersky Security Center 内にアプリケーションをインストールします。

  誤ったデータを入力した場合、リモートインストールタスクをスケジュール設定したデバイス上で、タスクはエラー終了します。

- **IAM ロール**

  AWS 環境のインスタンスにアプリケーションをインストール予定で、必要な権限が設定された IAM ロールを保有している場合、このオプションを選択します。

  このオプションを選択して、必要な権限が設定された IAM ロールを保有していなかった場合、リモートインストールタスクをスケジュール設定したデバイス上で、タスクはエラー終了します。

- **SSH 証明書**

  Linux を実行しているインスタンスでは、AWS または Azure の API ツールを使用してアプリケーションをインストールする予定がない場合は、このオプションを選択します。この場合、クラウドセグメントのデバイスが、要件を満たすことを確認してください。AWS API と Azure API のどちらも使用せずに Kaspersky Security Center 内にアプリケーションをインストールします。

  SSH 証明書の秘密鍵を指定するには、ssh-keygen ユーティリティを使用して生成できます。Kaspersky Security Center は PEM 形式の秘密鍵をサポートしますが、ssh-keygen ユーティリティは既定で SSH 鍵を OPENSSH 形式で生成します。OPENSSH 形式は Kaspersky Security Center ではサポートされていません。サポートされる PEM 形式で秘密鍵を作成するには、ssh-keygen コマンドに `-m PEM` オプションを追加します。例：

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<ユーザーのメールアドレス>"
  ```

新しい認証情報ごとに［**追加**］をクリックすると、複数の認証情報を提供できます。クラウドセグメント間で異なる認証情報が必要な場合は、すべてのセグメントに対して認証情報を提供します。

ウィザード終了後に、アプリケーションのリモートインストール用のタスクが［**タスク**］フォルダーの作業領域のタスクのリストに表示されます。

Microsoft Azure の仮想マシンにセキュリティ製品をインストールすると、仮想マシンにインストールされているカスタムスクリプト拡張機能が削除される場合があります。

クラウドデバイスのプロパティの表示

クラウドデバイスのプロパティを表示するには：

1. コンソールツリーの［**デバイスの検索**］→［**クラウド**］フォルダーで、関連するインスタンスが置かれているグループに対応するサブフォルダーを選択します。

   関連する仮想デバイスが置かれているグループがわからない場合は、検索機能を使用します：

   a. ［**管理対象デバイス**］→［**クラウド**］フォルダーを右クリックし、コンテキストメニューで**検索**を選択します。

   b. 表示されたウィンドウで検索を実行します。

      設定した条件を満たすデバイスが存在する場合、その名前と詳細がウィンドウ下部に表示されます。

2. 関連するノードの名前を右クリックします。コンテキストメニューから［**プロパティ**］を選択します。

   開いたウィンドウに、オブジェクトのプロパティが表示されます。

   ［**システム情報**］→［システム全般情報］セクションには、クラウド環境のデバイスに固有のプロパティがあります：

   - **API を使用して検出されたデバイス**（**AWS**、**Azure**、または **Google Cloud**。API ツールを使用してデバイスを検出できない場合は、［**いいえ**］という値が表示されます）。
   - **クラウドのリージョン**。
   - **クラウドの VPC**（AWS と Google Cloud デバイスのみ）。
   - **クラウドのアベイラビリティーゾーン**（AWS と Google Cloud デバイスのみ）。
   - **クラウドのサブネット**。
   - **クラウドのプレイスメントグループ**（この単位はインスタンスがプレイスメントグループに属している場合のみ表示され、それ以外の場合は表示されません）。

   ［**ファイルへのエクスポート**］をクリックして、この情報を CSV ファイルまたは TXT ファイルにエクスポートできます。

クラウドとの同期

クラウド環境の設定の操作中に、［クラウドと同期］ルールが自動的に作成されます。このルールにより、各ポーリング中に見つかったインスタンスが［**未割り当てデバイス**］グループから［**管理対象デバイス**］の［**クラウド**］グループに自動的に移動されるため、インスタンスを一元管理することが可能になります。既定では、ルールは作成後にアクティブになります。ルールはいつでも無効にしたり、実行したりすることができます。

［クラウドと同期］ルールのプロパティを変更する、またはルールを実行するには：

1. コンソールツリーで、［**デバイスの検索**］フォルダーを右クリックします。
2. コンテキストメニューから［**プロパティ**］を選択します。
3. **プロパティ**ウィンドウが開いたら、［**セクション**］ペインで［**デバイスの移動**］を選択します。
4. 作業領域のデバイス移動ルールのリストで［**クラウドと同期**］ルールを選択し、ウィンドウ下部にある［**プロパティ**］をクリックします。

   ルールのプロパティウィンドウが開きます。
5. 必要に応じて、［**クラウドセグメント**］設定グループで次の設定を指定します：

   - **デバイスがクラウドセグメント内にある**

     選択したクラウドセグメント内にあるデバイスにのみルールが適用されるようになります。オフにすると、検出されたすべてのデバイスにルールが適用されます。

     既定では、このオプションがオンです。

     - **子オブジェクトも含む**

       選択されたセグメント内およびネストされたすべてのクラウドサブセクション内の全デバイスにルールが適用されるようになります。オフにすると、ルートセグメント内にあるデバイスにのみルールが適用されます。

       既定では、このオプションがオンです。

     - **デバイスをネストされたオブジェクトから対応するサブグループに移動する**

       このオプションをオンにすると、ネストされたオブジェクトのデバイスがその構造に対応するサブグループに自動的に移動します。

       このオプションをオフにすると、ネストされたオブジェクトのデバイスがクラウドサブグループのルートに移動し、ルートより下の分岐は行われません。

       既定では、このオプションはオンです。

       - **新しく検出されたデバイスの配置階層に対応するサブグループを作成する**

このオプションをオンにすると、デバイスが含まれるセクションに対応するサブグループが［**管理対象デバイス**］の［**クラウド**］グループの階層構造にない場合は、Kaspersky Security Center で対応するサブグループが作成されます。たとえば、デバイスの検索中に新しいサブネットが検出された場合、同じ名前のグループが［**管理対象デバイス**］の［**クラウド**］グループの下に新規に作成されます。

このオプションをオフにすると、Kaspersky Security Center で新しいサブグループは作成されません。たとえば、ネットワークのポーリング中に新しいサブネットが検出された場合、［**管理対象デバイス**］の［**クラウド**］グループにサブネットと同じ名前のグループが新規に作成されることはなく、サブネットに含まれていたデバイスは［**管理対象デバイス**］の［**クラウド**］グループに移動されます。

既定では、このオプションはオンです。

- **クラウドセグメントで何も検出されなかったサブグループを削除する**

  このチェックボックスをオンにすると、既存のクラウドオブジェクトのセクションに対応していないすべてのサブグループがクラウドグループから削除されます。

  このオプションをオフにすると、既存のクラウドオブジェクトのセクションに対応しないサブグループもすべて保持されます。

  既定では、このオプションはオンです。

クラウド環境の設定の実行時に［**クラウドと同期**］をオンにした場合、［**新しく検出されたデバイスのコンテナーに対応するサブグループを作成する**］と［**クラウドセグメントで一致が見つからないサブグループを削除する**］が選択された状態で［クラウドと同期］ルールが作成されます。

［**クラウドと同期**］がオフになっていると、作成される［クラウドと同期］ルール内の前述のオプションはオフになります。お使いの Kaspersky Security Center で、［**管理対象デバイス**］の［**クラウド**］サブグループ内にあるサブグループの構造とクラウドセグメントの構造が一致する必要がある場合、［**新しく検出されたデバイスの配置階層に対応するサブグループを作成する**］と［**クラウドセグメントで何も検出されなかったサブグループを削除する**］をオンにして、ルールを実行します。

6. ［**API を使用して検出されたデバイス**］から、次のいずれかの値を選択します：
   - **AWS**：AWS API を使用して検出されたデバイスで、これはデバイスが間違いなく AWS クラウド環境にあることを意味します。
   - **Azure**：Azure API を使用して検出されたデバイスで、これはデバイスが間違いなく Azure クラウド環境にあることを意味します。
   - **Google Cloud**：Google API を使用して検出されたデバイスで、これはデバイスが間違いなく Google Cloud 環境にあることを意味します。
   - ［**いいえ**］。デバイスは AWS API、Azure API、Google API のいずれでも検出できません。これはデバイスがクラウド環境外にあるか、クラウド環境内にあるが API では検出できないことを意味します。
7. **値なし**：この条件は当てはまりません。必要に応じて、他のセクションで他のルールのプロパティを設定します。
8. 必要に応じて、ウィンドウの下部にある［**強制実行**］をクリックしてルールを実行します。

   ルール実行ウィザードが開始します。ウィザードの指示に従ってください。ウィザードが完了すると、ルールが実行され、［**管理対象デバイス**］の［**クラウド**］サブグループ内にあるサブグループの構造がお使いのクラウド環境の構造と一致するようになります。
9. ［**OK**］をクリックします。

プロパティが設定され保存されます。

［クラウドと同期］ルールを無効にするには：

1. コンソールツリーで、［**デバイスの検索**］フォルダーを右クリックします。
2. コンテキストメニューから［**プロパティ**］を選択します。
3. **プロパティ**ウィンドウが開いたら、［**セクション**］ペインで［**デバイスの移動**］を選択します。
4. 作業領域のデバイス移動ルールのリストで［**クラウドと同期**］ルールをオフにし、ウィンドウ下部にある［OK］をクリックします。

ルールは無効になり、以降は適用されなくなります。

セキュリティ製品導入を目的とした導入スクリプトの使用

Kaspersky Security Center がクラウド環境に導入されている場合は、導入スクリプトを使用してセキュリティ製品の導入を自動化できます。Amazon Web Services、Microsoft Azure、Google Cloud の導入スクリプトは、カスペルスキーのサポートページで ZIP ファイル形式で入手できます。

導入スクリプトを使用して Kaspersky Endpoint Security for Linux と Kaspersky Security for Windows Server の最新バージョンを導入できるのは、これらのプログラムとプログラム用の管理プラグインのインストールパッケージが作成済みである場合のみです。導入スクリプトを使用してセキュリティ製品の最新バージョンを導入するには、クラウド環境の管理サーバーで次の操作を実行します：

1. クラウド環境の設定を起動します。
2. https://support.kaspersky.co.jp/14713 に記載されている手順に従います。

Yandex.Cloud での Kaspersky Security Center の導入

Yandex.Cloud に Kaspersky Security Center を導入できます。従量課金制モードのみが利用可能です。クラウドデータベースはサポートされていません。

Yandex.Cloud では、セキュリティ製品に次の導入方法を使用できます：

- Kaspersky Security Center のネイティブな方法による、つまり*リモートインストールタスク*を介する方法（セキュリティプログラムの導入は、管理サーバーと保護対象の仮想マシンが同じネットワークセグメント上にある場合にのみ可能です）
- 導入スクリプトを使用する方法

Yandex.Cloud に Kaspersky Security Center を導入するには、Yandex.Cloud にサービスアカウントが必要です。このアカウントに marketplace.meteringAgent 権限を付与し、このアカウントを仮想マシンに関連付ける必要があります（詳細については、https://cloud.yandex.com/en を参照してください）。

補足情報

このセクションでは、Kaspersky Security Center を使用する上での参考情報と追加情報を説明します。

詳細機能

このセクションでは、デバイス上のアプリケーションの一元管理機能を拡張するために設計された、様々な Kaspersky Security Center のオプションについて説明します。

Kaspersky Security Center 処理の自動化：klakaut ユーティリティ

klakaut ユーティリティを使用して、Kaspersky Security Center の処理を自動化できます。klakaut ユーティリティとそのヘルプは、Kaspersky Security Center のインストールフォルダーにあります。

カスタムツール

Kaspersky Security Center で、*カスタムツール*（単に *ツール*とも表記）のリスト、つまり、コンテキストメニューの［**カスタムツール**］セクションを使用して管理コンソールからクライアントデバイスでアクティブ化するアプリケーションのリストを作成できます。リストの各ツールは別個のメニューコマンドに関連付けられ、管理コンソールでは、そのコマンドを使用してツールに対応するアプリケーションを起動します。

アプリケーションは管理コンピューターで起動します。リモートクライアントデバイスの属性（NetBIOS 名、DNS 名、IP アドレス）をコマンドラインの引数として指定できます。トンネリングを使用して、リモートデバイスへの接続を確立できます。

カスタムツールの既定のリストには、クライアントデバイスごとに次のサービスプログラムが含まれます：

- **リモート診断** – Kaspersky Security Center のリモート診断ユーティリティ
- **リモートデスクトップ** – 標準の Microsoft Windows リモートデスクトップ接続コンポーネント
- **コンピューターの管理** – 標準の Microsoft Windows コンポーネント

カスタムツールを追加、削除、またはまたはその設定を編集するには：

クライアントデバイスのコンテキストメニューから、［**カスタムツール**］→［**カスタムツールの設定**］の順に選択します。

［**カスタムツール**］ウィンドウが開きます。このウィンドウでは、［**追加**］ボタンや［**変更**］ボタンを使用して、カスタム ツールを追加したり、その設定を編集したりできます。カスタム ツールを削除するには、赤い十字アイコンをクリックします（❌）。

ネットワークエージェントのディスククローンモード

新しいデバイスにソフトウェアをインストールする際、基準となるデバイスのハードディスクを複製する方法が一般的です。基準となるデバイスのハードディスク上でネットワークエージェントが標準モードで動作していると、次の問題が発生します：

新しいデバイス上に、ネットワークエージェントを含む基準ディスクイメージが導入されると、管理コンソール上ではそれらのデバイスが1つのアイコンとして表示されます。この問題は、管理サーバーが管理コンソール上でデバイスとアイコンを関連付けるために使用する内部データが、複製の結果として新しいデバイスで同一になるために発生します。

*ネットワークエージェントのディスククローンモード*を使用すると、複製後、管理コンソール上での新しいデバイスの表示の問題を回避できます。新しいデバイスに、ディスクを複製してネットワークエージェントとソフトウェアを導入する場合はこのモードを使用します。

ディスククローンモードでは、ネットワークエージェントは動作を継続しますが、管理サーバーには接続しません。ネットワークエージェントは、クローンモードを終了する時に、管理コンソール上で管理サーバーが複数のデバイスを単一のアイコンに関連付ける原因となる内部データを削除します。基準デバイスのイメージの複製が完了すると、新しいデバイスが管理コンソール上で正しく（個別のアイコンで）表示されます。

ネットワークエージェントのディスククローンモードの使用シナリオ

1. 基準となるデバイスにネットワークエージェントをインストールします。
2. ネットワークエージェントの管理サーバーへの接続を klnagchk ユーティリティを使用して確認します。
3. ネットワークエージェントのディスククローンモードを有効にします。
4. ソフトウェアとパッチをデバイスにインストールし、必要な回数再起動します。
5. 基準デバイスのハードディスクを必要な数のデバイス上に複製します。
6. 複製されたコピーは次の条件を満たす必要があります：
   a. デバイス名を変更する必要があります。
   b. デバイスを再起動する必要があります。
   c. ディスククローンモードを無効にする必要があります。

Klmover ユーティリティを使用したディスククローンモードの有効化および無効化

ネットワークエージェントのディスククローンモードを有効または無効にするには：

1. ネットワークエージェントがインストールされた複製元デバイス上で klmover ユーティリティを実行します。
   Klmover ユーティリティはネットワークエージェントのインストールフォルダーにあります。
2. ディスククローンモードを有効にするには、Windows コマンドプロンプトで次のコマンドを入力します：`klmover -cloningmode 1`
   ネットワークエージェントがディスククローンモードに切り替わります。
3. ディスククローンモードの現在のステータスを要求するには、コマンドプロンプトで次のコマンドを入力します：`klmover -cloningmode`
   ユーティリティウィンドウに、ディスククローンモードが有効か無効かが表示されます。
4. ディスククローンモードを無効にするには、ユーティリティのコマンドラインで次のコマンドを入力します：`klmover -cloningmode 0`

オペレーティングシステムのイメージを作成するために、ネットワークエージェントがインストールされた基準デバイスを準備する

ネットワークエージェントがインストールされた基準デバイスのオペレーティングシステムイメージを作成し、ネットワーク内のデバイスにイメージを導入することができます。この場合、ネットワークエージェントがまだ起動されていない基準デバイスのオペレーティングシステムイメージを作成します。オペレーティングシステムイメージを作成する前に基準デバイスでネットワークエージェントを起動すると、基準デバイスのオペレーティングシステムイメージから導入されたデバイスの管理サーバーの識別に問題が生じます。

オペレーティングシステムのイメージを作成するための基準デバイスを準備するには：

1. Windows オペレーティングシステムが基準デバイスにインストールされていることを確認し、そのデバイスに必要な他のソフトウェアをインストールします。

2. 基準デバイスの Windows ネットワークの接続設定で、Kaspersky Security Center がインストールされているネットワークから基準デバイスを切断します。

3. 基準デバイスで、setup.exe ファイルを使用してネットワークエージェントのローカルインストールを開始します。

   Kaspersky Security Center ネットワークエージェントのセットアップウィザードが起動します。ウィザードの指示に従ってください。

4. ウィザードの［**管理サーバー**］ページで、管理サーバーの IP アドレスを指定します。

   管理サーバーの正確なアドレスがわからない場合は、「localhost」と入力します。klmover ユーティリティで `-address` キーを使用することにより、後で IP アドレスを変更できます。

5. ウィザードの［**アプリケーションの開始**］ページで、［**インストール中にアプリケーションを開始する**］を無効にします。

6. ネットワークエージェントのインストールが完了したら、オペレーティングシステムイメージを作成する前にデバイスを再起動しないでください。

   デバイスを再起動する場合、オペレーティングシステムイメージを作成するために基準デバイスを準備するプロセス全体を繰り返す必要があります。

7. 参照デバイスでのコマンドラインで［sysprep ユーティリティ］を起動し、コマンド「`sysprep.exe /generalize /oobe /shutdown`」を実行します。

基準デバイスでオペレーティングシステムイメージを作成する準備が整いました。

ファイル変更監視からのメッセージの受信設定

Kaspersky Security for Windows Server や Kaspersky Security for Virtualization Light Agent などの管理対象製品は、ファイル変更監視コンポーネントからのメッセージを Kaspersky Security Center に転送します。また、Kaspersky Security Center を使用すると、システムの基幹コンポーネント（Web サーバーや ATM など）への変更を監視し、そのようなシステムの整合性違反に迅速に対応できます。監視と迅速な対応のために、ファイル変更監視からメッセージを受信できます。ファイル変更監視コンポーネントとの連携により、デバイスのファイルシステムだけでなく、そのレジストリエントリ、ファイアウォールのステータス、接続されたハードウェアのステータスも監視できます。

Kaspersky Security for Windows Server または Kaspersky Security for Virtualization Light Agent を使用せずにファイル変更監視からのメッセージを受信するには、Kaspersky Security Center を設定する必要があります。

ファイル変更監視からのメッセージの受信を設定するには：

1. 管理サーバーがインストールされたデバイスのシステムレジストリを開きます（たとえば、ローカルで［**スタート**］→［**ファイル名を指定して実行**］で regedit コマンドを使用します）。
2. 次のレジストリエントリに移動します：
   - 32 ビットシステム：

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - 64 ビットシステム：

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF
3. キーを作成します：
   - KLSRV_EVP_FIM_PERIOD_SEC キーを作成して、処理されたイベント数を数える期間を指定します。次の設定を指定します：
     a. キーの名前に KLSRV_EVP_FIM_PERIOD_SEC を指定します。
     b. キーの種別に DWORD を指定します。
     c. 43,200 ～ 172,800 秒の間で間隔の値を指定します。既定では、間隔は 86,400 秒です。
   - KLSRV_EVP_FIM_LIMIT キーを作成して、指定の期間中に受信するイベント数を制限します。次の設定を指定します：
     a. キーの名前に KLSRV_EVP_FIM_LIMIT を指定します。
     b. キーの種別に DWORD を指定します。
     c. 2,000 ～ 50,000 の間で受信イベントの範囲を指定します。既定のイベント数は 20,000 です。
   - KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC キーを作成して、一定の期間の間、イベントを正確に数えます。次の設定を指定します：
     a. キーの名前に KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC を指定します。
     b. キーの種別に DWORD を指定します。
     c. 120 ～ 600 秒の間で範囲を指定します。既定の期間は 300 秒です。
   - 一定期間が経過した後、期間中に処理されたイベント数が指定の制限より少ないかどうかをアプリケーションが確認できるように、KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC キーを作成します。この確認は、受信イベント数が制限に達すると実行されます。この条件が満たされると、データベースへのイベントの保存が再開されます。次の設定を指定します：
     a. キーの名前に KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC を指定します。
     b. キーの種別に DWORD を指定します。
     c. 600 ～ 3,600 秒の間で範囲を指定します。既定の期間は 1,800 秒です。

キーを作成しない場合、既定値が使用されます。

4. 管理サーバーサービスを再起動します。

ファイル変更監視からの受信イベント数の制限が設定されます。ファイル変更監視の結果に関する情報は、「**デバイスで適用された回数が多い 10 個のファイル変更監視 / システム整合性監視ルール**」および「**ファイル変更監視 / システム整合性監視ルールの適用回数が多い 10 台のデバイス**」というレポートで確認できます。

管理サーバーのメンテナンス

管理サーバーのメンテナンスにより、管理サーバーのフォルダー内のスペースを解放し、不要になったオブジェクトを削除して定義データベースのサイズを縮小できます。これにより、アプリケーションのパフォーマンスと動作の信頼性が向上します。管理サーバーのメンテナンスを少なくとも週に 1 回実行することを推奨します。

管理サーバーのメンテナンスは、専用のタスクで実施されます。管理サーバーのメンテナンス時、次の処理が実行されます：

- ストレージフォルダーから不要なフォルダとファイルを削除します。
- テーブルから不要なレコード（「ダングリングポインター」とも呼ばれます）を削除します。
- キャッシュをクリアします。
- 定義データベースを管理します（DBMS として SQL Server または PostgreSQL を使用する場合）：
  - 定義データベースのエラーをチェックします（SQL Server でのみ使用可能）
  - データベースのインデックスを再編成する
  - データベースの統計情報を更新する
  - データベースを縮小する（必要に応じて）

*管理サーバーのメンテナンス*タスクは、MariaDB バージョン 10.3 以降をサポートします。MariaDB バージョン 10.2 以前を使用する場合、管理者はこの DBMS を独自に維持する必要があります。

管理サーバーのメンテナンスを作成するには：

1. コンソールツリーで、*管理サーバーのメンテナンス*タスクを作成する管理サーバーのノードを選択します。
2. ［**タスク**］フォルダーを選択します。
3. ［**タスク**］フォルダーの作業領域の［**新規タスク**］をクリックします。
   新規タスクウィザードが起動します。
4. ウィザードの［**タスク種別の選択**］ウィンドウで、タスク種別として［**管理サーバーのメンテナンス**］を選択して、［**次へ**］をクリックします。
5. メンテナンス時に管理サーバーのデータベースを縮小する場合は、ウィザードの［**設定**］ウィンドウで、［**データベースを縮小する**］をオンにします。

6. 引き続きウィザードの指示に従って操作します。

新規作成されたタスクが、［**タスク**］フォルダーの作業領域のタスクのリストに表示されます。1台の管理サーバーに対して実行できる*管理サーバーのメンテナンス*タスクは1つのみです。管理サーバーに対して、既に*管理サーバーのメンテナンス*タスクが作成されている場合は、新たに*管理サーバーのメンテナンス*タスクを作成することはできません。

パブリック DNS サーバーへのアクセス

システム DNS を使用してカスペルスキーのサーバーにアクセスできない場合、Kaspersky Security Center では、以下のパブリック DNS サーバーを次の順序で使用できます：

1. Google Public DNS （8.8.8.8）
2. Cloudflare DNS（1.1.1.1）
3. Alibaba Cloud DNS（223.6.6.6）
4. Quad9 DNS（9.9.9.9）
5. CleanBrowsing（185.228.168.168）

DNS サーバーへの TCP/UDP 接続を確立するため、これらの DNS サーバーへの要求にはドメインアドレスと管理サーバーのパブリック IP アドレスが含まれる場合があります。Kaspersky Security Center がパブリック DNS サーバーを使用している場合、データ処理は関連するサービスのプライバシーポリシーによって管理されます。

klscflag ユーティリティを使ってパブリック DNS の使用を設定するには、次の手順を実行します：

1. Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。
2. パブリック DNS の使用を無効にするには、次のコマンドを実行します：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. パブリック DNS の使用を有効にするには、次のコマンドを実行します：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

［ユーザー通知方法］ウィンドウ

［**ユーザー通知方法**］ウィンドウでは、モバイルデバイスへの証明書のインストールをユーザーに通知する方法を設定できます：

- **ウィザード内で QR コードを表示**：このオプションをオンにすると、モバイルデバイスの接続ウィザードの最後の手順で、インストールパッケージへのリンクが表示されます。
- **QR コードをユーザーに送信**：このオプションをオンにすると、デバイスの接続に関するユーザーへの通知を設定できます。

［**メール**］セクションで、新規証明書をユーザーのモバイルデバイスへインストールしたことをメールで伝えるユーザー通知を設定できます。この通知方法は、SMTP サーバーが有効な場合のみ使用できます。

［**SMS 経由**］セクションで、証明書をユーザーのモバイルデバイスへインストールしたことを SMS で伝えるユーザー通知を設定できます。この通知方法は、SMS 通知が有効な場合のみ使用できます。

必要に応じて、［**メール**］または［**SMS 経由**］の［**メッセージの編集**］をクリックし、通知メッセージを表示して編集します。

［デバイスの抽出］ウィンドウ

［**デバイスの抽出**］リストから選択します。リストには、事前に定義された選択項目と、ユーザーが作成した選択項目が含まれています。

［**デバイスの抽出**］フォルダーの作業領域で、デバイスの抽出の詳細を表示できます。

新しいオブジェクトに名前を設定するためのウィンドウ

ウィンドウで、新しく作成したオブジェクトの名前を指定します。名前は 100 文字以内で指定します。特殊文字（"*<>?\:|）は使用できません。

［アプリケーションカテゴリ］セクション

このセクションでは、クライアントデバイスに対するアプリケーションカテゴリ情報の配信を設定できます。

全データ（ネットワークエージェント 10 Service Pack 2 以前で使用可能）

このオプションをオンにすると、アプリケーションカテゴリが変更された時、カテゴリのすべてのデータがクライアントデバイスに転送されます。このデータ転送オプションは、ネットワークエージェント Service Pack 2 以前のバージョンで使用します。

変更されたデータのみ（ネットワークエージェント 10 Service Pack 2 およびそれ以降で使用可能）

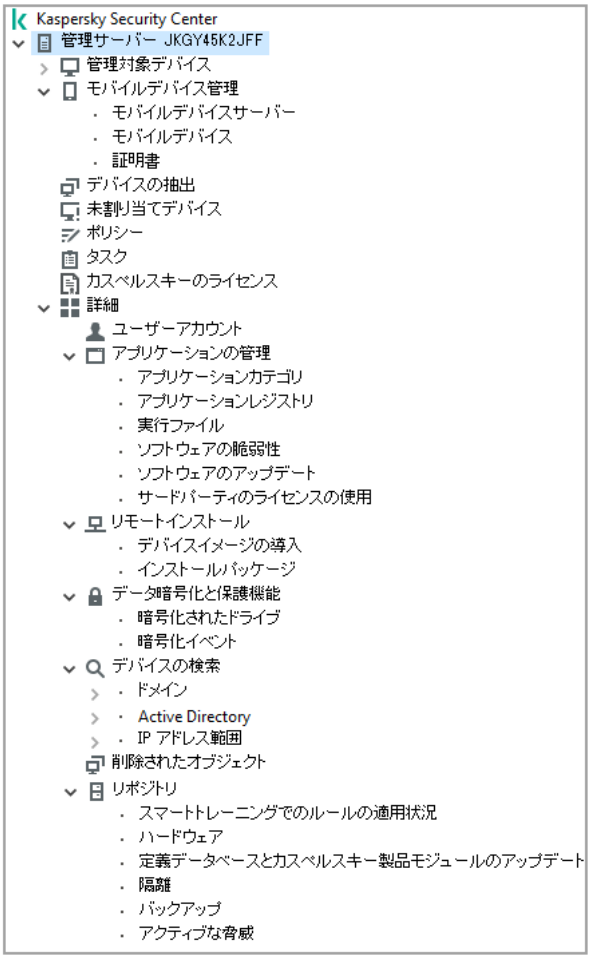
このオプションをオンにすると、アプリケーションカテゴリが変更された時、カテゴリのすべてのデータではなく変更されたデータのみがクライアントコンピューターに転送されます。このデータ転送オプションは、ネットワークエージェント Service Pack 2 以降のバージョンで使用します。

管理インターフェイスの機能

このセクションでは、Kaspersky Security Center のメインウィンドウで実行できる処理について説明します。

コンソールツリー

コンソールツリー（次の図を参照）には、企業ネットワーク上の管理サーバーの階層、その管理グループの構造、および製品のその他のオブジェクト（［**リポジトリ**］フォルダーや［**アプリケーションの管理**］フォルダーなど）が表示されます。Kaspersky Security Center のネームスペースには、階層内のインストール済み管理サーバーに対応するサーバー名など、複数のフォルダーを含めることができます。



コンソールツリー

［管理サーバー］フォルダー

［**管理サーバー – <デバイス名>**］フォルダーは、特定の管理サーバーの構造を示すフォルダーです。

［**管理サーバー**］フォルダーの作業領域には、管理サーバーによって管理されているアプリケーションとデバイスの現在のステータスに関する情報の要約が含まれます。作業領域に関する情報は、複数のタブにわたって表示されます。

- **監視**：アプリケーションの操作や、クライアントデバイスの現在のステータスに関する情報がリアルタイムモードで表示されます。脆弱性に関するメッセージ、検知されたウイルスなど管理者にとって重要な情報は特定の色で強調表示されます。［**監視**］タブのリンクを利用して、管理者の標準的なタスク（セキュリティ製品をクライアントデバイスにインストールし設定するなど）を実行し、コンソールツリーの他のフォルダーに移動できます。

- **統計**：トピック（保護のステータス、アンチウイルスの統計、アップデートなど）ごとにグループ化された図表を表示します。これらの図表はアプリケーションの操作やクライアントデバイスのステータスに関する情報を視覚的に表示します。

- **レポート**：アプリケーションが生成したレポート用のテンプレートが含まれます。このタブでは、カスタムテンプレートレポートを作成したり、定義済みのテンプレートを利用してレポートを作成したりできます。

- ［**イベント**］ウィンドウ：アプリケーションの操作中に登録されたイベントの記録が含まれます。これらの記録は、閲覧やフィルタリングがしやすいように、トピックごとにまとめられます。このタブでは、自動で生成されたイベントやカスタマイズされたイベントを表示することができます。

管理サーバーノード上のフォルダー

［**管理サーバー – <デバイス名>**］フォルダーには、次のフォルダーが含まれます：

- **管理対象デバイス**：このフォルダーでは、管理グループ、グループポリシー、グループタスクの構造を格納、表示、設定、変更することが可能です。

- **モバイルデバイス管理**：このフォルダーは、モバイルデバイスの管理を目的としています。［**モバイルデバイス管理**］フォルダーには、次のサブフォルダーがあります：

  - **モバイルデバイスサーバー**：iOS MDM サーバーの管理を目的としています。

  - **モバイルデバイス**：モバイルデバイス、KES、iOS MDM を管理を目的としています。

  - **証明書**：モバイルデバイスの証明書の管理を目的としています。

- **デバイスの抽出**：これは、すべての管理対象デバイス内で、特定の基準に合致するデバイス（デバイスの抽出）をすぐに選択するためのフォルダーです。たとえば、セキュリティ製品がインストールされていないデバイスをすぐに選択し、リストを表示して対象デバイスに移動することができます。これらの選択されたデバイスで、タスクを割り当てるなどの特定の操作を実行できます。定義済みの基準を利用することも、自分で定義して抽出することも可能です。

- **未割り当てデバイス**：このフォルダーには、管理グループに属していないデバイスのリストが含まれます。未割り当てデバイスに対して、管理グループへ移動したり、アプリケーションをインストールしたりなどの操作を実行できます。

- **ポリシー**：このフォルダーは、ポリシーを表示したり作成したりするためのフォルダーです。

- **タスク**：このフォルダーは、タスクを表示したり作成したりするためのフォルダーです。

- **カスペルスキーのライセンス**：カスペルスキー製品に適用可能なライセンスのリストが含まれます。このフォルダーの作業領域で、リポジトリに新しいライセンスを追加したり、管理対象デバイスにライセンスを導入したり、ライセンスの使用状況に関するレポートを表示したりできます。

- **詳細**：アプリケーションの様々な機能のグループに対応するサブフォルダーが含まれます。

詳細フォルダー：コンソールツリー内のフォルダーの移動

［**詳細**］フォルダーには、次のサブフォルダーがあります：

- **ユーザーアカウント**：ネットワークユーザーアカウントのリストが含まれています。

- **アプリケーションの管理**：ネットワーク上のデバイスにインストールされたアプリケーションの管理を目的としています。［**アプリケーションの管理**］フォルダーには、次のサブフォルダーがあります：

  - **アプリケーションカテゴリ**：カスタムアプリケーションのカテゴリの管理を目的としています。

  - **アプリケーションレジストリ**：ネットワークエージェントがインストールされたデバイスにインストールされているアプリケーションのリストが含まれます。

- **実行ファイル**：ネットワークエージェントがインストールされたクライアントデバイスに保存されている実行ファイルのリストが含まれます。

- **ソフトウェアの脆弱性**：ネットワークエージェントがインストールされたデバイスにインストールされているアプリケーション内の脆弱性のリストが含まれます。

- **ソフトウェアのアップデート**：管理サーバーが受信し、デバイスに配信可能なアプリケーションのアップデートのリストが含まれます。

- **サードパーティのライセンスの使用**：ライセンス認証済みアプリケーションのグループのリストが含まれます。ライセンス認証済みアプリケーションのグループのリストを使用して、サードパーティのソフトウェア（カスペルスキー以外の製品）の使用状況や、起きうるライセンスの違反を監視できます。

- **リモートインストール**：このフォルダーは、オペレーティングシステムとアプリケーションのリモートインストールの管理を目的としています。［**リモートインストール**］フォルダーには、次のサブフォルダーがあります：

  - **デバイスイメージの導入**：デバイスに対するオペレーティングシステムのイメージの導入を目的としています。

  - **インストールパッケージ**：インストールパッケージのリストが含まれます。このリストを使用して、アプリケーションをデバイスにリモートインストールできます。

- **データ暗号化と保護機能**：このフォルダーは、ハードドライブとリムーバブルドライブのデータ暗号化プロセスの管理を目的としています。

- **ネットワークポーリング**：このフォルダーは、管理サーバーがインストールされているネットワークを表示します。管理サーバーは、ネットワークの構造およびデバイスに関する情報を、企業のネットワーク上に存在する Windows ネットワーク、IP サブネットワーク、および Active Directory® に対する定期的なポーリングによって取得します。ポーリング結果は、対応するフォルダー（［**ドメイン**］、［**IP アドレス範囲**］、［**Active Directory**］）の作業領域に表示されます。

- **リポジトリ**：デバイスのステータス監視に使用するオブジェクトの操作、およびそのメンテナンスに使用されます。［**リポジトリ**］フォルダーには、次のサブフォルダーがあります：

  - **アダプティブアノマリー検知**：クライアントデバイス上のスマートトレーニングモードで動作する Kaspersky Endpoint Security ルールによって実行された異常検知のリストが含まれます。

  - **カスペルスキー製品のアップデートとパッチ**：管理サーバーが受信し、デバイスに配信可能なアップデートのリストが含まれます。

  - **ハードウェア**：組織のネットワークに接続されたハードウェアのリストが含まれます。

  - **隔離**：デバイス上のアンチウイルス製品によって隔離に移動されたオブジェクトのリストが含まれます。

  - **バックアップ**：デバイス上での駆除によって削除または変更されたファイルのバックアップコピーのリストが含まれます。

  - **未処理ファイル**：アンチウイルス製品によって後でスキャンするように指定されたファイルのリストが含まれます。

［**詳細**］フォルダー内のサブフォルダーを変更することができます。頻繁に使用されるサブフォルダーは、［**詳細**］フォルダーから1レベル上に移動することができます。あまり使用しないフォルダーを［**詳細**］内に移動できます。

*［**詳細**］フォルダーからサブフォルダーを移動するには：*

1. コンソールツリーで、［**詳細**］フォルダーから移動したいサブフォルダーを選択します。
2. サブフォルダーのコンテキストメニューで、［**表示**］→［**詳細フォルダーから移動する**］の順に選択します。

［**詳細**］フォルダーの作業領域内でも、セクション内の［**詳細フォルダーから移動する**］をクリックすることで［**詳細**］フォルダーからサブフォルダーを移動することができます。

*［**詳細**］フォルダーにサブフォルダーを移動するには：*

1. コンソールツリーで、［**詳細**］フォルダーに移動したいサブフォルダーを選択します。
2. サブフォルダーのコンテキストメニューで、［**表示**］→［**詳細フォルダーに移動する**］の順に選択します。

作業領域でデータを更新する方法

Kaspersky Security Center では、作業領域データ（デバイスのステータス、統計、レポートなど）が自動的に更新されることはありません。

作業領域のデータを更新するには：

- **F5** キーを押します。
- コンソールツリーのオブジェクトのコンテキストメニューで、［**更新**］を選択します。
- 作業領域で（）をクリックします。

コンソールツリーの操作方法

次のツールバーボタンを使用して、コンソールツリーを操作できます。

- –1つ前のステップへ。
- –1つ先のステップへ。
- –1つ上のレベルへ。

また、作業領域の右上端にあるナビゲーションチェーンも使用できます。ナビゲーションチェーンには、現在のコンソールツリーのフォルダーへの完全パスが含まれます。最後の要素を除き、チェーンのすべての要素がコンソールツリーのオブジェクトへのリンクとなっています。

作業領域でオブジェクトのプロパティを開く方法

オブジェクトのプロパティウィンドウでは、ほとんどの管理コンソールオブジェクトのプロパティを変更できます。

作業領域にあるオブジェクトのプロパティウィンドウを開くには：

- オブジェクトのコンテキストメニューから［**プロパティ**］を選択します。
- オブジェクトを選択して、**ALT+ENTER** キーを押します。

作業領域でオブジェクトのグループを選択する方法

作業領域ではオブジェクトのグループを選択できます。オブジェクトのグループを選択することで、たとえば、デバイスのグループに対してタスクを作成できます。

オブジェクトの範囲を選択するには：

1. 範囲の最初のオブジェクトを選択して、**SHIFT** キーを押します。
2. **SHIFT** キーを押したまま、範囲の最後のオブジェクトを選択します。

   範囲が選択されます。

個別のオブジェクトをグループ化するには：

1. グループの最初のオブジェクトを選択して、**CTRL** キーを押します。
2. **CTRL** キーを押したまま、グループに含める他のオブジェクトを選択します。

   オブジェクトがグループ化されます。

作業領域で列の組み合わせを変更する方法

管理コンソールでは、作業領域に表示される列の組み合わせを変更できます。

作業領域の表示列の組み合わせを変更するには：

1. コンソールツリーで、列の組み合わせを変更するオブジェクトをクリックします。
2. フォルダーの作業領域内の［**列の追加と削除**］をクリックして、列の組み合わせを設定するためのウィンドウを開きます。
3. ［**列の追加と削除**］ウィンドウで、表示する列の組み合わせを指定します。

参照情報

このセクションの表では、管理コンソールオブジェクトのコンテキストメニュー、コンソールツリーオブジェクトのステータス、作業領域オブジェクトのステータスに関するサマリー情報を提供します。

コンテキストメニューコマンド

このセクションでは、管理コンソールオブジェクトと対応するコンテキストメニュー項目をリストします（次の表を参照）。

管理コンソールオブジェクトのコンテキストメニュー項目

オブジェクト	メニュー項目	メニュー項目の目的
コンテキストメニューの全般項目	**検索**	デバイスの検索ウィンドウを開きます。
	更新	選択したオブジェクトの表示をアップデートします。
	リストのエクスポート	現在のリストをファイルにエクスポートします
	プロパティ	選択したオブジェクトのプロパティウィンドウを開きます。
	表示 → 列の追加と削除	作業領域にあるオブジェクトの表の列を追加または削除します。
	表示 → 大きいアイコン	作業領域のオブジェクトを大きいアイコンとして表示します。
	表示 → 小さいアイコン	作業領域のオブジェクトを小さいアイコンとして表示します。
	表示 → リスト	作業領域のオブジェクトをリストにして表示します。
	表示 → 表	作業領域のオブジェクトを表にして表示します。
	表示 → 設定	管理コンソール項目の表示を設定します。
Kaspersky Security Center	**新規 → 管理サーバー**	管理サーバーをコンソールツリーに追加します。
<管理サーバー名>	**管理サーバーに接続**	管理サーバーへ接続します。
	管理サーバーから切断	管理サーバーから切断します。
管理対象デバイス	**アプリケーションのインストール**	リモートインストールウィザードが起動します。
	表示 → インターフェイスの設定	インターフェイス要素の表示を設定します。
	削除	コンソールツリーから管理サーバーを削除します。
	アプリケーションのインストール	管理グループのリモートインストールウィザードを開始します。
	ウイルスカウンターのリセット	管理グループに含まれるデバイスのウイルスカウンターをリセットします。
	脅威レポートの表示	管理グループに属するデバイス上の脅威とウイルスアクティビティのレポートを作成します。
	新規 → グループ	管理グループを作成します。
	すべてのタスク → グループ構造の新規作成	ドメインまたは Active Directory の構造に基づいて、管理グループの構造を作成します。
	すべてのタスク → メッセージ表示	管理グループに含まれるデバイスのユーザーを対象とした、ユーザー宛メッセージ作成ウィザードを開始します。
管理対象デバイス → 管理サーバー	**新規 → セカンダリ管理サーバー**	セカンダリ管理サーバーの追加ウィザードを開始します。
	新規 → 仮想管理サーバー	新規仮想管理サーバーウィザードを開始します。
モバイルデバイス管理 → モバイルデバイス	**新規 → モバイルデバイス**	ユーザーの新規モバイルデバイスに接続します。
モバイルデバイス管理 → 証明書	**新規 → 証明書**	証明書を作成します。
	作成 → モバイルデバイス	ユーザーの新規モバイルデバイスに接続します。
デバイスの抽出	**新規 → 新規の抽出**	デバイスの抽出を作成します。
	すべてのタスク → インポート	抽出内容をファイルからインポートします。
カスペルスキーのライセンス	**アクティベーションコードまたはライセンス情報ファイルの追加**	ライセンスを管理サーバーリポジトリに追加します。
	アプリケーションのアクティ	アプリケーションのアクティベーションタスク作成ウィザ

	ベーション	ードを開始します。
	ライセンス使用レポート	クライアントデバイスのライセンスに関するレポートを作成して表示します。
アプリケーションの管理 → アプリケーションカテゴリ	**新規 → カテゴリ**	アプリケーションカテゴリを作成します。
アプリケーションの管理 → アプリケーションレジストリ	**フィルター**	アプリケーションリストのフィルターを設定します。
	監視対象アプリケーション	アプリケーションのインストールに関するイベントの発行を設定します。
	インストールされていないアプリケーションを削除する	ネットワーク上のデバイスからアンインストールされたアプリケーションに関する情報をクリアします。
アプリケーションの管理 → ソフトウェアのアップデート	**アップデートの使用許諾契約書に同意する**	ソフトウェアアップデートの使用許諾契約書に同意します。
アプリケーションの管理 → サードパーティのライセンスの使用	**新規 → ライセンス認証済みアプリケーショングループ**	ライセンス認証済みアプリケーショングループを作成します。
リモートインストール → インストールパッケージ	**現在入手可能な製品バージョンを表示**	Web サーバーで使用可能な最新バージョンのカスペルスキー製品のリストを表示します。
	新規 → インストールパッケージ	インストールパッケージを作成します。
	すべてのタスク → 定義データベースのアップデート	インストールパッケージ内の定義データベースをアップデートします。
	すべてのタスク → スタンドアロンパッケージのリストを表示	インストールパッケージに対して作成されたスタンドアロンパッケージのリストを表示します。
デバイスの検索 → ドメイン	**すべてのタスク → デバイスのアクティビティ**	ネットワーク上のデバイスが非アクティブの場合に、管理サーバーが対応する方法を設定します。
デバイスの検索 → IP アドレス範囲	**新規 → IP アドレス範囲**	IP アドレス範囲を作成します。
リポジトリ → 定義データベースとカスペルスキー製品モジュールのアップデート	**アップデートのダウンロード**	管理サーバーのリポジトリへのアップデートのダウンロードタスクのプロパティウィンドウを開きます。
	アップデートのダウンロードの設定	管理サーバーのリポジトリへのアップデートのダウンロードタスクを設定します。
	定義データベース使用レポート	定義データベースのバージョンに関するレポートを作成して表示します。
	すべてのタスク → アップデートリポジトリのクリア	管理サーバーのアップデートリポジトリをクリアします。
リポジトリ → ハードウェア	**新規 → デバイス**	デバイスを新規作成します。

管理対象デバイスのリスト：列の説明

次の表は、管理対象デバイスのリストの列について、名前とそれぞれの説明を示しています。

管理対象デバイスのリストの列の説明

列名	値
名前	クライアントデバイスの NetBIOS 名。デバイス名のアイコンに関する説明は、補足情報にあります。
OS の種別	クライアントデバイスにインストールされているオペレーティングシステムの種別
Windows ドメイン	クライアントデバイスが配置されている Windows ドメインの名前
ネットワークエージェントがインストール済み	クライアントデバイスでのネットワークエージェントインストールの結果（［*はい*］、［*いいえ*］、［*不明*］）

ネットワークエージェントが実行中	ネットワークエージェントの操作の結果（［*はい*］、［*いいえ*］、［*不明*］）
リアルタイム保護	セキュリティ製品がインストールされています（［*はい*］、［*いいえ*］、［*不明*］）
前回の管理サーバーへの接続	クライアントデバイスが管理サーバーに接続されてから経過した期間
前回の定義データベースのアップデート	管理対象デバイスの最終更新時刻から経過した時間範囲
ステータス	クライアントデバイスの現在のステータス（*OK*、*緊急*、*警告*）
ステータスの説明	クライアントデバイスのステータスを［*緊急*］または［*警告*］変更した理由 デバイスのステータスは、次の理由により［*警告*］または［*緊急*］に変更されます： • セキュリティ製品がインストールされていません • ウイルスが多数検知されました • リアルタイム保護レベルが管理者の設定と異なります • マルウェアスキャンが長期間実行されていません。 • 定義データベースがアップデートされていません • 長期間接続されていません • アクティブな脅威を検知しました • 再起動が必要です • 競合アプリケーションがインストールされています • ソフトウェアの脆弱性が検知されました • Windows Update 更新プログラムのチェックが長期間実行されていません • 暗号化ステータスが無効です • モバイルデバイスの設定がポリシーに適合していません • 未処理のセキュリティ問題が検出されました • 製品が定義したデバイスのステータス • デバイスに空き容量がありません • ライセンスの有効期間がまもなく終了します デバイスのステータスは、次の理由により［*緊急*］に変更されます： • ライセンスの有効期間が終了しました • デバイスが管理対象外になりました • プロテクションが無効です • セキュリティ製品が実行されていません クライアントデバイス上の管理対象のカスペルスキー製品が、リストにステータスの説明を追加することがあります。Kaspersky Security Center は、クライアントデバイスにインストールされた管理対象カスペルスキー製品からクライアントデバイスのステータスの説明を受け取ることができます。管理対象製品によってデバイスに割り当てられたステータスが Kaspersky Security Center によって割り当てられたものと異なる場合、管理コンソールは、そのデバイスのセキュリティにとって最も重要度が高いステータスを表示します。たとえば、管理対象製品がデバイスに［*緊急*］ステータスを割り当て、Kaspersky Security Center が［*警告*］ステータスを割り当てた場合、管理コンソールはそのデバイスを［*緊急*］ステータスにし、管理対象製品から提供された詳細を表示します。

情報更新	クライアントデバイスと管理サーバーが前回正常に同期（最後にネットワークスキャン）されてから経過した期間。
DNS 名	クライアントデバイスの DNS ドメイン名
DNS ドメイン	メインの DNS サフィックス
IP アドレス	クライアントデバイスの IP アドレス。IPv4 アドレスを使用してください。
前回の可視	クライアントデバイスがネットワークで可視状態だった期間
前回の完全スキャン	ユーザーの要求に基づきセキュリティ製品が実行したクライアントデバイスの前回のスキャンの日時
検知した脅威の数	検知された脅威の数。
リアルタイム保護のステータス	リアルタイム保護ステータス（*開始中*、*実行中*、*実行中（最大レベル）*、*実行中（速度重視）*、*実行中（推奨レベル）*、*実行中（カスタマイズされた設定）*、*停止*、*一時停止*、*失敗*）
接続 IP アドレス	Kaspersky Security Center 管理サーバーへの接続に使用される IP アドレス
ネットワークエージェントのバージョン	ネットワークエージェントのバージョン
アプリケーションのバージョン	クライアントデバイスにインストールされているセキュリティ製品のバージョン
定義データベースの公開日	定義データベースのバージョン
システムの前回の起動	前回クライアントデバイスの電源を入れた日時
再起動が必要です	クライアントデバイスの再起動が必要
ディストリビューションポイント	このクライアントデバイスに対するディストリビューションポイントとして動作するデバイスの名前
説明	ネットワークスキャンにより取得したクライアントデバイスの説明
暗号化ステータス	クライアントデバイスのデータ暗号化ステータス
Windows Update エージェントのステータス	クライアントデバイスの Windows Update エージェントのステータス ［*はい*］の場合は、クライアントデバイスが管理サーバーから Windows Update を使用して更新プログラムを取得していることを示します。 ［*いいえ*］の場合は、クライアントデバイスが他のソースから Windows Update を使用して更新プログラムを取得していることを示します。
OS のビット数	クライアントデバイスにインストールされているオペレーティングシステムのビットサイズ
スパムからの保護ステータス	スパム保護ステータス（*実行中*、*開始中*、*停止*、*一時停止*、*失敗*、*不明*）
データ漏洩対策のステータス	データ漏洩対策のステータス（*実行中*、*開始中*、*停止*、*一時停止*、*失敗*、*不明*）
コラボレ	コンテンツフィルタリングのステータス（*実行中*、*開始中*、*停止*、*一時停止*、*失敗*、*不明*）

ーションサーバーの保護ステータス	
メールサーバーの保護ステータス	メールサーバーの保護のステータス（*実行中*、*開始中*、*停止*、*一時停止*、*失敗*、*不明*）
Endpoint Sensor ステータス	Endpoint Detection and Response コンポーネントの状況（KATA）（*実行中*、*開始中*、*停止*、*一時停止*、*失敗*、*不明*）
作成日	<デバイス名> アイコンが作成された日時この属性は、様々なイベントを相互に比較するために使用されます。
仮想管理サーバーまたはセカンダリ管理サーバーの名前	仮想管理サーバーまたはセカンダリ管理サーバーの名前：この列は、異なる管理サーバーのデバイスが含まれるリストでのみ使用できます。
親グループ	<デバイス名> アイコンが表示される管理グループの名前。この列は、異なる管理サーバーのデバイスが含まれるリストでのみ使用できます。
別の管理サーバーの管理対象	このパラメータは、次のいずれかの値を取ることができます： • True：デバイスへのセキュリティ製品のリモートインストール中に、そのデバイスが別の管理サーバーによって管理されていることが判明した場合。 • False：それ以外の場合。
OS のビルド	オペレーティングシステムのビルド番号です。選択したオペレーティングシステムのビルド番号が、入力したビルド番号と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したビルド番号を除くすべてのビルド番号を検索するようにも設定できます。
OS のリリース ID	オペレーティングシステムのリリース ID です。選択したオペレーティングシステムのリリース ID が、入力したリリース ID と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したリリース ID を除くすべてのリリース ID を検索するようにも設定できます。

デバイス、タスク、ポリシーのステータス

次の表は、コンソールツリー、管理コンソール作業領域、デバイス名の横、タスク名の横、ポリシー名の横に表示されるアイコンのリストです。これらのアイコンはオブジェクトのステータスを示します。

デバイス、タスク、ポリシーのステータス

アイコン	ステータス
	システムで検出されたがいずれの管理グループにも含まれていない、ワークステーションのオペレーティングシステムを使用しているデバイス。
	管理グループに含まれており、ステータスが「*OK*」である、ワークステーションのオペレーティングシステムを使用しているデバイス。
	管理グループに含まれており、ステータスが「*警告*」である、ワークステーションのオペレーティングシステムを使用しているデバイス。
	管理グループに含まれており、ステータスが「*緊急*」である、ワークステーションのオペレーティングシステムを使用しているデバイス。

	管理グループに含まれているが管理サーバーとの接続が失われた、ワークステーションのオペレーティングシステムを使用しているデバイス。
	システムで検出されたがいずれの管理グループにも含まれていない、サーバーのオペレーティングシステムを使用しているデバイス。
	管理グループに含まれており、ステータスが「*OK*」である、サーバーのオペレーティングシステムを使用しているデバイス。
	管理グループに含まれており、ステータスが「*警告*」である、サーバーのオペレーティングシステムを使用しているデバイス。
	管理グループに含まれており、ステータスが「*緊急*」である、サーバーのオペレーティングシステムを使用しているデバイス。
	管理グループに含まれているが管理サーバーとの接続が失われた、サーバーのオペレーティングシステムを使用しているデバイス。
	ネットワークで検出された、どの管理グループにも含まれていないモバイルデバイス。
	管理グループに含まれており、ステータスが「*OK*」であるモバイルデバイス。
	管理グループに含まれており、ステータスが「*警告*」であるモバイルデバイス。
	管理グループに含まれており、ステータスが「*緊急*」であるモバイルデバイス。
	管理グループに含まれているが、管理サーバーとの接続が失われたモバイルデバイス。
	ネットワークで検出されたが、いずれの管理グループにも含まれていない UEFI 保護デバイス。UEFI 保護デバイスはネットワーク上に存在します。
	ネットワークで検出されたが、いずれの管理グループにも含まれていない UEFI 保護デバイス。UEFI 保護デバイスはネットワーク上に存在しません。
	管理グループに含まれており、ステータスが「*OK*」である UEFI 保護デバイス。UEFI 保護デバイスはネットワーク上に存在します。
	管理グループに含まれており、ステータスが「*OK*」である UEFI 保護デバイス。UEFI 保護デバイスはネットワーク上に存在しません。
	管理グループに含まれており、ステータスが「*警告*」である UEFI 保護デバイス。UEFI 保護デバイスはネットワーク上に存在します。
	管理グループに含まれており、ステータスが「*警告*」である UEFI 保護デバイス。UEFI 保護デバイスはネットワーク上に存在しません。
	管理グループに含まれており、ステータスが「*緊急*」である UEFI 保護デバイス。UEFI 保護デバイスはネットワーク上に存在します。
	管理グループに含まれており、ステータスが「*緊急*」である UEFI 保護デバイス。UEFI 保護デバイスはネットワーク上に存在しません。
	アクティブポリシー。
	非アクティブポリシー。
	プライマリ管理サーバー上で作成されたグループから継承されたアクティブポリシー。
	トップレベルのグループから継承されたアクティブポリシー。
	ステータスが「*スケジュール済み*」または「*正常終了*」のタスク（グループタスク、管理サーバータスク、特定のデバイスに対するタスク）。
	ステータスが「*実行中*」のタスク（グループタスク、管理サーバータスク、特定のデバイスに対するタスク）。
	ステータスが「*失敗*」のタスク（グループタスク、管理サーバータスク、特定のデバイスに対するタスク）。
	プライマリ管理サーバー上で作成されたグループから継承されたタスク。
	トップレベルのグループから継承されたタスク。

管理コンソールのファイルステータスアイコン

Kaspersky Security Center 管理コンソールでは、ファイル管理を容易にするため、ファイル名の横にアイコンが表示されます（次の表を参照）。アイコンは、クライアントデバイス上の管理対象カスペルスキー製品によってファイルに割り当てられたステータスを示します。アイコンは、［**隔離**］フォルダー、［**バックアップ**］フォルダー、［**アクティブな脅威**］フォルダーの作業領域で表示されます。

クライアントデバイスにインストールされている Kaspersky Endpoint Security によってステータスがオブジェクトに割り当てられます。

アイコンとファイルステータスの対応

アイコン	ステータス
	「*感染*」ステータスのファイル。
	「*警告*」または「*感染の可能性あり*」ステータスのファイル。
	「*ユーザーによる追加*」ステータスのファイル。
	「*誤検知*」ステータスのファイル。
	「*駆除済み*」ステータスのファイル。
	「*削除済み*」ステータスのファイル。
	［**隔離**］フォルダーの、［*感染なし*］、［*パスワードによる保護*］、［*カスペルスキーに送信する必要があります*］ステータスのファイル。アイコンの横にステータスの説明がない場合、クライアントデバイス上の管理対象カスペルスキー製品が、Kaspersky Security Center にとって未知のステータスを報告しています。
	［**バックアップ**］フォルダーの、［*感染なし*］、［*パスワードによる保護*］、［*カスペルスキーに送信する必要があります*］ステータスのファイル。アイコンの横にステータスの説明がない場合、クライアントデバイス上の管理対象カスペルスキー製品が、Kaspersky Security Center にとって未知のステータスを報告しています。
	［**アクティブな脅威**］フォルダーの、［*感染なし*］、［*パスワードによる保護*］、［*カスペルスキーに送信する必要があります*］ステータスのファイル。アイコンの横にステータスの説明がない場合、クライアントデバイス上の管理対象カスペルスキー製品が、Kaspersky Security Center にとって未知のステータスを報告しています。

データの検索とエクスポート

このセクションでは、データの検索方法とデータのエクスポートについて説明します。

既存のデバイスの検索

Kaspersky Security Center では、条件を指定してデバイスを検索できます。検索結果はテキストファイルに保存できます。

検索機能により、次のデバイスを見つけることができます：

- 管理サーバーとセカンダリ管理サーバーの管理グループに属するクライアントデバイス
- 管理サーバーとセカンダリ管理サーバーで管理される未割り当てデバイス

管理グループに属するクライアントデバイスを検索するには：

1. コンソールツリーで、管理グループフォルダーを選択します。
2. 管理グループフォルダーのコンテキストメニューから［**検索**］を選択します。
3. ［**検索**］ウィンドウの各タブでデバイスの検索基準を指定し、［**今すぐ検索**］をクリックします。

   指定した検索基準を満たすデバイスが［**検索**］ウィンドウの下部に表示されます。

未割り当てデバイスを検索するには：

1. コンソールツリーで、［**未割り当てデバイス**］フォルダーを選択します。
2. ［**未割り当てデバイス**］フォルダーのコンテキストメニューから［**検索**］を選択します。
3. ［**検索**］ウィンドウの各タブでデバイスの検索基準を指定し、［**今すぐ検索**］をクリックします。

   指定した検索基準を満たすデバイスが［**検索**］ウィンドウの下部に表示されます。

管理グループに属するかどうかに関係なくデバイスを検索するには：

1. コンソールツリーで、［**管理サーバー %s** ］フォルダーを選択します。
2. フォルダーのコンテキストメニューで、［**検索**］を選択します。
3. ［**検索**］ウィンドウの各タブでデバイスの検索基準を指定し、［**今すぐ検索**］をクリックします。

   指定した検索基準を満たすデバイスが［**検索**］ウィンドウの下部に表示されます。

［**検索**］ウィンドウでは、ウィンドウ右上隅のドロップダウンリストを使用して管理グループとセカンダリ管理サーバーも検索できます。［**検索**］ウィンドウを［**未割り当てデバイス**］フォルダーから開いた場合、管理グループとセカンダリ管理サーバーの検索機能を使用することはできません。

デバイスの検索に、［**検索**］ウィンドウのフィールドで正規表現を使用できます。

［**検索**］ウィンドウでは、以下で全文テキスト検索が可能です：

- ［**ネットワーク**］タブの［**説明**］
- ［**ハードウェア**］タブの［**デバイス**］、［**製造元**］、［**説明**］

デバイス検索の設定

管理対象デバイスの検索に使用する設定について説明します。検索結果はウィンドウの下部に表示されます。

ネットワーク

［**ネットワーク**］タブでは、ネットワークデータに従ってデバイスを検索するために使用する基準を指定できます：

- **デバイス名または IP アドレス**

  デバイスの Windows ネットワーク名（NetBIOS 名）、あるいは IPv4 アドレスまたは IPv6 アドレス。

- **Windows ドメイン**

  指定した Windows ドメインに含まれるデバイスをすべて表示します。

- **管理グループ**

  指定した管理グループに含まれるデバイスを表示します。

- **説明**

デバイスのプロパティウィンドウ（［**全般**］セクションの［**説明**］）のテキスト。
［**説明**］で検索に使用する表現として、次の文字を使用できます：

- 1つの単語：
  - ***** -文字数不定の任意の文字列を表します。

    例：

    Server または **Server's** などの単語を記述するには、**Server*** と入力します。
  - **?** -任意の1文字を表します。

    例：

    Window または **Windows** などの単語を記述するには、**Windo?** と入力します。
    アスタリスク（*****）または疑問符（**?**）は、クエリの先頭文字としては使用できません。
- 複数の単語による検索：
  - スペース -指定した単語のいずれかがコメントに含まれているデバイスがすべて表示されます。

    例：

    Secondary または **Virtual** という単語が含まれている語句を検索する場合は、クエリに **Secondary Virtual** と入力します。
  - **+** -単語の前にプラス記号を付けると、すべての検索結果にその単語が含まれます。

    例：

    Secondary と **Virtual** の両方が含まれた語句を検索するには、クエリに **+Secondary+Virtual** と入力します。
  - **-** -単語の前にマイナス記号を付けると、すべての検索結果にその単語が含まれません。

    例：

    Secondary が含まれ、**Virtual** が含まれない語句を検索するには、クエリに **+Secondary-Virtual** と入力します。
  - **"<任意のテキスト>"** -引用符で囲まれたテキストを含むテキストが検索されます。

    例：

    Secondary Server という語句を検索する場合は、クエリに **"Secondary Server"** と入力します。

- **IP アドレス範囲**

  このオプションをオンにすると、検索されるデバイスが属する IP アドレス範囲の最初と最後の IP アドレスを入力できます。
  既定では、このオプションはオフです。

- **別の管理サーバーの管理対象**

次のいずれかの値を選択します：

- **はい**別の管理サーバーで管理されているクライアントデバイスのみが対象になります。
- ［**いいえ**］。同じ管理サーバーで管理されているクライアントデバイスのみが対象になります。
- **値を選択しない**：基準は適用されません。

タグ

［**タグ**］タブでは、管理対象デバイスの説明に追加済みのキーワード（タグ）を基にデバイスの検索を設定できます：

- **少なくとも 1 個のタグが一致する場合に適用する**

  このオプションをオンにすると、選択されたタグを 1 つ以上説明に含むデバイスが検索結果に表示されます。

  このオプションをオフにすると、選択されたすべてのタグを説明に含むデバイスのみが検索結果に表示されます。

  既定では、このオプションはオフです。

- **タグを含む**

  このオプションをオンにすると、検索結果には、選択したタグが説明内に含まれるデバイスが表示されます。デバイスを検索するため、文字数不定の任意の文字列を表すアスタリスクを使用できます。

  既定では、このオプションがオンです。

- **タグを含まない**

  このオプションをオンにすると、検索結果には、選択したタグが説明内に含まれないデバイスが表示されます。デバイスを検索するため、文字数不定の任意の文字列を表すアスタリスクを使用できます。

Active Directory

［**Active Directory**］タブで、Active Directory 組織単位（OU）またはグループで検索されるデバイスを指定できます。指定した Active Directory OU のすべての子 OU のデバイスを抽出に含めることもできます。デバイスを抽出するには、次の設定を定義します：

- **デバイスが配置されている Active Directory 組織単位**

  このオプションをオンにすると、抽出には、入力フィールドで指定した Active Directory 組織単位のデバイスが含まれます。

  既定では、このオプションはオフです。

- **子組織単位を含める**

このオプションをオンにすると、抽出には、指定したドメイン組織単位のすべての子組織単位（OU）のデバイスが含まれます。

既定では、このオプションはオフです。

- **デバイスが属している Active Directory グループ**

  このオプションを有効にすると、抽出には、入力フィールドで指定した Active Directory グループのデバイスが含まれます。

  既定では、このオプションはオフです。

ネットワーク活動

［**ネットワーク活動**］タブでは、ネットワークアクティビティを基にしたデバイスの検索に使用する基準を指定できます：

- **ディストリビューションポイント**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：
  - **はい**：ディストリビューションポイントとして動作するデバイスが抽出に含まれます。
  - ［**いいえ**］。ディストリビューションポイントとして機能するデバイスが抽出に含まれません。
  - **値を選択しない**：基準は適用されません。

- **管理サーバーから切断しない**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：
  - **有効**：［**管理サーバーから切断しない**］をオンにしたデバイスが抽出に含まれます。
  - **無効**：［**管理サーバーから切断しない**］をオフにしたデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

- **接続プロファイルの切り替え**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：
  - **はい**：接続プロファイルを切り替えた結果として管理サーバーに接続されたデバイスが抽出に含まれます。
  - ［**いいえ**］。接続プロファイルを切り替えた結果として管理サーバーに接続されたデバイスが抽出に含まれません。
  - **値を選択しない**：基準は適用されません。

- **前回の管理サーバーへの接続**

このチェックボックスを使用して、管理サーバーに前回接続した日時によるデバイスの検索の基準を設定できます。

このチェックボックスをオンにすると、入力フィールドで、クライアントデバイスにインストールされたネットワークエージェントと管理サーバーとの間に前回接続が確立された日時の範囲を指定できます。指定された間隔内のデバイスが抽出に含まれます。

このチェックボックスをオフにすると、この基準は適用されません。

既定では、このチェックボックスはオフです。

- **ネットワークポーリングで検出された新規デバイス**

過去数日間のネットワークポーリングで検出された新規デバイスを検索します。

このオプションをオンにすると、［**検出期間（日）**］フィールドで指定した期間中のデバイスの検索で検出された新規デバイスのみが、抽出に含まれます。

このオプションをオフにすると、デバイスの検索で検出された新規デバイスがすべて抽出に含まれます。

既定では、このオプションはオフです。

- **デバイスが可視**

検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：

- **はい**：ネットワークで現在可視のデバイスを抽出に含めます。
- ［**いいえ**］。ネットワークで現在不可視のデバイスを抽出に含めます。
- **値を選択しない**：基準は適用されません。

アプリケーション

［**アプリケーション**］タブでは、選択した管理対象アプリケーションに基づいたデバイスの検索に使用する基準を指定できます：

- **アプリケーション名**

カスペルスキー製品の名前で検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます。

リストには、管理コンピューターに管理プラグインがインストールされているアプリケーションの名前のみが表示されます。

アプリケーションが選択されていない場合、この基準は適用されません

- **アプリケーションのバージョン**

カスペルスキー製品のバージョン番号で検索を実行する場合、抽出に含めるデバイスの基準を、入力フィールドで設定できます。

バージョン番号が指定されていない場合、この基準は適用されません。

- **重要なアップデート名**

製品の名前またはアップデートパッケージ番号で検索する場合の、抽出に含めるデバイスの基準を、入力フィールドで設定できます。

このフィールドが空白の場合、この基準は適用されません。

- **前回のモジュールアップデート**

  このオプションを使用して、デバイスにインストールされているソフトウェアモジュールの前回のアップデート日時でデバイスを検索する基準を設定できます。

  このチェックボックスをオンにすると、入力フィールドで、デバイスにインストールされているアプリケーションモジュールの前回のアップデートが実行された日時の範囲を指定できます。

  このチェックボックスをオフにすると、この基準は適用されません。

  既定では、このチェックボックスはオフです。

- **デバイスを Kaspersky Security Center で管理する**

  ドロップダウンリストで、Kaspersky Security Center で管理されているデバイスを抽出に含めることができます：

  - **はい**Kaspersky Security Center で管理されているデバイスが抽出に含まれます。
  - ［**いいえ**］。Kaspersky Security Center により管理されていないデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

- **セキュリティ製品がインストールされている**

  ドロップダウンリストで、セキュリティ製品がインストールされているすべてのデバイスを抽出に含めることができます：

  - **はい**：セキュリティ製品がインストールされているすべてのデバイスが抽出に含まれます。
  - ［**いいえ**］。セキュリティ製品がインストールされていないすべてのデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

オペレーティングシステム

［**オペレーティングシステム**］タブでは、オペレーティングシステム（OS）の種別を基にデバイスを検索する基準を指定できます。

- **オペレーティングシステムのバージョン**

  このチェックボックスをオンにすると、オペレーティングシステムをリストから選択できます。指定したオペレーティングシステムがインストールされたデバイスが検索結果に含まれます。

- **OS のビット数**

ドロップダウンリストで、オペレーティングシステムのアーキテクチャを選択できます。これによって、デバイスに対する移動ルールの適用方法が決定されます（［**不明**］、［**x86**］、［**AMD64**］、［**IA64**］）。既定では、リストでオプションが選択されていないため、オペレーティングシステムのアーキテクチャは定義されていません。

- **OS サービスパックのバージョン**

  このフィールドでは、オペレーティングシステムのパッケージバージョンを「*X.Y*」形式で指定できます。これによって、デバイスに対する移動ルールの適用方法が決定されます。既定では、バージョンの値は指定されていません。

- **OS のビルド**

  この設定は Windows オペレーティングシステムにのみ適用できます。

  オペレーティングシステムのビルド番号です。選択したオペレーティングシステムのビルド番号が、入力したビルド番号と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したビルド番号を除くすべてのビルド番号を検索するようにも設定できます。

- **OS のリリース ID**

  この設定は Windows オペレーティングシステムにのみ適用できます。

  オペレーティングシステムのリリース ID です。選択したオペレーティングシステムのリリース ID が、入力したリリース ID と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したリリース ID を除くすべてのリリース ID を検索するようにも設定できます。

デバイスのステータス

［**デバイスのステータス**］タブでは、管理対象アプリケーションからのデバイスのステータスを基にデバイスを検索する基準を指定できます：

- **デバイスのステータス**

  ドロップダウンリストからデバイスのステータス（「*OK*」「*緊急*」「警告」）を選択します。

- **リアルタイム保護のステータス**

  リアルタイム保護のステータスを選択できるドロップダウンリスト。指定されたリアルタイム保護ステータスのデバイスが抽出に含まれます。

- **デバイスのステータスの説明**

このフィールドで、「*OK*」「*緊急*」「*警告*」のいずれかのステータスをデバイスに割り当てる条件に対応するチェックボックスをオンにできます。

- **製品が定義したデバイスのステータス**

  リアルタイム保護のステータスを選択できるドロップダウンリスト。指定されたリアルタイム保護ステータスのデバイスが抽出に含まれます。

保護コンポーネント

［**保護コンポーネント**］タブでは、プロテクションのステータスを基にクライアントデバイスを検索する基準を設定できます。

- **定義データベースの公開日時**

  このオプションをオンにすると、定義データベースの公開日時でクライアントデバイスを検索できます。入力フィールドで設定した期間に基づいて検索が実行されます。

  既定では、このオプションはオフです。

- **前回のスキャン**

  このオプションをオンにすると、前回マルウェアスキャンを実行した日時でクライアントデバイスを検索できます。入力フィールドで、前回マルウェアスキャンを実行した期間を指定できます。

  既定では、このオプションはオフです。

- **検知した脅威の数**

  このオプションをオンにすると、検知されたウイルスの数でクライアントデバイスを検索できます。入力フィールドで、ウイルス検知数の上下のしきい値を設定できます。

  既定では、このオプションはオフです。

アプリケーションレジストリ

［**アプリケーションレジストリ**］タブでは、インストール済みのアプリケーションに基づいたデバイスの検索を設定できます：

- **アプリケーション名**

  アプリケーションを選択できるドロップダウンリスト。指定したアプリケーションがインストールされているデバイスが抽出に含まれます。

- **アプリケーションのバージョン**

  選択したアプリケーションのバージョンを指定できる入力フィールド。

- **製造元**

デバイスにインストールされているアプリケーションの製造元を選択できるドロップダウンリスト。

- **アプリケーションのステータス**

  アプリケーションのステータス（*インストール済み*、*未インストール*）を選択できるドロップダウンリスト。指定のアプリケーションがインストール済みまたは未インストールのデバイスが、選択したステータスに応じて抽出に含まれます。

- **アップデートによって検索**

  このオプションをオンにすると、該当するデバイスにインストールされているアプリケーションのアップデートに関する情報を使用して検索が実行されます。このチェックボックスをオンにすると、［**アプリケーション名**］、［**アプリケーションのバージョン**］、［**アプリケーションのステータス**］というフィールドがそれぞれ、［**アップデート名**］、［**アップデートのバージョン**］、［**ステータス**］に変わります。

  既定では、このオプションはオフです。

- **競合するセキュリティ製品**

  サードパーティのセキュリティ製品を選択できるドロップダウンリスト。指定したアプリケーションがインストールされているデバイスが、検索時に抽出に含まれます。

- **アプリケーションタグ**

  このドロップダウンリストでは、アプリケーションタグを選択できます。選択したタグが説明にあるアプリケーションをインストール済みのすべてのデバイスが、デバイスの抽出に含まれます。

管理サーバーの階層

セカンダリ管理サーバーに保存されている情報をデバイスの検索時の検索対象に含めるには、［**管理サーバーの階層**］タブで［**セカンダリ管理サーバーのデータを含める（階層数）**］をオンにします。これにより、入力フィールドで、デバイスの検索時に対象とするセカンダリ管理サーバーの階層数を指定できるようになります。既定では、このチェックボックスはオフです。

仮想マシン

［**仮想マシン**］タブでは、仮想マシンであるか仮想デスクトップインフラストラクチャ（VDI）の一部であるかを基にしたデバイスの検索を設定できます：

- **仮想マシン**

  このドロップダウンリストで、次のオプションを選択できます：

  - **判断しない**。
  - ［**いいえ**］。仮想マシンでないデバイスを検索します。
  - **はい**：仮想マシンであるデバイスを検索します。

- **仮想マシンの種別**

  このドロップダウンリストで、仮想マシンの製造元を選択できます。

  このドロップダウンリストは、［**仮想マシン**］の値が［**はい**］または［**判断しない**］である場合に使用できます。

- **仮想デスクトップインフラストラクチャの一部**

  このドロップダウンリストで、次のオプションを選択できます：

  - **判断しない**。
  - ［**いいえ**］。仮想デスクトップインフラストラクチャの一部でないデバイスを検索します。
  - **はい**：仮想デスクトップインフラストラクチャ（VDI）の一部であるデバイスを検索します。

ハードウェア

［**ハードウェア**］タブでは、ハードウェアを基にしたクライアントデバイスの検索を設定できます：

- **デバイス**

  このドロップダウンリストでは、装置の種別を選択できます。その装置を備えたすべてのデバイスが検索結果に含まれます。

  このフィールドでは全文検索が可能です。

- **製造元**

  このドロップダウンリストで、装置の製造元の名前を選択できます。その装置を備えたすべてのデバイスが検索結果に含まれます。

  このフィールドでは全文検索が可能です。

- **説明**

  デバイスまたはハードウェア装置の説明。このフィールドで指定された説明が付けられたデバイスが抽出に含まれます。

  デバイスの説明は、そのデバイスのプロパティウィンドウにあらゆる形式で入力できます。このフィールドでは全文検索が可能です。

- **インベントリ番号**

  このフィールドで指定されたインベントリ番号が付けられた機器が抽出に含まれます。

- **CPU の周波数(MHz)**

  CPU の周波数範囲。これらのフィールドで指定された CPU の周波数範囲に適合するデバイスが抽出に含まれます。

- **仮想 CPU コア**

  仮想 CPU コア数の範囲。これらのフィールドで指定された CPU の範囲に適合するデバイスが抽出に含まれます。

- **ハードディスク容量（GB）**

  デバイスのハードディスクの容量の範囲。これらの入力フィールドで指定されたハードディスクの容量の範囲に適合するデバイスが抽出に含まれます。

- **RAM サイズ（MB）**

  デバイスの RAM サイズの値の範囲。この範囲の値（指定した値を含む）のサイズの RAM を実装するデバイスが抽出に含まれます。

脆弱性とアップデート

［**脆弱性とアップデート**］タブでは、Windows Update をどこから取得するかを基にデバイスを検索するための基準を設定できます：

- **Windows Update エージェントの管理サーバーへの切り替え**

  このドロップダウンリストから、次のいずれかを選択できます：
  - **はい**：これを選択すると、Windows Update の更新プログラムを管理サーバーから受信するデバイスが検索結果に含まれます。
  - ［**いいえ**］。これを選択すると、Windows Update の更新プログラムを他の提供元から受信するデバイスが検索結果に含まれます。

ユーザー

［**ユーザー**］タブでは、オペレーティングシステムにログインしたユーザーのアカウントを基にデバイスを検索する基準を設定できます。

- **前回システムにログインしたユーザー**

  このオプションをオンにする場合は、［**参照**］をクリックしてユーザーアカウントを指定します。指定したユーザーがシステムの前回のログインを実行したデバイスが検索結果に含まれます。

- **少なくとも 1 回システムにログインしたユーザー**

  このオプションをオンにする場合は、［**参照**］をクリックしてユーザーアカウントを指定します。指定したユーザーがシステムに少なくとも 1 回ログインしたデバイスが検索結果に含まれます。

管理対象アプリケーションのステータスに影響がある問題

［**管理対象アプリケーションのステータスに影響がある問題**］タブでは、管理対象アプリケーションからのステータスの説明に基づくデバイスの検索を設定できます：

- **デバイスステータスの説明**

  管理対象アプリケーションからのステータスの説明に対応するチェックボックスをオンにできます。これらのステータスが受信されると、デバイスが抽出に含まれます。複数のアプリケーションを対象とするステータスについては、同じステータスをすべてのアプリケーションのリストで自動的に選択するオプションがあります。

管理対象アプリケーションのコンポーネントのステータス

［**管理対象アプリケーションのコンポーネントのステータス**］タブでは、管理対象アプリケーションのコンポーネントのステータスを基にデバイスを検索する基準を設定できます：

- **データ漏洩対策のステータス**

  データ漏洩対策のステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **コラボレーションサーバーの保護ステータス**

  サーバーコラボレーションの保護ステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **メールサーバーの保護ステータス**

  メールサーバーの保護のステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **Endpoint Sensor のステータス**

  Endpoint Sensor のステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

暗号化

- **暗号化**

  Advanced Encryption Standard（AES）対称ブロック暗号アルゴリズム。ドロップダウンリストから、暗号化キーのサイズ（56 ビット、128 ビット、192 ビット、または 256 ビット）を選択できます。

  指定可能な値：*AES56*、*AES128*、*AES192*、または *AES256*。

クラウドセグメント

［**クラウドセグメント**］タブでは、デバイスが特定のクラウドセグメントに属するかどうかを基に検索を設定できます：

- **デバイスがクラウドセグメント内にある**

このオプションを有効にすると、［**参照**］をクリックして、検索するセグメントを指定できます。

［**子オブジェクトも含む**］オプションも有効にする場合は、指定したセグメントのすべての子オブジェクトに対して検索が実行されます。

検索結果には、指定したセグメントのデバイスしか含まれません。

- **API を使用して検出されたデバイス**

  ドロップダウンリストで、API ツールによりデバイスが検出されるかどうかを選択できます：

  - **AWS**：AWS API を使用して検出されたデバイスで、これはデバイスが間違いなく AWS クラウド環境にあることを意味します。
  - **Azure**：Azure API を使用して検出されたデバイスで、これはデバイスが間違いなく Azure クラウド環境にあることを意味します。
  - **Google Cloud**：Google API を使用して検出されたデバイスで、これはデバイスが間違いなく Google Cloud 環境にあることを意味します。
  - ［**いいえ**］。デバイスは AWS API、Azure API、Google API のいずれでも検出できません。これはデバイスがクラウド環境外にあるか、クラウド環境内にあるが API では検出できないことを意味します。
  - **値なし**：この条件は当てはまりません。

製品コンポーネント

このセクションでは、対応する管理プラグインが管理コンソールにインストールされているアプリケーションのコンポーネントのリストが表示されます。

［**製品コンポーネント**］セクションでは、選択したアプリケーションの管理下にあるコンポーネントのステータスとバージョン番号を基にデバイスを抽出に含めるための基準を設定できます：

- **ステータス**

アプリケーションから管理サーバーに送信されたコンポーネントのステータスに基づいてデバイスを検索します。*デバイスからのデータなし*、*停止*、*開始中*、*一時停止*、*実行中*、*エラー*、*未インストール*のいずれかのステータスを選択できます。管理対象デバイスにインストールされたアプリケーションの選択したコンポーネントのステータスが指定したステータスと一致する場合、そのデバイスが抽出に含まれます。

製品から送信されるステータス：

- *開始中* - コンポーネントが利用開始プロセスを実行中です。
- *実行中* - コンポーネントが有効で正常に動作しています。
- *一時停止* - コンポーネントの動作が中断中です（例：管理対象製品でユーザーが保護を一時停止した）。
- *エラー* - コンポーネントの動作中にエラーが発生しました。
- *停止* - コンポーネントが無効で、現在動作していません。
- *未インストール* - 製品のカスタムインストールの設定時に、ユーザーがコンポーネントをインストール対象として選択しませんでした。

他のステータスとは異なり、［*デバイスからのデータなし*］ステータスはアプリケーションから送信されたものではありません。このステータスは、選択したコンポーネントのステータスについて、アプリケーションに情報がないことを示します。たとえば、デバイスにインストールされているアプリケーションのいずれにも選択したコンポーネントが属していない場合や、デバイスの電源がオフの場合などです。

- **バージョン**

リストで選択したコンポーネントのバージョン番号に基づいてデバイスを検索します。`3.4.1.0` などのバージョン番号を入力し、選択したコンポーネントのバージョン番号がこれと「等しい」「それより古い」「それより新しい」かを指定できます。また、指定したバージョンを除くすべてのバージョンを検索するようにも設定できます。

文字列変数でのマスクの使用

文字列の値に対してマスクを使用できます。マスクの作成に、次の正規表現を使用できます：

- ワイルドカード文字（*） - 0 文字以上の任意の文字列。
- 疑問符（?） - 任意の 1 文字。
- [<任意の範囲の文字列>] - 指定した範囲または集合に含まれる任意の 1 文字。
  例：[0–9] – 任意の数字。[abcdef] – a、b、c、d、e、f のうちの任意の 1 文字。

検索フィールドでの正規表現の使用

次の正規表現を検索フィールドで使用して、特定の単語や文字を検索することができます：

- * -任意の文字列に置き換えられます。Server、Servers、または Server room といった単語を検索するには、検索フィールドに「`Server*`」と入力します。

- ? -任意の 1 文字を表します。Word または Ward といった単語を検索するには、検索フィールドに「`W?rd`」と入力します。

  検索フィールドのテキストを疑問符（?）で始めることはできません。

- [<任意の範囲の文字列>] -指定した範囲または集合に含まれる任意の 1 文字を表します。任意の数字を検索するには、検索フィールドに「`[0-9]`」と入力します。a、b、c、d、e、または f のいずれかの文字を検索するには、検索フィールドに「`[abcdef]`」と入力します。

検索フィールドで以下の正規表現を使用することにより全文検索を実行できます：

- スペース -指定した単語のいずれかがコメントに含まれているデバイスがすべて検索されます。たとえば、「Secondary」または「Virtual」のいずれか（または両方）の単語が含まれる語句を検索するには、検索フィールドに「`Secondary Virtual`」と入力します。

- プラス記号（+）、AND、または && -単語の前にプラス記号を付けると、すべての検索結果にその単語が含まれます。たとえば、「Secondary」と「Virtual」両方の単語を含む語句を検索するには、検索フィールドに「`+Secondary+Virtual`」「`Secondary AND Virtual`」「`Secondary && Virtual`」のいずれかを入力します。

- OR または || -2 つの単語の間に置いた場合、どちらかの単語がテキスト内に含まれることを示します。「Secondary」または「Virtual」のどちらかの単語を含む語句を検索するには、検索フィールドに「`Secondary OR Virtual`」または「`Secondary || Virtual`」と入力します。

- マイナス記号（-） -単語の前にマイナス記号を付けると、すべての検索結果にその単語が含まれません。「Secondary」という単語を含み、「Virtual」という単語を含まない語句を検索するには、検索フィールドに「`+Secondary-Virtual`」と入力します。

- "< 任意のテキスト >"。引用符で囲まれたテキストを含むテキストが検索されます。「Secondary Server」といった単語の組み合わせを含む語句を検索するには、検索フィールドに「`" Secondary Server "`」と入力します。

全文検索は以下のフィルタリングブロックで使用可能です：

- イベントリストフィルタリングブロックでは、［**イベント**］列および［**説明**］列による

- ユーザーアカウントフィルタリングブロックでは、［**名前**］列による

- アプリケーションレジストリフィルタリングブロックでは、［**リストで表示**］セクションでフィルタリング条件として［**グループ化なし**］が選択されている場合、［**名前**］列による

ウィンドウからのリストのエクスポート

アプリケーションのウィンドウで、オブジェクトのリストをエクスポートできます。

オブジェクトのリストをエクスポートするには、ダイアログボックスで［**ファイルへのエクスポート**］をクリックします。

タスク設定

このセクションでは、Kaspersky Security Center のタスクのすべての設定について説明します。

タスクの全般的な設定

このセクションでは、ほとんどのタスクで表示および構成できる設定について説明します。使用可能な設定のリストは、構成しているタスクによって異なります。

タスク作成時に指定する設定

タスク作成時に次の設定を指定できます。これらの設定の一部は、作成したタスクのプロパティから変更することもできます。

- OS の再起動設定：
  - **デバイスを再起動しない**

    操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

  - **デバイスを再起動する**

    インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

  - **ユーザーに処理を確認する**

    手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

    既定では、このオプションがオンです。

  - **通知の繰り返し間隔（分）**

    このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

    既定では、このオプションはオンです。既定の間隔は 5 分です。1分から1,440 分までの値を指定できます。

    このオプションをオフにすると、確認メッセージは1回だけ表示されます。

- **再起動するまでの時間（分）**

  ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

  既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

- タスクスケジュールの設定：
  - **実行予定設定：**
    - **N 時間ごと**

      指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

      既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

    - **N 日ごと**

      日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

      既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

    - **N 週間ごと**

      指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

      既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

    - **N 分ごと**

      タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

      既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

    - **毎日（サマータイムはサポートしていません）**

日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を1時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

このスケジュールの使用は推奨されません。Kaspersky Security Center の旧バージョンとの後方互換性を維持するために用意されているオプションとなります。

既定では、毎日、現在のシステム時刻にタスクが実行されます。

- **毎週**

  毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。

  指定した日付が存在しない月には、月の最終日にタスクを実行します。

  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。

  規定では、日付は選択されていません。規定の開始時間は 18:00 です。

- **新しいアップデートがリポジトリにダウンロードされ次第**

  アップデートのリポジトリへのダウンロードが完了すると、タスクが実行されます。たとえば、脆弱性とアプリケーションのアップデートの検索タスクのスケジュールを設定する時に、このオプションを使用すると便利です。

- **ウイルスアウトブレイク検知次第**

［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

- ワークステーションとファイルサーバー向けアンチウイルス製品
- 境界防御向けアンチウイルス製品
- メールサーバー向けアンチウイルス製品

既定では、すべてのアプリケーション種別がオンです。

ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

- タスク名で検索するには、検索フィールドにタスク名を入力します。
- 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。

  既定では、タスクはアルファベットの昇順で並べ替えられます。
- フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる(分)**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  既定では、このオプションはオフです。既定の時間は1分です。

- タスクを割り当てるデバイス：

  - **ネットワークの管理サーバーによって検出されたデバイスを選択する**

    タスクを特定のデバイスに割り当てます。特定のデバイスには、管理グループに属するデバイスと管理グループが割り当てられていないデバイスの両方を含めることができます。

    たとえば、未割り当てデバイスでネットワークエージェントのインストールタスクを実行する時に、このオプションを使用すると便利です。

  - **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

    タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

    特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

  - **デバイスの抽出にタスクを割り当てる**

    デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

    たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

  - **管理グループにタスクを割り当てる**

任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

- アカウントの設定：
  - **既定のアカウント**

    タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。

    既定では、このオプションがオンです。

  - **アカウントの指定**

    ［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

  - **アカウント**

    タスクを実行するアカウント。

  - **パスワード**

    タスクが実行されるアカウントのパスワード。

タスク作成後に指定する設定

次の設定は、タスク作成後にのみ指定できます。

- グループタスクの設定：
  - **サブグループへ導入**

    このオプションはグループタスクの設定内でのみ使用可能です。

    このオプションをオンにすると、タスク範囲には次のものが含まれます：
    - タスクの作成中に選択した管理グループ。
    - 選択された管理グループに属する管理グループのすべてのレベルはグループ階層の下にあります。

    このオプションをオフにすると、タスク範囲にはタスクの作成中に選択された管理グループのみが含まれます。

    既定では、このオプションはオンです。

- **セカンダリまたは仮想管理サーバーに配信**

  このオプションをオンにすると、プライマリ管理サーバーに対して有効なタスクがセカンダリ管理サーバーに対しても適用されます（仮想管理サーバーも含まれます）。同じ種別のタスクがセカンダリ管理サーバーに既に存在する場合は、既存のタスクとプライマリ管理サーバーから継承した両方のタスクがセカンダリ管理サーバーに適用されます。

  このオプションは［**サブグループへ導入**］がオンになっている場合にのみ使用可能です。

  既定では、このオプションはオフです。

- スケジュールの詳細設定

  - **Wake on LAN の機能を使用してタスク開始前にデバイスを起動する（分）**

    タスク開始よりも指定した時間だけ前に、デバイス上のオペレーティングシステムが起動します。既定では、時間は 5 分です。

    タスクの開始予定時刻が近づいても電源がオフだったデバイスも含めて、タスク範囲に含まれるすべてのクライアントデバイスでタスクを実行するには、このオプションをオンにします。

    タスクの完了後にデバイスの電源を自動的にオフにする場合は、［**タスク完了後にデバイスをシャットダウンする**］を有効にします。このオプションは同じウィンドウ内にあります。

    既定では、このオプションはオフです。

  - **タスク完了後にデバイスをシャットダウンする**

    たとえば、毎週金曜日の業務時間終了後にクライアントデバイスへのアップデートのインストールを行い、その後デバイスの電源を切りたい時に、アップデートインストールタスクでこのオプションを使用できます。

    既定では、このオプションはオフです。

  - **次の時間を超える場合はタスクを停止する（分）**

    指定した時間が経過すると、タスクが完了したかどうかに関係なくタスクが自動的に停止します。

    実行に時間がかかり過ぎているタスクを中断したい時に、このオプションを使用します。

    既定では、このオプションはオフです。既定のタスク実行時間は 120 分です。

- 通知の設定：

  - ［**タスク履歴の保存**］セクション：

    - **管理サーバー上に保存（日）**

      タスク範囲に含まれるすべてのクライアントデバイスでのタスク実行に関するアプリケーションイベントが、指定した日数の間、管理サーバーに保存されます。この期間が過ぎると、情報が管理サーバーから削除されます。

      既定では、このオプションはオンです。

    - **デバイスの OS イベントログに保存**

タスク実行に関するアプリケーションイベントが、各クライアントデバイスの Windows イベントログにローカルで保存されます。

既定では、このオプションはオフです。

- **管理サーバーの OS イベントログに保存**

  タスク範囲に含まれるすべてのクライアントデバイスでのタスク実行に関するアプリケーションイベントが、管理サーバーのオペレーティングシステムの Windows イベントログに一元的に保存されます。

  既定では、このオプションはオフです。

- **すべてのイベントを保存**

  このオプションをオンにすると、タスクに関するすべてのイベントがイベントログに保存されます。

- **タスクの進捗に関連したイベントを保存**

  このオプションをオンにすると、タスク実行に関するイベントのみがイベントログに保存されます。

- **タスク実行結果のみ保存**

  このオプションをオンにすると、タスクの実行結果に関するイベントのみがイベントログに保存されます。

- **管理者にタスク実行結果を通知**

  管理者がタスク実行結果の通知を受け取る方法を、メール、SMS、実行ファイルの実行から選択できます。通知を設定するには、［**設定**］をクリックします。

  既定では、すべての通知方法がオフです。

- **エラーのみ通知**

  このオプションをオンにすると、管理者はタスクでエラーが発生して終了した場合にのみ通知を受け取ります。

  このオプションをオフにすると、管理者はタスク終了時に常に通知を受け取ります。

  既定では、このオプションはオンです。

- セキュリティ設定
- タスク範囲の設定

  タスク範囲の指定方法に応じて、次の設定が表示されます：

  - **デバイス**

タスク範囲が管理グループを使用して指定されている場合、該当するグループを表示できます。ここでは、設定を変更することはできません。ただし、［**タスク範囲からの除外**］を設定できます。

タスク範囲がデバイスのリストを使用して指定されている場合、デバイスを追加したり削除してこのリストを変更できます。

- **デバイスの抽出**

  タスクが適用されるデバイスの抽出を変更できます。

- **タスク範囲からの除外**

  タスクを適用しないデバイスのグループを指定できます。タスク範囲から除外できるのは、タスクが適用されない管理グループのサブグループのみです。

- **変更履歴**

［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの設定

タスク作成時に指定する設定

タスク作成時に次の設定を指定できます。これらの設定の一部は、作成したタスクのプロパティから変更することもできます。

- **アップデート元**

管理サーバーのアップデート元として、使用できるものは次のとおりです：

- カスペルスキーのアップデートサーバー

  カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。既定では、管理サーバーは HTTPS プロトコルを使用してカスペルスキーのアップデートサーバーに接続し、アップデートをダウンロードします。必要に応じて、管理サーバーで HTTPS プロトコルの代わりに HTTP プロトコルを使用するように設定を編集できます。

  既定では、この項目が選択されます。

- プライマリ管理サーバー

  セカンダリ管理サーバーまたは仮想管理サーバーを対象とするタスクに適用されます。

- ローカルまたはネットワークフォルダー

  最新のアップデートが保存されたローカルフォルダーまたはネットワークフォルダー：ネットワークフォルダーとしては FTP サーバー、HTTP サーバー、または SMB 共有を指定できます。ネットワークフォルダーに認証が必要な場合、SMB プロトコルのみがサポートされています。ローカルフォルダーの選択時には、管理サーバーがインストールされているデバイスのフォルダーを指定する必要があります。

  > アップデート元で使用される FTP/HTTP サーバーまたはネットワークフォルダーは、アップデートを含み、フォルダーの構造がカスペルスキーのアップデートサーバーの使用時に作成された構造と一致する必要があります。

- **その他の設定**

セカンダリ管理サーバーの強制アップデート

このオプションをオンにすると、管理サーバーは、新しいアップデートがダウンロードされるとすぐに、セカンダリ管理サーバーのアップデートタスクを開始します。アップデートタスクは、セカンダリ管理サーバーのタスクプロパティで構成されているアップデートソースを使用して開始されます。

このオプションをオフにすると、セカンダリ管理サーバーのアップデートタスクは、スケジュールに従って開始されます。

既定では、このオプションはオフです。

ダウンロード済みのアップデートを追加のフォルダーにコピー

管理サーバーがアップデートを受信すると、指定されたフォルダーにコピーします。ネットワークでのアップデートの配信を手動で管理する場合は、このオプションをオンにします。

このオプションの使用を検討する状況としては、たとえば、組織のネットワークが複数の独立したサブネットワークで構成され、各サブネットワークに属するデバイスは別のサブネットワークへのアクセス権を付与されていない場合があります。ただし、すべてのサブネットワークのデバイスは共通のネットワーク共有へのアクセス権は付与されています。この場合、いずれかのサブネットワークの管理サーバーでカスペルスキーのアップデートサーバーからアップデートをダウンロードするように設定した後、このオプションをオンにし、ネットワーク共有をコピー先に指定します。他の管理サーバーでは、リポジトリへのアップデートのダウンロードタスクのアップデート元として、このネットワーク共有を指定します。

既定では、このオプションはオフです。

アップデートのコピーが完了していない場合はデバイスおよびセカンダリ管理サーバーを強制アップデートしない

クライアントデバイスとセカンダリ管理サーバーでのアップデートのダウンロードタスクは、元のネットワークフォルダーから追加のアップデートフォルダーにアップデートがコピーされるまで開始されません。

クライアントデバイスとセカンダリ管理サーバーが、追加のネットワークフォルダーからアップデートをダウンロードする場合は、このオプションをオンにする必要があります。

既定では、このオプションはオフです。

タスク作成後に指定する設定

次の設定は、タスク作成後にのみ指定できます。

- ［**設定**］セクション→［**アップデートの内容**］ブロック

  差分ファイルのダウンロード

  このオプションで差分ファイルのダウンロードを有効にすることができます。

  既定では、このオプションはオフです。

- ［**アップデートの検証**］セクション

  配信前にアップデートを検証する

  管理サーバーはアップデート元からアップデートをダウンロードし、それらを一時リポジトリに保存して、［**アップデート検証タスク**］で定義されたタスクを実行します。タスクが正常に終了すると、アップデートは一時保管領域から管理サーバーの共有フォルダーにコピーされ、この管理サーバーをアップデート元とするすべてのデバイスに配信されます（［**新しいアップデートがリポジトリにダウンロードされ次第**］のスケジュールが設定されたタスクが開始されます）。アップデートをリポジトリにダウンロードするタスクが完了するのは、*アップデートの検証*タスクの完了後のみです。

  既定では、このオプションはオフです。

  アップデート検証タスク

  このタスクでは、ダウンロードされたアップデートが管理サーバーをアップデート元とするすべてのデバイスに配信される前にアップデートの検証を行います。

  このフィールドで、以前作成した*アップデートの検証*タスクを選択することができます。または、*アップデートの検証*タスクを新規に作成することもできます。

［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの設定

タスク作成時に指定する設定

タスク作成時に次の設定を指定できます。これらの設定の一部は、作成したタスクのプロパティから変更することもできます。

- **アップデート元**

  ディストリビューションポイントのアップデート元として、使用できるものは次の通りです：

  - カスペルスキーのアップデートサーバー

    カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。

    既定ではこのオプションが選択されます。

  - プライマリ管理サーバー

    セカンダリ管理サーバーまたは仮想管理サーバーを対象とするタスクに適用されます。

  - ローカルまたはネットワークフォルダー

    最新のアップデートが保存されたローカルフォルダーまたはネットワークフォルダー：ネットワークフォルダーとしては FTP サーバー、HTTP サーバー、または SMB 共有を指定できます。ネットワークフォルダーに認証が必要な場合、SMB プロトコルのみがサポートされています。ローカルフォルダーの選択時には、管理サーバーがインストールされているデバイスのフォルダーを指定する必要があります。

    > アップデート元で使用される FTP/HTTP サーバーまたはネットワークフォルダーは、アップデートを含み、フォルダーの構造がカスペルスキーのアップデートサーバーの使用時に作成された構造と一致する必要があります。

- ［**その他の設定**］→［**アップデート保存先フォルダー**］

  保存したアップデートを保管するためのフォルダーのパス。指定したフォルダーのパスをクリップボードにコピーすることができます。グループタスクに対して指定されたフォルダーのパスを変更することはできません。

タスク作成後に指定する設定

タスクが作成された後でのみ、［**設定**］セクションの［**アップデートの内容**］ブロックで次の設定を指定できます。

差分ファイルのダウンロード

このオプションで差分ファイルのダウンロードを有効にすることができます。

既定では、このオプションはオフです。

脆弱性とアプリケーションのアップデートの検索タスクの設定

タスク作成時に指定する設定

タスク作成時に次の設定を指定できます。これらの設定の一部は、作成したタスクのプロパティから変更することもできます。

- **Microsoft による脆弱性とアップデートのリストを検索する**

  脆弱性とアップデートの検索時に、Kaspersky Security Center は、現時点で適用可能な Microsoft Update のアップデート元からの該当する Microsoft Update の情報を使用します。

  Microsoft Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

  既定では、このオプションはオンです。

- **アップデートサーバーに接続してアップデートを取得**

管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元として指定した場所に接続します。以下のサーバーを Microsoft Update のアップデート元として動作させることができます：

- Kaspersky Security Center 管理サーバー（詳細は、「ネットワークエージェントのポリシーの設定」を参照してください）
- 組織ネットワーク内で Microsoft Windows Server Update Services（WSUS）として機能している Windows Server
- Microsoft Update サーバー

このオプションをオンにすると、管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元に接続して、該当する Microsoft Windows Update の情報を最新にします。

このオプションをオフにすると、管理対象デバイス上の Windows Update エージェントは Microsoft アップデートプログラムのソースから以前に受信した、該当する Microsoft Windows アップデートプログラムに関する情報を使用します。

Microsoft Update のアップデート元への接続は、多くのリソースを消費します。別のタスクまたはセクション［**ソフトウェアのアップデートと脆弱性**］のネットワークエージェントのポリシーのプロパティで、アップデート元へ定期的に接続するように設定している場合は、このオプションをオフにすることを検討してください。このオプションをオフにしない場合は、サーバーの負荷を下げるために、タスクの開始を 360 分以内でランダムに遅延させるようにタスクのスケジュールを設定できます。

既定では、このオプションはオンです。

ネットワークエージェントのポリシーの設定の各オプションの組み合わせに応じて、以下のようにアップデートの取得方法が異なります：

- 管理対象デバイス上の Windows Update エージェントがアップデートサーバーに接続してアップデートを取得するのは、［*脆弱性とアプリケーションのアップデートの検索*］タスクのプロパティでアップデートサーバーに［**アップデートサーバーに接続してアップデートを取得**］が有効になっており、ネットワークエージェントポリシーの設定で［**Windows Update 検索モード**］が［**アクティブ**］に設定されている場合のみです。
- *脆弱性スキャン*タスクを実行する時に、ネットワークエージェントが Microsoft Windows アップデート元への接続を開始して更新をダウンロードする必要がない場合は、［**Windows Update 検索モード**］を［**パッシブ**］に設定できますが、［**アップデートサーバーに接続してアップデートを取得**］は有効のままにする必要があります。これにより、リソースを節約し、以前に受信した Windows アップデートプログラムを使用して脆弱性をスキャンできるようになります。
  Microsoft Windows アップデートプログラムの受信を別の方法で構成する場合は、パッシブモードを使用できます。Microsoft Windows アップデートプログラムの受信が別の方法で構成されていない場合は、**Windows Update 検索モード**オプションを**[パッシブ]** に設定しないでください。この場合、アップデートプログラムに関する情報は受信されません。
- ［**アップデートサーバーに接続してアップデートを取得**］の状態（オンまたはオフ）に関係なく、［**Windows Update 検索モード**］が［**無効**］に設定されている場合、Kaspersky Security Center はアップデートプログラムに関する情報を要求しません。

- **カスペルスキーによるサードパーティ製品の脆弱性とアップデートのリストを検索する**

このオプションをオンにすると、Kaspersky Security Center は Windows のレジストリおよび［**ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**］で指定したフォルダーに存在するサードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）の脆弱性とアップデートを検索します。サポート対象のサードパーティ製品の全リストはカスペルスキーが管理しています。

このオプションをオフにすると、サードパーティ製品の脆弱性とアップデートの検索は行われません。Microsoft Windows Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

既定では、このオプションはオンです。

- **ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**

  Kaspersky Security Center が脆弱性の修正とアップデートのインストールが必要なアプリケーションを検索する時に対象とするフォルダーです。システム変数を使用できます。

  アプリケーションがインストールされているフォルダーを指定します。既定では、ほとんどのアプリケーションのインストール先となっているシステムフォルダーがリストに含まれます。

- **詳細な診断を有効にする**

  このオプションをオンにすると、Kaspersky Security Center リモート診断ユーティリティでネットワークエージェントによるトレースがオフになっていても、ネットワークエージェントがトレースを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

  このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center リモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

  タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

  既定では、このオプションはオフです。

- **詳細な診断ファイルの最大サイズ（MB）**

  既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

［アップデートのインストールと脆弱性の修正］タスクの設定

タスク作成時に指定する設定

タスク作成時に次の設定を指定できます。これらの設定の一部は、作成したタスクのプロパティから変更することもできます。

- **アップデートのインストールのルールを指定します**

  これらのルールはクライアントデバイスでのアップデートのインストールに適用されます。ルールが指定されていない場合、タスクはなにも実行しません。ルールの使用法については、「アップデートインストールのルール」を参照してください。

- **デバイスの再起動時またはシャットダウン時にインストールを開始する**

  このオプションをオンにすると、デバイスの再起動時またはシャットダウン時にアップデートがインストールされます。オプションがオフの場合、アップデートのインストールはスケジュールに従って実行されます。

  アップデートのインストールによりデバイスのパフォーマンスに影響を与える可能性がある場合は、このオプションを使用します。

  既定では、このオプションはオフです。

- **必要なシステムコンポーネントをインストールする**

  このオプションをオンにすると、アップデートのインストール前にインストールが必要な一般システムコンポーネントをすべて自動的にインストールします。インストールが必要な対象とは、たとえばオペレーティングシステムのアップデートなどです。

  このオプションをオフにすると、必須コンポーネントを手動でインストールすることが必要となる場合があります。

  既定では、このオプションはオフです。

- **アップデート中に新しい製品のバージョンのインストールを許可する**

  このオプションをオンにすると、製品の新しいバージョンをインストールするアップデートを許可できます。

  このオプションをオフにすると、製品はアップグレードされません。製品の新しいバージョンは手動でインストールするか、別のタスクを通してインストールできます。この設定は、所属企業のインフラストラクチャでソフトウェアの新しいバージョンがサポートされていなかったり、アップグレードをテスト環境で確認したい場合に使用します。

  既定では、このオプションはオンです。

  > 製品をアップデートすることにより、クライアントデバイスにインストールされた対象製品に依存するアプリケーションが正しく動作しなくなることがあります。

- **デバイスにアップデートをダウンロードするがインストールしない**

  このオプションをオンにすると、アップデートをデバイスにダウンロードしますが、自動ではインストールしません。ダウンロードされたアップデートを手動でインストールできます。

  Microsoft 製品のアップデートは、システム Windows フォルダーにダウンロードされます。サードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートは、［**アップデートのダウンロード先**］で指定したフォルダーにダウンロードされます。

  このオプションをオフにすると、アップデートはデバイスに自動的にインストールされません。

  既定では、このオプションはオフです。

  - **アップデートのダウンロード先**

このフォルダーはサードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートのダウンロードに使用されます。

- **詳細な診断を有効にする**

  このオプションをオンにすると、Kaspersky Security Center リモート診断ユーティリティでネットワークエージェントによるトレースがオフになっていても、ネットワークエージェントがトレースを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

  このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center リモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

  タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

  既定では、このオプションはオフです。

  - **詳細な診断ファイルの最大サイズ（MB）**

    既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

タスク作成後に指定する設定

以下の一覧に表示された設定は、タスク作成後にのみ指定できます。タスク設定の詳細な説明については、「タスクの全般的な設定」を参照してください。

- **全般**。このセクションには、タスクに関する一般的な情報が表示されます。また、*アップデートのインストールと脆弱性の修正*タスクを適用するデバイスを指定できます。

  - **サブグループへ導入**

    このオプションはグループタスクの設定内でのみ使用可能です。

    このオプションをオンにすると、タスク範囲には次のものが含まれます：

    - タスクの作成中に選択した管理グループ。
    - 選択された管理グループに属する管理グループのすべてのレベルはグループ階層の下にあります。

    このオプションをオフにすると、タスク範囲にはタスクの作成中に選択された管理グループのみが含まれます。

    既定では、このオプションはオンです。

  - **セカンダリまたは仮想管理サーバーに配信**

このオプションをオンにすると、プライマリ管理サーバーに対して有効なタスクがセカンダリ管理サーバーに対しても適用されます（仮想管理サーバーも含まれます）。同じ種別のタスクがセカンダリ管理サーバーに既に存在する場合は、既存のタスクとプライマリ管理サーバーから継承した両方のタスクがセカンダリ管理サーバーに適用されます。

このオプションは［**サブグループへ導入**］がオンになっている場合にのみ使用可能です。

既定では、このオプションはオフです。

- インストールするアップデート

  ［**インストールするアップデート**］セクションで、タスクでインストールされるアップデートのリストを確認できます。適用するタスク設定の条件に一致するアップデートのみが表示されます。

- アップデートのテストインストール：

  - **スキャンしない**：アップデートのテストインストールを実行しない場合は、このオプションを選択します。

  - **選択されたデバイスでスキャンを実行**：選択したデバイスでアップデートのインストールをテストする場合、このオプションを選択します。［**追加**］をクリックし、アップデートのテストインストールを実行するデバイスを選択します。

  - **指定されたグループのデバイスでスキャンを実行**：特定のグループ内のデバイスでアップデートのインストールをテストする場合、このオプションを選択します。［**テストグループの指定**］に、テストインストールを実行するデバイスのグループを指定します。

  - **指定された割合のデバイスにスキャンを実行**：デバイスの一部でアップデートのインストールをテストする場合、このオプションを選択します。［**対象の全デバイス内でテストデバイスが占める割合**］に、アップデートのテストインストールを実行するデバイスの割合をパーセントで指定します。

サブネットのグローバルリスト

このセクションでは、ルールで使用できるサブネットのグローバルリストについて説明します。

ネットワークに含まれるサブネットの情報を保存するために、使用している各管理サーバーに対してサブネットのグローバルリストを設定できます。リストは、IP アドレスとマスクのペアと支社などの物理的な単位を対応させる上で役立ちます。ネットワークのルールと設定でこのリストにあるサブネットを使用できます。

サブネットのグローバルリストへのサブネットの追加

サブネットのグローバルリストに、サブネットとその説明を追加できます。

サブネットのグローバルリストにサブネットを追加するには

1. コンソールツリーで、目的の管理サーバーを選択します。

2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。

3. **プロパティ**ウィンドウが表示されたら、［**セクション**］ペインで［**グローバルサブネットのリスト**］を選択します。

4. ［**追加**］をクリックします。
［**新規サブネット**］ウィンドウが表示されます。

5. 次のフィールドに値を入力します：

- **全般z設定**

  追加するサブネットのサブネット IP アドレス

- **サブネットマスク**

  追加するサブネットのサブネットマスク

- **名前**

  サブネットの名前です。サブネットのグローバルリスト内では一意である必要があります。リスト内に既に存在する名前を入力した場合は、次のような接尾辞が追加されます：~~1、~~2.

- **説明**

  説明には、該当するサブネットに対応する支社の情報などを追加で記載することができます。この説明は、トラフィック制限ルールのリストなどサブネットが表示されるすべてのリストに表示されます。

  このフィールドの入力は必須ではなく、空白のままにすることも可能です。

6. ［**OK**］をクリックします。

サブネットがサブネットのリストに表示されます。

サブネットのグローバルリストでのサブネットのプロパティの表示と編集

サブネットのグローバルリストで、サブネットのプロパティを表示したり編集できます。

サブネットのグローバルリストでサブネットのプロパティを表示または編集するには：

1. コンソールツリーで、目的の管理サーバーを選択します。

2. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。

3. **プロパティ**ウィンドウが表示されたら、左側の［**セクション**］ペインで［**グローバルサブネットのリスト**］を選択します。

4. リスト内の目的のサブネットを選択します。

5. ［**プロパティ**］をクリックします。
［**新規サブネット**］ウィンドウが表示されます。

6. 必要に応じて、サブネットの設定を変更します。

7. ［OK］をクリックします。

変更を行った場合は、その内容が保存されます。

Windows 用、macOS 用、Linux 用ネットワークエージェントの用途：比較

ネットワークエージェントの用途は、デバイスのオペレーティングシステムによって異なります。ネットワークエージェントのポリシーの設定とインストールパッケージの設定も、オペレーティングシステムによって異なります。次の表は、Windows、macOS、および Linux オペレーティングシステムで使用可能なネットワークエージェントの機能と使用シナリオを比較したものです。

ネットワークエージェントの機能の比較

ネットワークエージェントの機能	Windows	macOS	Linux
インストール			
Kaspersky Security Center のインストール後に、ネットワークエージェントのインストールパッケージを自動作成	✓	–	–
Kaspersky Security Center のリモートインストールタスクでの特別なオプションを使用した強制的なインストール実行	✓	✓	✓
Kaspersky Security Center が生成したスタンドアロンパッケージに対して、デバイスユーザーリンクを送信してのインストール	✓	✓	✓
オペレーティングシステムとネットワークエージェントをインストールした管理者のハードディスクのイメージをクローン化してのインストール：ディスクイメージ処理用として Kaspersky Security Center から提供されたツールを使用する。	✓	–	–
サードパーティ製のツールを使用した、管理者のハードドライブのイメージの複製によるオペレーティングシステムとネットワークエージェントのインストール	✓	✓	✓
アプリケーションのリモートインストールにおけるサードパーティ製のツールを使用したインストール	✓	✓	✓
デバイスでアプリケーションインストーラーを実行しての手動インストール	✓	✓	✓
サイレントモードでのネットワークエージェントのインストール	✓	✓	✓
クライアントデバイスから管理サーバーへの手動接続：klmover ユーティリティ	✓	✓	✓
Kaspersky Security Center コンポーネントのアップデートとパッチの自動インストール	✓	–	✓
ライセンスの自動配信	✓	✓	✓
強制同期	✓	✓	✓
ディストリビューションポイント			
ディストリビューションポイントとして使用	✓	✓	✓
ディストリビューションポイントの自動割り当て	✓	✓ Network Location Awareness（NLA）を使用しない場合。	✓

			Network Location Awareness（NLA）を使用しない場合。
ネットワークポーリング	✓ • Windows ネットワークのポーリング • IP アドレス範囲のポーリング • ドメインコントローラーのポーリング（Microsoft Active Directory）	✓ • IP アドレス範囲のポーリング • Zeroconf ポーリング • ドメインコントローラーのポーリング（Microsoft Active Directory、Samba 4 Active Directory）	–
ディストリビューションポイントでの KSN プロキシサービスの実行	✓	–	✓
管理対象デバイスにアップデートを配布するディストリビューションポイントリポジトリに、カスペルスキーのアップデートサーバー経由でアップデートをダウンロードする	✓	– （［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの対象範囲に Linux または macOS を実行しているデバイスが 1 台以上含まれている場合、すべての Windows デバイスでタスクが正常に完了した場合でも、タスクには「失敗」ステータスが付与されます）	✓
アプリケーションのプッシュインストール	✓	制限あり：macOS ディストリビューションポイントを使用して Windows デバイスにプッシュインストールを実行することはできません。	制限あり：Linux ディストリビューションポイントを使用して Windows デバイスにプッシュインストールを実行することはできません。
プッシュサーバーとしての使用	✓	–	✓
サードパーティ製品の取り扱い			
デバイスへのアプリケーションのリモートインストール	✓	–	–
ソフトウェアのアップデート	✓	–	–
ネットワークエージェントポリシーでのオペレーティングシステムのアップデートの設定	✓	–	–
ソフトウェアの脆弱性に関する情報の表示	✓	–	–
アプリケーションの脆弱性スキャン	✓	–	–
デバイスにインストールされたソフトウェアのインベントリ	✓	–	✓
仮想マシン			
仮想マシンへのネットワークエージェントのインストール	✓	✓	✓
仮想デスクトップインフラストラクチャ（VDI）に合わせた設定の最適化	✓	✓	✓
動的仮想マシンのサポート	✓	✓	✓
その他			
リモートクライアントデバイスでの Windows デスクトップ共有を使用した操作の監査	✓	–	–

アンチウイルスによる保護のステータスの監視	✓	✓	✓
デバイスの再起動の管理	✓	–	–
ファイルシステムロールバックのサポート	✓	✓	✓
ネットワークエージェントを接続ゲートウェイとして使用する	✓	✓	✓
接続マネージャー	✓	✓	✓
別の管理サーバーへのネットワークエージェントの接続先の切り替え（ネットワーク上の位置により自動的に実行）	✓	✓	–
クライアントデバイスと管理サーバー間の接続の確認：klnagchk ユーティリティ	✓	✓	✓
クライアントデバイスのデスクトップへのリモート接続	✓	✓ VNC（Virtual Network Computing）を使用	–
移行ウィザードを使用したスタンドアロンインストールパッケージのダウンロード	✓	✓	✓
Zeroconf ポーリング	–	–	✓

Kaspersky Security Center Web コンソール

Kaspersky Security Center Web コンソール（以降、Kaspersky Security Center Web コンソールとも表記）は、カスペルスキー製品により保護されるネットワークのセキュリティシステムのステータスを管理する目的で設計された Web アプリケーションです。

このアプリケーションを使用して、次のことができます：

- 組織のセキュリティシステムのステータスの管理
- ネットワーク上のデバイスへのカスペルスキー製品のインストールおよびインストールされた製品の管理
- ネットワーク上のデバイスに対して作成されたポリシーの管理
- ユーザーアカウントの管理
- ネットワーク上のデバイスにインストールされたアプリケーションのタスクの管理
- セキュリティシステムのステータスに関するレポートの表示
- システム管理者や他の IT 担当者へのレポート配信の管理

ハードウェアおよびソフトウェアの要件については、「Web コンソールの要件」を参照してください。

Kaspersky Security Center Web コンソールは、ブラウザーを使用してデバイスと管理サーバーが対話できるようにする Web インターフェイスを提供します。管理サーバーは、ネットワーク内のデバイスにインストールされたカスペルスキー製品の管理を目的として設計されたアプリケーションです。管理サーバーは、セキュアソケットレイヤー（SSL）プロトコルで保護されたチャネルでネットワークのデバイスに接続します。ブラウザーを使用して Kaspersky Security Center Web コンソールに接続する場合、ブラウザーは Kaspersky Security Center Web コンソールサーバーとの接続を確立します。

Kaspersky Security Center Web コンソールは、次のように操作します：

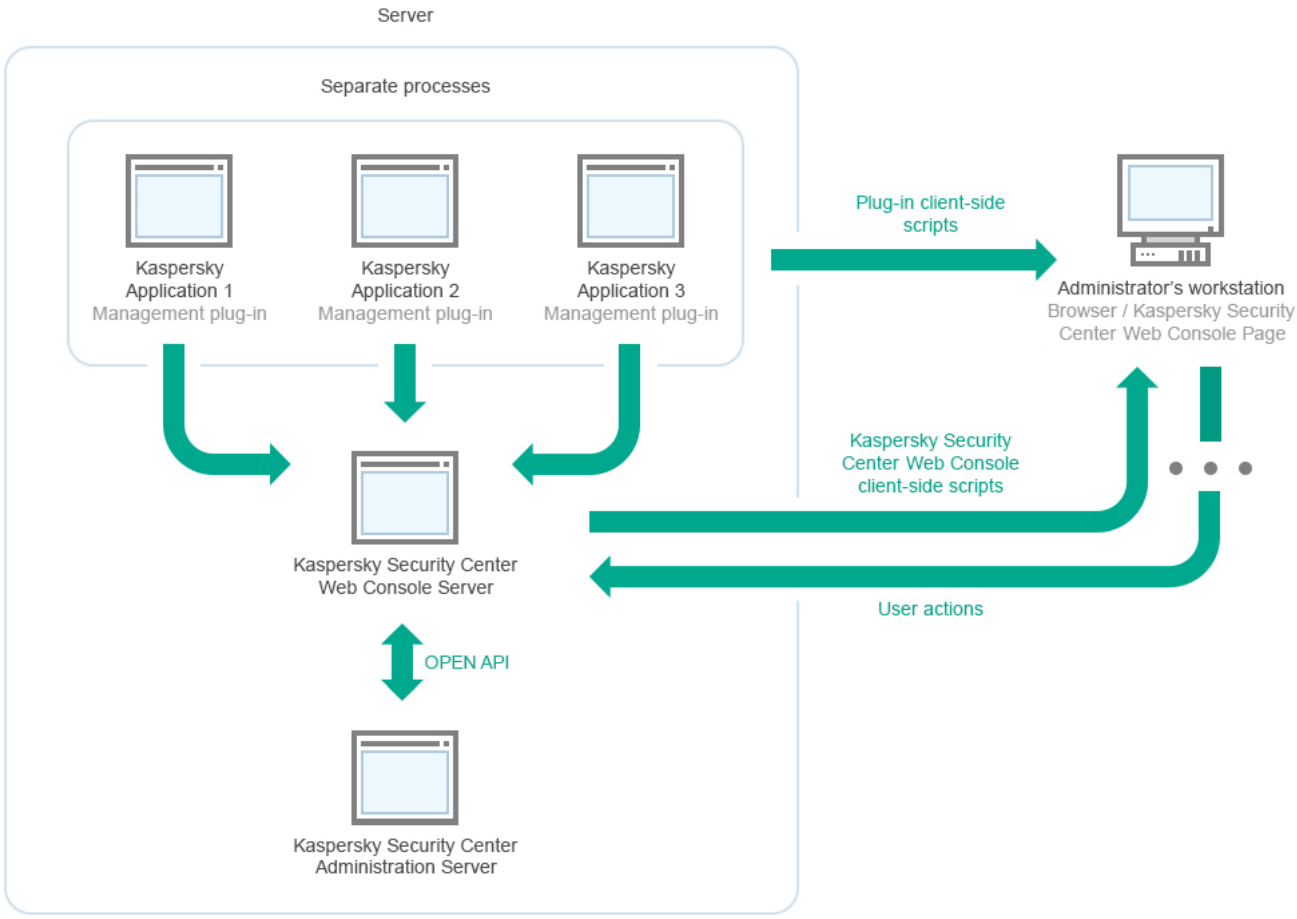
1. ブラウザーで Kaspersky Security Center Web コンソールに接続すると、Web ポータルのインターフェイスが表示されます。
2. Web ポータルによる管理を使用して、実行するコマンドを選択します。Kaspersky Security Center Web コンソールは次の操作を実行します：
   - 情報を受信する目的でコマンドを実行した場合（デバイスのリストを表示するなど）、Kaspersky Security Center Web コンソールは管理サーバーに対する情報のリクエストを生成し、必要なデータを受信し、表示に適した形式でブラウザーに送信します。
   - 管理用のコマンドを選択した場合（アプリケーションのリモートインストールなど）、Kaspersky Security Center Web コンソールはブラウザーからコマンドを受信し、それを管理サーバーに送信します。その後、管理サーバーからコマンドの結果を受信し、それを表示に適した形式でブラウザーに送信します。

Kaspersky Security Center Web コンソールは多言語で使用できます。本製品を開き直さずに、任意のタイミングでインターフェイスの言語を変更できます。Kaspersky Security Center Web コンソールを Kaspersky Security Center と合わせてインストールする場合、インストールファイルと同じ言語が Kaspersky Security Center Web コンソールのインターフェイス言語として選択されます。Kaspersky Security Center Web コンソールのみをインストールする場合、オペレーティングシステムと同じ言語がインターフェイス言語として選択されます。Kaspersky Security Center Web コンソールでインストールファイルやオペレーティングシステムの言語がサポートされていない場合、既定では英語が選択されます。

Kaspersky Security Center Web コンソールでは、モバイルデバイス管理はサポートされていません。ただし、MMC ベースの管理コンソールでモバイルデバイスを管理グループに追加した場合、これらのモバイルデバイスも Kaspersky Security Center Web コンソールで表示されます。

Kaspersky Security Center 管理サーバーと Kaspersky Security Center Web コンソールの導入図

Kaspersky Security Center 管理サーバーと Kaspersky Security Center Web コンソールの導入図を示します。



Kaspersky Security Center 管理サーバーと Kaspersky Security Center Web コンソールの導入図

保護対象デバイスにインストールされているカスペルスキー製品の管理プラグイン（1つの製品ごとに1つの管理プラグイン）は、Kaspersky Security Center Web コンソールサーバーがインストールされているサーバーに導入されます。

管理者ユーザーは、自分が使用しているワークステーションのブラウザーを使用して Kaspersky Security Center Web コンソールにアクセスします。

Kaspersky Security Center Web コンソールで個別の操作を実行すると、Kaspersky Security Center Web コンソールサーバーが OpenAPI を通して Kaspersky Security Center 管理サーバーと通信を行います。Kaspersky Security Center Web コンソールサーバーは Kaspersky Security Center 管理サーバーに必要な情報のリクエストを送信し、Kaspersky Security Center Web コンソールでの操作結果を表示します。

Kaspersky Security Center Web コンソールで使用されるポート

下表には、Kaspersky Security Center Web コンソールサーバー（単に「Kaspersky Security Center Web コンソール」とも表記）がインストールされたデバイスで開放しておく必要があるポートが一覧で表示されています。

Kaspersky Security Center Web コンソールで使用されるポート

ポート番号	サービス名	プロトコル	ポートの目的	範囲
2001	Kaspersky Security Center 製品プラグインサーバー	HTTPS	管理プラグインプロセスが「Kaspersky Security Center Web コンソール管理サービス」からのリクエストを受信するために使用する API ポート	管理プラグインの node.exe プロセスの実行
1329、2003	Kaspersky Security Center Web コンソール管理サービス	HTTPS	同一のデバイスで実行中の「Kaspersky Security Center Web コンソール管理サービス」からのリクエストを受信するために使用される API ポート	Kaspersky Security Center Web コンソールコンポーネントのアップデート
2005	Kaspersky Security Center Web コンソール	HTTPS	同一のデバイスで実行中の「Kaspersky Security Center Web コンソール管理サービス」からのリクエストを受信するために使用される API ポート	Kaspersky Security Center Web コンソールの node.exe プロセスの実行
3333	Kaspersky OSMP KAS サービス	HTTPS	OAuth2.0 認証エンドポイントポート	Identity and Access Manager
4004	Kaspersky OSMP Facade サービス	HTTPS	OAuth2.0 認証プロバイダーポート	Identity and Access Manager
4444	Kaspersky OSMP KAS サービス	HTTPS	OAuth2.0 トークンイントロスペクションエンドポイントポート	Identity and Access Manager
8200	—	HTTP	HashiCorp Vault を使用して証明書を生成するために使用される API ポート（詳細については、HashiCorp Vault の Web サイト を参照してください）	Kaspersky Security Center Web コンソールのインストールと Kaspersky Security Center Web コンソールコンポーネントのアップデート
4150、4151、4152	Kaspersky Security Center Web コンソールメッセージキュー	HTTPS	Kaspersky Security Center Web コンソールと管理プラグインの処理間で発生する通信に使用されるメッセージブローカーの API ポート	Kaspersky Security Center Web コンソールと管理プラグインとの対話

下の表では Kaspersky Security Center Web コンソールサーバーがインストールされているデバイスで開いている必要のないポートを一覧で示します。ただし Kaspersky Security Center Web コンソールはこれらのポートを Identity and Access Manager で使用します。

Kaspersky Security Center Web コンソールが Identity and Access Manager 用に使用するポート

ポート番号	サービス名	プロトコル	ポートの目的	範囲
4445	Kaspersky OSMP KAS サービス	HTTPS	OAuth2.0 認証エンドポイントポートの設定を KSC Web コンソールから受け取る主要な Identity and Access Manager のポート（詳細については OAuth の Web サイト を参照してください）。	Identity and Access Manager
2444	Kaspersky OSMP Facade サービス	HTTPS	Identity and Access Manager の設定用ポート	Identity and Access Manager
2445	Kaspersky OSMP Facade サービス	HTTPS	「Kaspersky OSMP KAS サービス」の「Kaspersky OSMP Facade サービス」への接続用ポート	Identity and Access Manager

Kaspersky Security Center Web コンソールインターフェイス

Kaspersky Security Center は、Kaspersky Security Center Web コンソールインターフェイスを通じて管理されます。

Kaspersky Security Center Web コンソールウィンドウには、次の項目が含まれています：

- ウィンドウ左側のメインメニュー
- ウィンドウ右側の作業領域

メインメニュー

メインメニューには次のセクションがあります：

- **管理サーバー**。現在接続している管理サーバーの名前が表示されます。設定アイコン（  ）をクリックして、管理サーバーのプロパティを開きます。
- **監視とレポート**。インフラストラクチャの状況、保護ステータス、統計情報を提供します。
- **資産（デバイス）**。資産、タスク、カスペルスキー製品ポリシーのためのツールが含まれています。
- **ユーザーとロール**。ユーザーとロールを管理し、ユーザーにロールを割り当ててユーザー権限を構成し、ポリシープロファイルをロールに関連付けることができます。
- **操作**。アプリケーションのライセンス管理、暗号化されたドライブと暗号化イベントの表示と管理、サードパーティのアプリケーションの管理など、さまざまな操作が含まれます。これにより、アプリケーションリポジトリへのアクセスも可能になります。
- **検出と製品の導入**。ネットワークをポーリングしてクライアントデバイスを検出し、デバイスを管理グループに手動または自動で配布できます。これには、クイックスタートウィザードと製品導入ウィザードも含まれています。
- **マーケットプレイス**。カスペルスキーの法人向けソリューション全体に関する情報が含まれており、必要なソリューションを選択して、カスペルスキーの Web サイトでそれらのソリューションの購入に進むことができます。
- **設定**。Web プラグインの現在の状態をバックアップして、後から保存した状態を復元できます。インターフェイスの言語またはテーマなど、インターフェイスの表示に関連する個人設定が含まれます。
- **アカウントメニュー**：Kaspersky Security Center ヘルプへのリンクが含まれています。また、Kaspersky Security Center からログアウトし、Kaspersky Security Center Web コンソールのバージョンとインストールされている管理 Web プラグインのリストを表示することもできます。

作業領域

作業領域には、Kaspersky Security Center Web コンソールインターフェイスウィンドウの各セクションで表示を選択した情報が表示されます。また、情報の表示方法の構成に使用できるコントロール要素も含まれています。

メインメニューのセクションのピン留めとピン留め解除

Kaspersky Security Center Web コンソールのセクションをピン留めしてお気に入りに追加し、メインメニューの［**ピン留め**］セクションからすばやくアクセスすることができます。

ピン留めされた要素がない場合、メインメニューに［**ピン留め**］セクションは表示されません。

ページのみを表示するセクションをピン留めできます。たとえば、［**アセット（デバイス）**］→［**管理対象デバイス**］に移動すると、デバイスの表を含むページが開き、［**管理対象デバイス**］セクションをピン留めできるようになります。メインメニューでセクションを選択した後にウィンドウまたは要素が表示されない場合は、そのセクションをピン留めすることはできません。

セクションをピン留めするには：

1. メインメニューで、ピン留めするセクションの上にマウスカーソルを置きます。
   ピン（📌）アイコンが表示されます。
2. ピン（📌）アイコンをクリックします。

セクションはピン留めされ、［**ピン留め**］セクションに表示されます。

ピン留めできる要素の最大数は 5 です。

ピン留めを解除することで、お気に入りから要素を削除することもできます。

セクションのピン留めを解除するには：

1. メインメニューで、［**ピン留め**］セクションに移動します。
2. ピン留めを解除したいセクションにマウスカーソルを合わせ、ピン留め解除（📌）アイコンをクリックします。

このセクションはお気に入りから削除されました。

Kaspersky Security Center Web コンソールのインストールと初期セットアップのシナリオ

このシナリオでは、Kaspersky Security Center 管理サーバーと Kaspersky Security Center Web コンソールをインストールする方法、クイックスタートウィザードを使用して管理サーバーの初期セットアップを行う方法、および製品導入ウィザードを使用して管理対象デバイスにカスペルスキー製品をインストールする方法について説明します。

Kaspersky Security Center Web コンソールのインストールと初期セットアップは、以下の手順で進みます：

1. **DBMS（データベース管理システム）のインストール**

   Kaspersky Security Center 用の DBMS（データベース管理システム）をインストールするか、既存の DBMS を使用します。

   選択した DBMS のインストール方法については、該当製品のマニュアルを参照してください。

2. **管理サーバー、管理コンソール、ネットワークエージェントのインストール**

   管理コンソールとサーバー版のネットワークエージェントが管理サーバーとともにインストールされます。

Kaspersky Security Center 管理サーバーのインストール時に、Kaspersky Security Center Web コンソールを同じデバイス上にインストールするかを指定します。同じデバイス上に両方のコンポーネントをインストールする選択をした場合、Kaspersky Security Center Web コンソールは自動的にインストールされるため、別途インストールする必要はありません。Kaspersky Security Center Web コンソールを別のデバイスにインストールする場合、Kaspersky Security Center 管理サーバーをインストールした後に、別途 Kaspersky Security Center Web コンソールのインストールを行います。

3 Kaspersky Security Center Web コンソールのインストール

Kaspersky Security Center Web コンソールと一緒に Kaspersky Security Center 管理サーバーをインストールしない選択をした場合、別のデバイスに Kaspersky Security Center Web コンソールをインストールします。Kaspersky Security Center Web コンソールは、別のデバイスにインストールすることも、管理サーバーがインストールされているものと同じデバイスにインストールすることもできます。

4 初期セットアップの実行

管理サーバーのインストールが完了すると、管理サーバーへの最初の接続時にクイックスタートウィザードが自動的に開始します。既存要件に従って、管理サーバーの初期設定を行います。初期設定段階中に、ウィザードが既定値設定を使用して、保護の導入に必要なポリシーとタスクを作成します。しかしながら、既定の設定は組織のニーズに対して十分ではない場合があります。必要に応じて、ポリシーやタスクの設定を編集できます。

5 Kaspersky Security Center のライセンス（オプション）

Kaspersky Security Center 管理コンソールの基本機能のみを使用する場合、ライセンスは不要です。製品版ライセンスが必要となるのは追加機能を 1 つ以上使用する場合で、脆弱性とパッチ管理、モバイルデバイス管理、SIEM システムとの連携機能が追加機能に当たります。これらの機能のライセンス情報ファイルやアクティベーションコードは、クイックスタートウィザードの該当するステップで追加するか、あるいは手動で追加できます。

6 ネットワーク上のデバイスの検出

このステップはクイックスタートウィザードの一部として実行できます。後から手動でデバイスを検出することもできます。Kaspersky Security Center は、ネットワークで検出されたすべてのデバイスのアドレスと名前を受信します。その後、Kaspersky Security Center を使用してカスペルスキー製品と他社製ソフトウェアを、検出されたデバイスにインストールできます。Kaspersky Security Center はデバイスの検索を定期的に開始するため、新しいインスタンスがネットワークに現れると、それらのインスタンスは自動的に検出されます。

7 管理グループ内へのデバイスの配置

このステップはクイックスタートウィザードの一部として実行できますが、検出されたデバイスを後から手動でグループに移動することもできます。

8 ネットワーク接続されたデバイスへのネットワークエージェントとセキュリティ製品のインストール

企業ネットワークへの保護の導入時には、デバイス検出中に管理サーバーによって検出されたデバイスにネットワークエージェントとセキュリティ製品（Kaspersky Endpoint Security for Windows など）をインストールする必要があります。

リモートで製品をインストールするには、製品導入ウィザードを実行します。

セキュリティ製品は、脅威をもたらすウイルスなどのプログラムからデバイスを保護します。ネットワークエージェントは、デバイスと管理サーバー間の通信が確実に行われるようにします。ネットワークエージェントは自動的に設定されるようになっています。

ネットワーク接続されたデバイスへのネットワークエージェントとセキュリティ製品のインストールを開始する前に、それらのデバイスがアクセス可能である（電源が入っている）ことを確認してください。

9 ライセンスのクライアントデバイスへの導入

クライアントデバイスにライセンスを導入し、デバイス上の管理対象セキュリティ製品をアクティベートします。

10 Kaspersky Security for Mobile のインストール（省略可能）

企業のモバイルデバイスを管理する場合は、Kaspersky Security for Mobile のヘルプの手順に従って Kaspersky Endpoint Security for Android を導入してください。

⑪ カスペルスキー製品のポリシーの設定

異なるデバイスに異なる設定を適用するには、デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理を使用できます。デバイスベースのセキュリティ管理は、ポリシーとタスクを使用することで実施できます。タスクは特定の条件を満たすデバイスに対してのみ適用できます。デバイスのフィルター処理の条件を設定するには、デバイスの抽出とタグを使用します。

⑫ ネットワーク保護ステータスの監視

ダッシュボードにあるウィジェットを使用したネットワーク監視、カスペルスキー製品からのレポートの生成、管理対象デバイス上のアプリケーションから受信したイベントの抽出の設定と表示、通知リストの表示ができます。

インストール

このセクションでは、Kaspersky Security Center と Kaspersky Security Center Web コンソールのインストールについて説明しています。

Kaspersky Security Center のインストール（標準インストール）

Kaspersky Security Center をインストールする方法について説明します。インストールの前に、あらかじめデータベース管理システムをインストールしておく必要があります。

Kaspersky Security Center をインストールするには：

1. 管理者権限を持つアカウントで、ksc_<ビルド番号>_full_<ローカリゼーション言語>.exe 実行ファイルを実行します。
2. インストールするアプリケーションを選択するウィンドウが表示されるので、［**Kaspersky Security Center 管理サーバーのインストール**］をクリックします。

   Kaspersky Security Center 管理サーバーセットアップウィザードが開始されます。
3. 最初のウィンドウから順に、［**次へ**］をクリックしながらウィザードに従って手順を進めます。
4. Microsoft .NET Framework がインストールされていない場合は、インストールします。
5. 使用許諾契約書とプライバシーポリシーの条項に同意します。
6. インストール方法を選択します。試用評価が目的の場合は、既定の［**標準**］の値をそのまま使用することを推奨します。
7. Kaspersky Security Center Web コンソールを同じデバイスにインストールする場合は、［**Kaspersky Security Center Web コンソールのインストール**］をオンにします。

   チェックボックスをオフにした場合は、後で別途、同じデバイスまたは別のデバイスに Kaspersky Security Center Web コンソールをインストールできます。
8. ネットワークのサイズを選択します。試用評価が目的の場合は、既定の［**ネットワーク上のデバイスが 100 台以下**］の値をそのまま使用することを推奨します。

9. インストール済みの定義データベースサーバーの種別を選択します。

10. インストール済みのデータベースサーバーの接続パラメータを指定します。

11. インストール済みのデータベースサーバーの認証パラメータを指定します。

12. ［**インストール**］をクリックして、インストールを開始します。

13. インストールが正常に完了したら、ウィザードの終了直後に管理コンソールを起動するかどうかを選択します。

    Kaspersky Security Center Web コンソールの開始を選択した場合、ログイン画面が開きます。この後に、クイックスタートウィザードを使用して、管理サーバーの初期設定を行えます。

    Kaspersky Security Center Web コンソールが既にインストールされている場合のみ、Kaspersky Security Center 12 Web コンソールを開くことができます。Kaspersky Security Center のインストール中のインストールも、別途単独でのインストールも実行していない場合、Kaspersky Security Center Web コンソールを開くことはできません。

14. 管理コンソールウィンドウが開いたら、インストール済みの管理サーバーをクリックします。

15. 管理サーバー証明書ウィンドウが開いたら、［**はい**］をクリックして次に進みます。

    Web ベースの管理コンソールで未実行の場合は、管理サーバークイックスタートウィザードが開始されます。

トラブルシューティング

管理サーバー証明書ウィンドウが開かず、接続エラーが表示された場合、次を試してください：

1. Windows の場合、［**サービス**］を開きます（［**コントロールパネル**］→［**管理ツール**］→［**サービス**］）。Kaspersky Security Center ネットワークエージェントおよび Kaspersky Security Center 管理サーバーのサービスが実行中かを確認する。

2. Windows の場合、［**イベントビューアー**］を開き（［**コントロールパネル**］→［**管理ツール**］→［**イベント ビューアー**］）、［**アプリケーションとサービス ログ**］→［**Kaspersky Event Log**］の順に選択します。ログにエラーが含まれておらず、「**管理サーバー <バージョン番号> が実行中です**」という内容のイベントが含まれていることを確認します。

Kaspersky Security Center Web コンソールのインストール

このセクションでは、Kaspersky Security Center Web コンソールサーバー（単に「Kaspersky Security Center Web コンソール」とも表記）を単独でインストールする方法について説明しています。インストールの前に、DBMS と Kaspersky Security Center 管理サーバーをインストールする必要があります。Kaspersky Security Center Web コンソールは、Kaspersky Security Center がインストールされている同じデバイスまたは別のデバイスにインストールできます。

Kaspersky Security Center Web コンソールをインストールするには：

1. 管理者権限を持つアカウントで、実行ファイル ksc-web-console- <バージョン番号>.<ビルド番号>.exe を実行します。

   セットアップウィザードが起動します。

2. セットアップウィザードの言語を選択します。

3. ［ようこそ］ウィンドウで［**次へ**］をクリックします。

4. ［**使用許諾契約書**］ウィンドウで、使用許諾契約書の条項を読んで同意します。EULA に同意するとインストールを進めることができますが、同意しない場合、［**次へ**］が使用できません。

5. ［**インストール先フォルダー**］ウィンドウで Kaspersky Security Center Web コンソールをインストールするフォルダーを選択します（既定では、%ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console にインストールされます）。このフォルダーがない場合は、インストール中に自動的に作成されます。

   インストール先フォルダーは、［**参照**］を使用して変更できます。

6. ［**Kaspersky Security Center Web コンソールの接続設定**］ウィンドウで、次の情報を指定します：

   - Kaspersky Security Center Web コンソールのアドレス（既定では、127.0.0.1）
   - Kaspersky Security Center Web コンソールが受信接続に使用するポート、つまりブラウザーから Kaspersky Security Center Web コンソールへのアクセスを許可するポート（既定では 8080）

   アドレスとポート番号は既定値のままにしておくことを推奨します。

   必要に応じて［**テスト**］をクリックして、選択したポートが使用可能であることを確認します。

   Kaspersky Security Center Web コンソールでの動作のログ記録を有効にする場合は、適切なオプションを選択します。このオプションをオフにすると、Kaspersky Security Center Web コンソールのログファイルは作成されません。

7. ［**アカウントの設定**］ウィンドウで、アカウント名とパスワードを指定します。

   既定のアカウントの使用を推奨します。

8. ［**クライアント証明書**］ウィンドウで、次のいずれかを選択します。

   - **新しい証明書の生成**：このオプションは、ブラウザーの証明書がない場合に推奨されます。
   - **既存の証明書を選択**：このオプションは、ブラウザーの証明書を既に保有しており、パスを指定できる場合に選択できます。
   - 新しい証明書の生成を選択する場合、Kaspersky Security Center Web コンソールを開くと、ブラウザーから Kaspersky Security Center Web コンソールとの接続はプライベートでなく Kaspersky Security Center Web コンソールの証明書が無効であると通知されます。この警告は、Kaspersky Security Center Web コンソールの証明書が自己署名で、Kaspersky Security Center によって自動で生成されたものであるために表示されます。この警告を解除するには、企業のインフラストラクチャで信頼済みで、かつ、カスタム証明書の要件を満たす証明書を作成します。次に、［**クライアント証明書**］ウィンドウで［**既存の証明書を選択**］をオンにしてから、カスタム証明書のパスを指定します。

   > PFX 形式の証明書は、Kaspersky Security Center Web コンソールではサポートされていません。このような証明書を使用するには、まず OpenSSL ベースのクロスプラットフォームユーティリティ（OpenSSL for Windows など）を使用して、サポートされている PEM 形式に変換する必要があります。

9. ［**信頼済みの管理サーバー**］ウィンドウで、使用する管理サーバーがリスト上にあるか確認し、［**次へ**］をクリックしてインストーラーの最後のウィンドウに進みます。

   新しい管理サーバーをリストに追加する必要がある場合は、［**追加**］をクリックします。開いたウィンドウで、信頼できる新しい管理サーバーのプロパティを指定します。

   - **管理サーバー名**

     Kaspersky Security Center Web コンソールのログインウィンドウに表示される管理サーバー名。

- **管理サーバーアドレス**

  管理サーバーをインストールするデバイスの IP アドレス。

- **管理サーバーのポート**

  Kaspersky Security Center Web コンソールが管理サーバーへの接続に使用する OpenAPI ポート（既定値は 13299）。

- **管理サーバー証明書**

  証明書ファイルは、管理サーバーがインストールされているデバイスに保存されます。管理サーバー証明書への既定のパス：

  - Windowsの場合 - %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
  - Linuxの場合 - /var/opt/kaspersky/klnagent_srv/1093/cert/

  管理サーバーがインストールされているデバイスにKaspersky Security Center Web Consoleをインストールする場合は、上記のいずれかのパスを使用します。それ以外の場合は、管理サーバーがインストールされているデバイスから、 Kaspersky Security Center Web Consoleがインストールされているデバイスに証明書ファイルをコピーし、証明書へのローカル パスを指定します。

10. ［**Identity and Access Manager（IAM）**］ウィンドウで Identity and Access Manager（IAM とも表記）をインストールするかどうかを指定します。Identity and Access Manager をインストールする場合は次のポート番号を指定します：

    - **KAS 管理者ポート**：既定では、ポート 4445 を使用して Kaspersky Security Center Web コンソールからの OAuth2.0 認証エンドポイントポートの設定を受け取ります。
    - **Facade 管理者ポート**：既定では、ポート 2444 は Identity and Access Manager の設定に使用されます。
    - **Facade 対話ポート**：既定では、ポート 2445 は Kaspersky OSMP KAS サービスの Kaspersky OSMP Facade サービスへの接続用ポートとして使用されます。

    必要に応じて、既定のポート番号を変更できます。以降 Kaspersky Security Center Web コンソールでは変更することができなくなります。

11. インストーラーの最後のウィンドウで、［**インストール**］をクリックしてインストールを開始します。

インストールが正常に完了したら、デスクトップにショートカットが作成され、Kaspersky Security Center Web コンソールにログインできます。

MMC ベースの管理コンソールで未実行の場合は、管理サーバークイックスタートウィザードが開始されます。

トラブルシューティング

お使いのブラウザーで入力した URL に Kaspersky Security Center Web コンソールが表示されない場合、次のことを試してください：

1. Kaspersky Security Center Web コンソールがインストールされたデバイスのホスト名または IP アドレスが正しく指定されているかを確認します。
2. ブラウザーを開いているデバイスが、Kaspersky Security Center Web コンソールのインストールされたデバイスに対してアクセス権があるかを確認します。

3. Kaspersky Security Center Web コンソールがインストールされたデバイスのファイアウォールの設定で、ポート番号 8080 経由の受信接続およびアプリケーション node.exe への受信接続が許可されているかを確認します。

4. Windows の場合、［**サービス**］を開きます。Kaspersky Security Center Web コンソールのサービスが実行されているか確認します。

5. 管理コンソールを使用して Kaspersky Security Center にアクセスできるかを確認します。

6. Windows の場合、［**イベントビューアー**］を開き、［**アプリケーションとサービス ログ**］→［**Kaspersky Event Log**］の順に選択します。ログにエラーが含まれていないことを確認します。

フェイルオーバークラスターノードにインストールされた管理サーバーに接続された Kaspersky Security Center Web コンソールのインストール

このセクションでは、Kaspersky Security Center または Windows Server のフェールオーバークラスターノードにインストールされた管理サーバーに接続する Kaspersky Security Center Web コンソールサーバー（以降、「Kaspersky Security Center Web コンソール」と表記）をインストールする方法について説明します。Kaspersky Security Center Web コンソールをインストールする前に、DBMS と Kaspersky Security Center 管理サーバーを Kaspersky Security Center のフェールオーバークラスターノードまたは Windows Server のフェールオーバークラスターノードにインストールします。

Windows Server のフェールオーバークラスターを使用する場合、Kaspersky Security Center Web コンソールをフェールオーバークラスターノードにインストールすることは推奨しません。ノードで障害が発生すると、管理サーバーにアクセスできなくなります。

フェイルオーバー クラスター ノードにインストールされた管理サーバーに接続する Kaspersky Security Center Web コンソールをインストールするには：

1. ステップ 1 からステップ 8 まで、Kaspersky Security Center Web コンソールのインストールのステップを実行します。

2. 手順 9 の［**信頼済みの管理サーバー**］ウィンドウで、［**追加**］をクリックして、フェールオーバー クラスターを信頼された管理サーバーとして追加します。

   開いたウィンドウで、次のプロパティを指定します。

   - **管理サーバー名**

     Kaspersky Security Center Web コンソールのログインウィンドウに表示されるクラスター名。

   - **管理サーバーアドレス**

     フェールオーバー クラスターの種類に応じて、クラスターアドレスを指定します。

     - **Kaspersky Security Center のフェールオーバークラスター**。クラスターノードの準備時にセカンダリネットワークアダプタを作成した場合は、仮想ネットワークアダプタの IP アドレスをクラスターアドレスとして指定します。そうでない場合は、使用するサードパーティのロードバランサーの IP アドレスを指定します。

     - **Windows Server のフェールオーバークラスター**。Windows Server のフェールオーバークラスターの作成時に取得したクラスターアドレスを指定します。

   - **管理サーバーのポート**

Kaspersky Security Center Web コンソールが管理サーバーへの接続に使用する OpenAPI ポート（既定値は 13299）。

- **管理サーバー証明書**

  管理サーバーの証明書は、Kaspersky Security Center のフェールオーバークラスターまたは Windows Server のフェールオーバークラスターの共有データストレージにあります。証明書ファイルの既定のパス：<共有データフォルダー>\1093\cert\klserver.cer。証明書ファイルを共有データストレージから Kaspersky Security Center Web コンソールをインストールするデバイスにコピーします。管理サーバーの証明書のローカルパスを指定します。

3. Kaspersky Security Center Web コンソールの標準インストールを続行します。

インストールが完了したら、デスクトップにショートカットが作成され、Kaspersky Security Center Web コンソールにログインできます。

Kaspersky Security Center のフェールオーバークラスターを使用する場合、［**検出と製品の導入**］→［**未割り当てデバイス**］の順に移動して、クラスターノードとファイルサーバーに関する情報を表示できます。

Kaspersky Security Center Web コンソールのアップグレード

Kaspersky Security Center Web コンソールの新バージョンを、現在インストールされているバージョンを削除せずに使用する場合、Kaspersky Security Center Web コンソールインストーラーの標準的なアップグレード手順を使用できます。

Kaspersky Security Center Web コンソールをアップグレードするには：

1. 管理者権限を持つアカウントで、インストールファイル ksc-web-console-<バージョン番号>.<ビルド番号>.exe を実行します。<ビルド番号> は Kaspersky Security Center Web コンソールのビルド番号で、現在インストールされているインスタンスよりも後になっています。

2. 表示されるセットアップウィザードのウィンドウで言語を選択し、［**OK**］をクリックします。

3. 最初のウィンドウで、［**アップグレード**］を選択し、［**次へ**］をクリックします。

4. ［**使用許諾契約書**］ウィンドウで、使用許諾契約書の条項を読んで同意します。EULA に同意するとインストールを進めることができますが、同意しない場合、［**次へ**］が使用できません。

5. インストールが完了するまで、セットアップウィザードの手順を進めます。続行中に、前回のインストール中に指定したKaspersky Security Center Web コンソールの設定を変更することもできます。**Kaspersky Security Center Web コンソールの変更準備完了**ステップに到達したら、［**アップグレード**］をクリックします。新しい設定が適用されるまで待ち、セットアップウィザードの次のステップで、［**終了**］をクリックします。［**Kaspersky Security Center Web コンソールをブラウザーで開始する**］をクリックし、Kaspersky Security Center Web コンソールのアップグレードされたインスタンスをすぐに開始することも可能です。

   アップグレード中の Kaspersky Security Center Web コンソール設定の変更は、Kaspersky Security Center Web コンソールのバージョン 12.2 以降でのみ行うことができます。

Kaspersky Security Center Web コンソールがアップグレードされます。

Kaspersky Security Center Web コンソールを使用するための証明書

このセクションでは、Kaspersky Security Center Web コンソール向けの証明書を発行および置き換える方法と、サーバーが Kaspersky Security Center Web コンソールと対話する場合に管理サーバー向けの証明書を更新する方法について説明します。

Kaspersky Security Center Web コンソールの証明書の再発行

ほとんどの Web ブラウザーは、証明書の有効期間に制限があります。この制限内に収まるように、Kaspersky Security Center Web コンソール証明書の有効期間は 397 日間に制限されています。新しい自己署名証明書を手動で発行することにより、証明機関（CA）から受け取った既存の証明書を置き換えることができます。または、有効期限切れの Kaspersky Security Center Web コンソール証明書を再発行することもできます。

Kaspersky Security Center Web コンソールの証明書の自動再発行はサポートされていません。期限切れの証明書は手動で再発行する必要があります。

自己署名証明書を既に使用している場合は、インストーラーの標準的な手順で Kaspersky Security Center Web コンソール をアップグレードすることにより、証明書を再発行することもできます（［**アップグレード**］）。

Web コンソールを開くと、ブラウザーから Web コンソールとの接続がプライベートでなく Web コンソールの証明書が無効であると通知される場合があります。この警告は、Web コンソールの証明書が自己署名で、Kaspersky Security Center によって自動で生成されているために表示されます。この警告が表示されないようにするには、次の操作のうち 1 つを実行します：

- 再発行する場合はカスタム証明書を指定する（推奨オプション）。企業のインフラストラクチャで信頼済みで、かつ、カスタム証明書の要件を満たす証明書を作成する。
- 証明書を再発行した後で、ブラウザーの信頼済み証明書のリストに Web コンソールの証明書を追加する。カスタム証明書を作成できない場合には、この方法を推奨します。

Kaspersky Security Center Web コンソールの初回インストール時に新しい証明書を発行するには：

1. Kaspersky Security Center Web コンソールのルーチンインストールを実行します。
2. **クライアント証明書**のステップまで進んだら、［**新しい証明書の生成**］を選択し、［**次へ**］をクリックします。
3. インストールが完了するまで、セットアップウィザードの残りのステップを進めます。

   Kaspersky Security Center Web コンソールの新しい証明書が発行されます。有効期間は 397 日です。

有効期限切れの Kaspersky Security Center Web コンソール証明書を再発行するには：

1. 管理者権限を持つアカウントで、 インストールファイル ksc-web-console-<バージョン番号>.<ビルド番号>.exe を実行します。
2. 表示されるセットアップウィザードのウィンドウで言語を選択し、［OK］をクリックします。
3. 最初のウィンドウで、を選択し、［**証明書を再発行する**］を選択し、［**次へ**］をクリックします。
4. 次のステップで、Kaspersky Security Center Web コンソールの再設定が完了するまで待ち、［**終了**］をクリックします。

   Kaspersky Security Center Web コンソールの証明書が再発行されます。有効期間は 397 日です。

Identity and Access Manager を使用している場合は、Identity and Access Manager が使用するポートに対してすべての TLS 証明書を再発行する必要があります。Kaspersky Security Center Web コンソールは証明書の有効期間が終了すると通知を表示します。通知の手順に従ってください。

Kaspersky Security Center Web コンソールの証明書の置き換え

既定では、Kaspersky Security Center Web コンソールサーバーをインストールすると、Web コンソールのブラウザー証明書が自動的に生成されます。必要に応じて、自動的に生成された証明書をカスタム証明書で置き換えることができます。

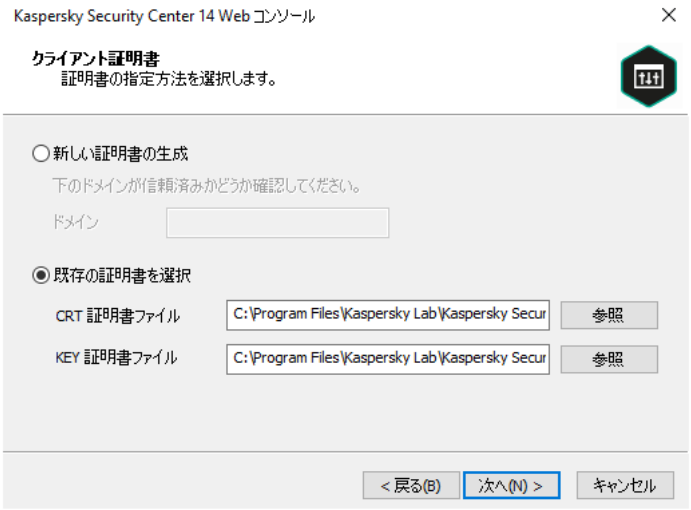
Kaspersky Security Center Web コンソールサーバーの証明書をカスタム証明書で置き換えるには：

1. Kaspersky Security Center Web コンソールサーバーがインストールされているデバイスで、管理者権限が付与されたアカウントを使用し、インストールファイル ksc-web-console-<バージョン番号>.<ビルド番号>.exe を実行します。

   セットアップウィザードが起動します。

2. ウィザードの最初のページで、［**アップグレード**］を選択します。

3. ［**クライアント証明書**］ウィンドウで、［**既存の証明書を選択**］を選択してカスタム証明書のパスを指定します。



クライアントの証明書の指定

4. セットアップウィザードの最終ページで［**変更**］をクリックし、新しい設定を適用します。

5. Web コンソールの再設定が正常に完了したら、［**終了**］をクリックします。

   指定した証明書を使用して Kaspersky Security Center Web コンソールが動作するようになります。

Kaspersky Security Center Web コンソールでの信頼済みの管理サーバーの証明書の指定

管理サーバーの既存の証明書は、証明書の有効期限が切れる前に新しい証明書で自動的に置換されます。管理サーバーの既存の証明書を、カスタム証明書で置換することもできます。証明書を変更するたびに、Kaspersky Security Center Web コンソールの設定で新しい証明書を指定する必要があります。この操作を実行しない場合、Kaspersky Security Center Web コンソールは管理サーバーに接続できなくなります。

管理サーバーの新しい証明書を指定するには：

1. 管理サーバーがインストールされているデバイスで、証明書をコピーし、外部接続のデバイスなどに保存します。

   既定では、証明書ファイルは次のフォルダーに保存されます：

   - Windowsの場合 - %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
   - Linuxの場合 - /var/opt/kaspersky/klnagent_srv/1093/cert/

2. Kaspersky Security Center Web コンソールがインストールされているデバイスで、コピーしておいた証明書ファイルをローカルフォルダーに配置します。

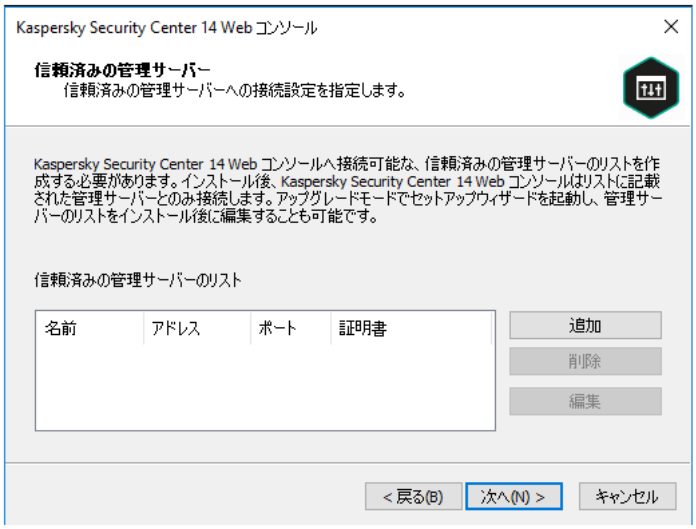
3. 管理者権限が付与されたアカウントで、インストールファイル ksc-web-console-<バージョン番号>.<ビルド番号>.exe を実行します。

   セットアップウィザードが起動します。

4. ウィザードの最初のページで、［**アップグレード**］をオンにします。

   ウィザードの指示に従ってください。

5. ［**信頼済みの管理サーバー**］ページで、必要とする管理サーバーを選択し、［**編集**］をクリックします。



信頼済みの管理サーバーの指定

6. 表示された［**管理サーバーの編集**］ウィンドウで、［**参照**］をクリックし、新しい証明書ファイルへのパスを指定してから、［**アップデート**］をクリックして変更を適用します。

7. ウィザードの［**Kaspersky Security Center Web コンソールの変更準備完了**］ページで、［**アップグレード**］をクリックしてアップグレードを開始します。

8. 製品の再設定が正常に完了したら、［**終了**］をクリックします。

9. Kaspersky Security Center Web コンソールにログインします。

指定した証明書を使用して Kaspersky Security Center Web コンソールが動作するようになります。

PFX 証明書を PEM 形式に変換する

Kaspersky Security Center Web コンソールで PFX 証明書を使用するには、まず、OpenSSL ベースの簡便に使用できる任意のクロスプラットフォームユーティリティを使用して PEM 形式に変換する必要があります。

Windows オペレーティングシステムで PFX 証明書を PEM 形式に変換するには：

1. OpenSSL ベースのクロスプラットフォームユーティリティで、次のコマンドを実行します。

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys -out server.crt
   ```

   ```
   openssl pkcs12 -in <filename.pfx> -nocerts -nodes -out key.pem
   ```

   この結果、.crt ファイルとして公開鍵を、パスフレーズ保護された .pem ファイルとして秘密鍵を取得します。

2. .crt および .pem ファイルが PFX ファイルが格納されているのと同じフォルダーに生成されていることを確認します。

3. .crt または .pem ファイルに「Bag 属性」が含まれている場合は、簡便に使用できる任意のテキスト編集ソフトウェアを使用してこれらの属性を削除し、ファイルを保存します。

4. Windows サービスを再起動します。

5. Kaspersky Security Center Web コンソールはパスフレーズで保護された証明書はサポートしていません。そのため、OpenSSL ベースのクロスプラットフォームユーティリティで次のコマンドを実行して .pem ファイルからパスフレーズを削除します：

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > 入力と出力用の .pem ファイルに同じ名前を使用しないでください。

   結果、.pem ファイルが非暗号化となります。ファイルを使用する際にパスフレーズを入力する必要はありません。

.crt ファイルと .pem ファイルを使用する準備ができたので、Kaspersky Security Center Web コンソールのインストーラーでそれらを指定できるようになります。

Linux オペレーティングシステムで PFX 証明書を PEM 形式に変換するには：

1. OpenSSL ベースのクロスプラットフォームユーティリティで、次のコマンドを実行します。

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <filename.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. 証明書ファイルと秘密鍵が、.pfx ファイルが格納されているのと同じディレクトリに生成されていることを確認してください。

3. Kaspersky Security Center Web コンソールはパスフレーズで保護された証明書はサポートしていません。そのため、OpenSSL ベースのクロスプラットフォームユーティリティで次のコマンドを実行して .pem ファイルからパスフレーズを削除します：

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > 入力と出力用の .pem ファイルに同じ名前を使用しないでください。

結果、.pem ファイルが非暗号化となります。ファイルを使用する際にパスフレーズを入力する必要はありません。

.crt ファイルと .pem ファイルを使用する準備ができたので、Kaspersky Security Center Web コンソールのインストーラーでそれらを指定できるようになります。

Kaspersky Security Center Windows からの移行

このセクションでは、管理対象デバイスと関連オブジェクト（ポリシー、タスク、グループ、タグ、その他のオブジェクト）を Kaspersky Security Center Windows から次の製品に移行する方法について説明します：

- Kaspersky Security Center Cloud コンソール
- Kaspersky Security Center Linux

Kaspersky Security Center Cloud コンソールへの移行について

Kaspersky Security Center Web コンソールから Kaspersky Security Center Cloud コンソールへの移行を実行できます。その後、カスペルスキーのインフラストラクチャでホストされている管理サーバーとデータベース管理システム（DBMS）にアクセスできます。物理サーバーや DBMS は必要ありません。いずれも、カスペルスキーのエキスパートにより維持されています。

Kaspersky Security Center Cloud コンソールの制御下で、Windows、Linux、または macOS オペレーティングシステムを実行している管理対象デバイスを移行できます。ネットワークに管理サーバーの階層が含まれている場合は、Kaspersky Security Center Cloud コンソールに保存できます。さらに、次を転送できます：

- 管理対象アプリケーションのタスクとポリシー
- グローバルタスク
- デバイスのカスタム抽出
- 管理グループの構造と含まれるデバイス
- 移行するデバイスに割り当てられているタグ

移行の完了後、Kaspersky Security Center Cloud コンソールを使用してデバイスを管理できます。同時に、転送されたオブジェクトは保持され、ネットワークエージェントはすべての管理対象デバイスに再インストールされます。

移行の実行方法と前提条件のリストに関する情報は、*Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

Kaspersky Security Center Linux への移行について

このシナリオに従うと、Kaspersky Security Center Linux の管理下で Kaspersky Security Center Windows から、管理対象デバイスとその他のグループオブジェクト（ポリシー、タスク、グローバルタスク、タグ、およびデバイスの抽出）を含む管理グループ構造を転送できます。

制限事項：

- 移行は、Kaspersky Security Center Windows バージョン 14.2 以降から Kaspersky Security Center Linux バージョン 15 以降にのみ可能です。
- このシナリオは、Kaspersky Security Center Web コンソールを使用してのみ実行できます。

始める前に、Kaspersky Security Center Linux の機能と制限事項について確認してください：

- Kaspersky Security Center Windows と Kaspersky Security Center Linux の機能の違い
- Kaspersky Security Center Linux がサポートするカスペルスキー製品のリスト

実行するステップ

移行シナリオは段階的に進行します：

1. **移行方法を選択します**

   Kaspersky Security Center Linux への移行は、移行ウィザードを使用して行います。移行ウィザードの手順は、Kaspersky Security Center Windows および Kaspersky Security Center Linux の管理サーバーが階層に配置されているかどうかによって異なります：

   - 管理サーバーの階層を使用した移行

     Kaspersky Security Center Windows の管理サーバーが Kaspersky Security Center Linux の管理サーバーのセカンダリとして機能する場合は、このオプションをオンにします。移行プロセスの管理とサーバーの切り替えは、Kaspersky Security Center Web コンソールの単一インスタンス内で行います。このオプションを使用する場合は、管理サーバーを階層構造にまとめて、移行手順を簡素化できます。これを行うには、移行を開始する前に階層を作成します。

   - エクスポートファイル（ZIP アーカイブ）を使用した移行

     Kaspersky Security Center Windows と Kaspersky Security Center Linux の管理サーバーが階層化されていない場合は、このオプションをオンにします。移行プロセスの管理には、Kaspersky Security Center Web コンソールの 2 つのインスタンス（Kaspersky Security Center Windows 用のインスタンスと Kaspersky Security Center Linux 用のインスタンス）を使用します。この場合、Kaspersky Security Center Windows からのエクスポート中に作成およびダウンロードしたエクスポートファイル（ZIP アーカイブ）を使用し、このファイルを Kaspersky Security Center Linux にインポートします。

2. **Kaspersky Security Center Windows 管理サーバーの証明書と秘密鍵をバックアップします（オプションの手順）**

   管理サーバーの証明書と秘密鍵をバックアップコピーから復元して、管理対象デバイスを Kaspersky Security Center Linux の管理サーバーの管理下に置くことができます。この場合、Kaspersky Security Center Windows 管理サーバーの証明書と秘密鍵をバックアップします。次に、ステージ 6 で証明書と秘密鍵を復元します。

3. **Kaspersky Security Center Windows からのデータのエクスポート**

   Kaspersky Security Center Windows を開き、移行ウィザードを実行します。

4. **Kaspersky Security Center Linux へのデータのインポート**

   移行ウィザードを続行して、エクスポートされたデータを Kaspersky Security Center Linux にインポートします。サーバーが階層に配置されている場合、同じウィザード内でエクスポートが成功する時、インポートが自動的に開始されます。サーバーが階層に配置されていない場合は、Kaspersky Security Center Linux に切り替えた後、移行ウィザードを続行します。

5. **追加の操作を実行することで、Kaspersky Security Center Windows から Kaspersky Security Center Linux にオブジェクトと設定を手動で転送します（任意のステップ）**

移行ウィザードによる転送できないオブジェクトと設定も転送したい場合があります。たとえば、さらに次のことを実行できます：

- 管理サーバーと管理対象アプリケーションで使用されるライセンスの転送
- 管理サーバーのグローバルタスクの設定
- ネットワークエージェントのポリシー設定のこと
- 製品のインストールパッケージの作成
- 仮想サーバーの作成
- ディストリビューションポイントの割り当てと設定
- デバイス移動ルールの設定
- デバイスの自動タグルールの設定
- アプリケーションカテゴリの作成

6 インポートされた管理対象デバイスを Kaspersky Security Center Linux の管理下に移動する

移行を完了するには、インポートされた管理対象デバイスを Kaspersky Security Center Linux の管理下に移動します。次のいずれかの方法で、これを行うことができます：

- klmover ユーティリティを使用します

  klmover ユーティリティを使用して、新しい管理サーバーの接続設定を指定します。

- *管理サーバーの変更*タスクを通じて

  *管理サーバーの変更*タスクを作成し、インポートされた管理対象デバイス、新しい管理サーバー、およびその他のタスク設定を指定します。次に、管理対象デバイスを Kaspersky Security Center Linux の管理サーバーの管理下に置くタスクを実行します。

- （既にインストールされている場合は）削除し、管理対象デバイスにネットワークエージェントをさらにインストールします。

  新しいネットワークエージェントインストールパッケージを作成し、インストールパッケージのプロパティで新しい管理サーバーの接続設定を指定します。インポートされた管理対象デバイス上のネットワークエージェントを削除し、インストールパッケージを使用して、リモートインストールタスクを通じてインポートされた管理対象デバイスにネットワークエージェントをインストールします。スタンドアロンインストールパッケージを作成および使用して、ネットワークエージェントをローカルにインストールすることもできます。詳細については、管理対象デバイスを Kaspersky Security Center Linux の管理下に切り替えるを参照してください。

- バックアップコピーから管理サーバー証明書と秘密鍵を復元します（Kaspersky Security Center Linux 15.1 またはそれ以降への移行のみ）。

  Kaspersky Security Center Linux の管理サーバーを使用するデバイスには、Kaspersky Security Center Windows の管理サーバーと同じネットワークアドレスを割り当てます。`-cert_only` パラメータを指定して klbackup ユーティリティを実行し、ステージ 2 で保存したバックアップコピーから管理サーバー証明書とプライベートライセンスを復元します。コマンドラインで、次のコマンドを実行します：`/opt/kaspersky/ksc64/sbin/klbackup -path <`管理サーバー証明書のバックアップコピーへのパス`> -restore -cert_only`。詳細については、「klbackup ユーティリティを使用して、別の管理サーバーの管理下にある管理対象デバイスを切り替える」を参照してください。

7 ネットワークエージェントを最新バージョンにアップデートします

Network Agent for Linux を Kaspersky Security Center と同じバージョンにアップグレードすることを推奨します。

8. **管理対象デバイスが新しい管理サーバーに表示されることを確認します**

   Kaspersky Security Center Linux 管理サーバーで、管理対象デバイスのリスト（［**アセット（デバイス）**］→［**管理対象デバイス**］）を開き、［**可視**］、［**ネットワークエージェントがインストール済み**］および［**前回の管理サーバーへの接続**］列の値を確認します。

データ移行のその他の方法

移行ウィザードのほかに、特定のタスクとポリシーを転送することもできます：

- Kaspersky Security Center Windows からのタスクをエクスポートして、Kaspersky Security Center Linux にそのタスクをインポートします。
- Kaspersky Security Center Windows から特定のポリシーをエクスポートして、Kaspersky Security Center Linux にそのポリシーをインポートします。関連するポリシープロファイルは、選択したポリシーとともにエクスポートおよびインポートされます。

Kaspersky XDR Expert への移行について

このシナリオに従うと、Kaspersky XDR Expert の管理下で Kaspersky Security Center Windows から、管理対象デバイスとその他のグループオブジェクト（ポリシー、タスク、グローバルタスク、タグ、およびデバイスの抽出）を含む管理グループ構造を転送できます。

制限事項：

- Kaspersky Security Center 14.2 Windows から Kaspersky XDR Expert バージョン 1.0 への移行のみ可能です。
- このシナリオは、Kaspersky Security Center Web コンソールを使用してのみ実行できます。

実行するステップ

移行シナリオは段階的に進行します：

1. **移行方法を選択します**

   Kaspersky XDR Expert への移行は、移行ウィザードを使用して行います。移行ウィザードの手順は、Kaspersky Security Center Windows および Kaspersky XDR Expert の管理サーバーが階層に配置されているかどうかによって異なります：

   - 管理サーバーの階層を使用した移行

     Kaspersky Security Center Windows の管理サーバーが Kaspersky XDR Expert の管理サーバーのセカンダリとして機能する場合は、このオプションをオンにします。OSMP コンソール内で移行プロセスを管理し、サーバー間を切り替えます。このオプションを使用する場合は、管理サーバーを階層構造にまとめて、移行手順を簡素化できます。これを行うには、移行を開始する前に階層を作成します。

   - エクスポートファイル（ZIP アーカイブ）を使用した移行

     Kaspersky Security Center Windows と Kaspersky XDR Expert の管理サーバーが階層化されていない場合は、このオプションをオンにします。移行プロセスは、Kaspersky Security Center Windows のインスタンスと OSMP コンソールの 2 つのコンソールで管理します。この場合、Kaspersky Security Center Windows からのエクスポート中に作成およびダウンロードしたエクスポートファイル（ZIP アーカイブ）を使用し、このファイルを Kaspersky XDR Expert にインポートします。

2. **Kaspersky Security Center Windows からのデータのエクスポート**

Kaspersky Security Center Windows を開き、移行ウィザードを実行します。

3. **Kaspersky XDR Expert へのデータのインポート**

   移行ウィザードを続行して、エクスポートされたデータを Kaspersky XDR Expert にインポートします。

   サーバーが階層に配置されている場合、同じウィザード内でエクスポートが成功する時、インポートが自動的に開始されます。サーバーが階層に配置されていない場合は、Kaspersky XDR Expert に切り替えた後、移行ウィザードを続行します。

4. **追加の操作を実行することで、Kaspersky Security Center Windows から Kaspersky XDR Expert にオブジェクトと設定を手動で転送します（任意の手順）**

   移行ウィザードによる転送できないオブジェクトと設定も転送したい場合があります。たとえば、さらに次のことを実行できます：

   - 管理サーバーのグローバルタスクの設定
   - ネットワークエージェントのポリシー設定のこと
   - 製品のインストールパッケージの作成
   - 仮想サーバーの作成
   - ディストリビューションポイントの割り当てと設定
   - デバイス移動ルールの設定
   - デバイスの自動タグルールの設定
   - アプリケーションカテゴリの作成

5. **インポートされた管理対象デバイスを Kaspersky XDR Expert の管理下に移動する**

   移行を完了するには、インポートされた管理対象デバイスを Kaspersky XDR Expert の管理下に移動します。次のいずれかの方法で、これを行うことができます：

   - Kaspersky Security Center グループタスクを使用

     管理サーバーの変更タスクを使用して、特定のクライアントデバイスの管理サーバーを別のサーバーに変更します。

   - klmover ユーティリティを使用します

     klmover ユーティリティを使用して、新しい管理サーバーの接続設定を指定します。

   - 管理対象デバイスにネットワークエージェントをインストールまたは再インストールします。

     新しいネットワークエージェントインストールパッケージを作成し、インストールパッケージのプロパティで新しい管理サーバーの接続設定を指定します。インストールパッケージを使用して、リモートインストールタスク経由でインポートされた管理対象デバイスにネットワークエージェントをインストールします。

     スタンドアロンインストールパッケージを作成および使用して、ネットワークエージェントをローカルにインストールすることもできます。

6. **ネットワークエージェントを最新バージョンにアップデートします**

   ネットワークエージェントを OSMP コンソールと同じバージョンにアップグレードすることを推奨します。

7. **管理対象デバイスが新しい管理サーバーに表示されることを確認します**

Kaspersky XDR Expert 管理サーバーで、管理対象デバイスのリスト（［**アセット（デバイス）**］→［**管理対象デバイス**］）を開き、［**可視**］、［**ネットワークエージェントがインストール済み**］および［**前回の管理サーバーへの接続**］列の値を確認します。

データ移行のその他の方法

移行ウィザードのほかに、特定のタスクとポリシーを転送することもできます：

- Kaspersky Security Center Windows からタスクをエクスポートして、Kaspersky XDR Expert にそのタスクをインポートします。
- Kaspersky Security Center Windows からポリシーをエクスポートして、Kaspersky XDR Expert にそのポリシーをインポートします。関連するポリシープロファイルは、選択したポリシーとともにエクスポートおよびインポートされます。

Kaspersky Security Center Windows からのグループオブジェクトのエクスポート

Kaspersky Security Center Windows から Kaspersky Security Center Linux へ管理対象デバイスやその他のグループオブジェクトを含む管理グループ構造を移行するには、最初にエクスポートするデータを選択し、エクスポートファイルを作成する必要があります。エクスポートファイルには、移行するすべてのグループオブジェクトに関する情報が含まれています。このエクスポートファイルは、続けて実行する Kaspersky Security Center Linux へのインポートに使用します。

次のオブジェクトをエクスポートできます：

- 管理対象アプリケーションのタスクとポリシー
- グローバルタスク
- デバイスのカスタム抽出
- 管理グループの構造と含まれるデバイス
- 移行するデバイスに割り当てられているタグ

エクスポートを開始する前に、Kaspersky Security Center Linux への移行に関する一般情報をご確認ください。Kaspersky Security Center Windows および Kaspersky Security Center Linux の管理サーバーの階層を使用するかどうか、移行方法を選択します。

移行ウィザードを使用して管理対象デバイスと関連グループオブジェクトをエクスポートするには：

1. Kaspersky Security Center Windows と Kaspersky Security Center Linux の管理サーバーが階層構造にまとめられているかどうかに応じて、次のいずれかを実行します：
   - サーバーが階層構造にまとめられている場合は、Kaspersky Security Center Web コンソールを開き、Kaspersky Security Center Windows のサーバーに切り替えます。
   - サーバーが階層構造にまとめられていない場合は、Kaspersky Security Center Windows に接続された Kaspersky Security Center Web コンソールを開きます。
2. メインメニューで、［**操作**］→［**移行**］の順に選択します。

3. ウィザードを開始してその手順に従うには、データと設定を転送する場所を選択します。

   - データと設定を Kaspersky Security Center Cloud コンソールに転送する場合は、［**Kaspersky Security Center Cloud コンソールへの移行**］を選択します。

   - データと設定を Kaspersky Security Center Linux または Kaspersky XDR Expert に転送する場合は、［**Kaspersky Security Center Linux または Open Single Management Platform へ移行**］を選択します。

4. エクスポートする管理グループまたはサブグループを選択します。選択した管理グループまたはサブグループに含まれるデバイスが 10,000 台以下であることを確認します。

5. タスクとポリシーをエクスポートする管理対象アプリケーションを選択します。Kaspersky Security Center Linux でサポートされているアプリケーションのみを選択してください。サポートされていないアプリケーションのオブジェクトもエクスポートされますが、操作はできなくなります。

6. 左側のリンクを使用して、エクスポートするグローバルタスク、デバイスの抽出、およびレポートを選択します。［**グループオブジェクト**］を使用すると、カスタムロール、内部ユーザーとセキュリティグループ、およびカスタムアプリケーションカテゴリをエクスポート対象から除外できます。

エクスポートファイル（ZIP アーカイブ）が作成されます。管理サーバーの階層サポートを使用して移行を実行するかどうかに応じて、エクスポートファイルは次のように保存されます：

- サーバーが階層に配置されている場合、エクスポートファイルは Kaspersky Security Center Web コンソールサーバーの一時フォルダーに保存されます。

- サーバーが階層に配置されていない場合、エクスポートファイルはデバイスにダウンロードされます。

管理サーバーの階層サポートのある移行では、エクスポートが正常に完了すると、インポートが自動的に開始されます。管理サーバーの階層サポートなしで移行する場合は、保存したエクスポートファイルを Kaspersky Security Center Linux に手動でインポートできます。

エクスポートファイルを Kaspersky Security Center Linux にインポート

管理対象デバイス、オブジェクト、および Kaspersky Security Center Windows からエクスポートされた設定に関する情報を転送するには、Kaspersky Security Center Linux または Kaspersky XDR Expert にインポートする必要があります。

移行ウィザードを使用して管理対象デバイスと関連グループオブジェクトをインポートするには：

1. Kaspersky Security Center Windows と Kaspersky Security Center Linux の管理サーバーが階層構造にまとめられているかどうかに応じて、次のいずれかを実行します：

   - サーバーが階層に配置されている場合は、エクスポートの完了後に移行ウィザードの次のステップに進みます。このウィザード内でエクスポートが成功すると、インポートが自動的に開始されます（この手順のステップ 2 を参照）。

   - サーバーが階層に配置されていない場合：

     a. Kaspersky Security Center Linux または Kaspersky XDR Expert に接続されている Kaspersky Security Center Web コンソールを開きます。

     b. メインメニューで、［**操作**］→［**移行**］の順に選択します。

c. Kaspersky Security Center Windows からのエクスポート中に作成およびダウンロードしたエクスポートファイル（ZIP アーカイブ）を選択します。エクスポートファイルのアップロードが開始されます。

2. エクスポートファイルが正常にアップロードされたら、インポートを続行できます。別のエクスポートファイルを指定する場合は、［**変更**］リンクをクリックし、必要なファイルを選択します。

3. Kaspersky Security Center Linux の管理グループの階層全体が表示されます。

   エクスポートされた管理グループのオブジェクト（管理対象デバイス、ポリシー、タスク、およびその他のグループオブジェクト）を復元する必要があるターゲット管理グループの横にあるチェックボックスをオンにします。

4. グループオブジェクトのインポートが開始されます。移行ウィザードを最小化して、インポート中に他の操作を同時に実行することはできません。オブジェクトのリスト内のすべてのアイテムの横にある更新アイコン（）が緑色のチェックマーク（）に変わり、インポートが完了するまで待ちます。

5. インポートが完了すると、エクスポートされた管理グループの構造（デバイスの詳細を含む）が、選択したターゲットの管理グループの下に表示されます。復元するオブジェクトの名前が既存のオブジェクトの名前と同じである場合、復元されたオブジェクトには増分サフィックスが追加されます。

> 移行されたタスクで、タスクを実行するアカウントの詳細が指定されている場合は、インポートの完了後にタスクを開いてパスワードを再度入力する必要があります。

インポートがエラーで完了した場合は、次のいずれかを実行できます：

- 管理サーバー階層サポートを使用した移行の場合は、エクスポートファイルのインポートを再度開始できます。
- 管理サーバー階層サポートを使用しない移行の場合は、移行ウィザードを開始して別のエクスポートファイルを選択し、それを再度インポートします。

エクスポート範囲に含まれるグループオブジェクトが Kaspersky Security Center Linux に正常にインポートされたかどうかを確認できます。これを行うには、［**アセット（デバイス）**］セクションに移動し、インポートされたオブジェクトが対応するサブセクションに表示されるかどうかを確認します。

インポートされた管理対象デバイスは［**管理対象デバイス**］サブセクションに表示されますが、ネットワーク内では表示されず、ネットワークエージェントがインストールされて実行されていないことに注意してください（［**可視**］、［**ネットワークエージェントがインストール済み**］、および［**ネットワークエージェントが実行中**］列の値が *NO*）。

移行を完了するには、管理対象デバイスを Kaspersky Security Center Linux の管理下に切り替える必要があります。

管理対象デバイスを Kaspersky Security Center Linux の管理下に切り替える

管理対象デバイス、オブジェクト、およびそれらの設定に関する情報が Kaspersky Security Center Linux に正常にインポートされたら、移行を完了するには、管理対象デバイスを Kaspersky Security Center Linux の管理下に切り替える必要があります。

次のいずれかの方法で、管理対象デバイスを Kaspersky Security Center Linux に移動できます：

- klmover ユーティリティを使用します。

- *管理サーバーの変更*タスクを使用します。
- バックアップコピーから管理サーバーの証明書と秘密鍵を復元します（Kaspersky Security Center Linux 15.1 またはそれ以降への移行のみ）。

  詳細については、メイン移行シナリオのステージ 6 を参照してください。
- リモートインストールタスクを通じて管理対象デバイスにネットワークエージェントをインストールします。

ネットワークエージェントをインストールして、管理対象デバイスを Kaspersky Security Center Linux の管理下に切り替えるには：

1. Kaspersky Security Center Linux の管理下に切り替えるインポートされた管理対象デバイス上のネットワークエージェントを削除します。
2. Kaspersky Security Center Windows の管理サーバーに切り替えます。
3. ［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動し、ネットワークエージェントの既存のインストールパッケージのプロパティを開きます。

   ネットワークエージェントのインストールパッケージがパッケージリストにない場合は、新しいパッケージをダウンロードします。

   スタンドアロンインストールパッケージを作成および使用して、ネットワークエージェントをローカルにインストールすることもできます。
4. ［**設定**］タブで［**接続**］セクションを選択します。Kaspersky Security Center Linux の管理サーバーの接続設定を指定します。
5. インポートされた管理対象デバイスのリモートインストールタスクを作成し、再構成されたネットワークエージェントインストールパッケージを指定します。

   ネットワークエージェントは、Kaspersky Security Center Windows の管理サーバーを通じて、またはディストリビューションポイントとして機能する Windows ベースのデバイスを通じてインストールできます。管理サーバーを使用する場合は、［**管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**］をオンにします。ディストリビューションポイントを使用する場合は、［**ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**］をオンにします。
6. リモートインストールタスクを実行します。

リモートインストールタスクが正常に完了したら、Kaspersky Security Center Linux の管理サーバーに移動し、管理対象デバイスがネットワーク内に表示されていること、およびネットワークエージェントがインストールされて実行されていることを確認します（［**可視**］、［**ネットワークエージェントがインストール済み**］、［**ネットワークエージェントが実行中**］列の値が *Yes*）。

Kaspersky Security Center Web コンソールへのサインインとサインアウト

管理サーバーと Web コンソールサーバーのインストールが完了すると、Kaspersky Security Center Web コンソールにサインインできます。インストール中に指定した管理サーバーのアドレスとポート番号の情報が必要になります（既定のポート番号は 8080 です）。ブラウザーでは、JavaScript が有効になっている必要があります。

次の方法を使用して、 Kaspersky Security Center Web コンソールにサインインできます：

- ドメイン認証を使用する

この方法を選択する場合は、ドメインコントローラーポーリングが有効になっていて、ドメインユーザーが管理サーバーに追加されていることを確認してください。

- 管理者のユーザー名とパスワードを指定する

ドメイン認証を使用したサインイン

ドメイン認証を使用して Kaspersky Security Center Web コンソールにサインインするには：

1. ブラウザーで、「<管理サーバーの Web アドレス>:<ポート番号>」にアクセスします。
   サインインページが表示されます。
2. 複数台の信頼する管理サーバーを追加している場合、管理サーバーのリストから接続する管理サーバーを選択します。
   管理サーバーを 1 つだけ追加した場合、管理サーバーのリストは表示されません。
3. 次のいずれかの手順を実行します：
   - ［**ドメイン認証を使用する**］ボタンをクリックします。
   - サーバー上に 1 つ以上の仮想管理サーバーが作成されており、ドメイン認証を使用して仮想サーバーにサインインしたい場合：
     a. ［**仮想サーバーのオプションを表示する**］をクリックします。
     b. 仮想サーバーの作成時に指定した仮想管理サーバー名を入力します。
     c. ［**ドメイン認証を使用する**］ボタンをクリックします。
4. アカウントで二段階認証が有効になっている場合は、モバイルデバイスの認証アプリによって生成されたセキュリティコードを指定します。
   必要に応じて、サインインページに戻ることができます。

サインイン後、ダッシュボードが表示されます。言語設定とテーマは、前回使用したものが使用されます。Kaspersky Security Center Web コンソールを操作して、Kaspersky Security Center による処理を実行できます。

管理者のユーザー名とパスワードを指定してサインインする

管理者のユーザー名とパスワードを指定して Kaspersky Security Center Web コンソールにサインインするには：

1. ブラウザーで、「<管理サーバーの Web アドレス>:<ポート番号>」にアクセスします。
   サインインページが表示されます。
2. 複数台の信頼する管理サーバーを追加している場合、管理サーバーのリストから接続する管理サーバーを選択します。
   管理サーバーを 1 つだけ追加した場合、管理サーバーのリストは表示されません。
3. 次のいずれかの手順を実行します：

- 管理サーバーにサインインするには：

  a. ローカル管理者のユーザー名とパスワードを入力します。

  b. ［**サインイン**］をクリックします。

- サーバー上に1つ以上の仮想管理サーバーが作成されており、仮想サーバーにサインインしたい場合：

  a. ［**仮想サーバーのオプションを表示する**］をクリックします。

  b. 仮想サーバーの作成時に指定した仮想管理サーバー名を入力します。

  c. 仮想管理サーバーの権限を持つ管理者のユーザー名とパスワードを入力します。

  d. ［**サインイン**］をクリックします。

4. アカウントで二段階認証が有効になっている場合は、モバイルデバイスの認証アプリによって生成されたセキュリティコードを指定します。

   必要に応じて、サインインページに戻ることができます。

5. アカウントで強制パスワード変更が有効になっている場合、またはパスワードの有効期限が切れている場合は、パスワード変更ウィンドウが表示されます。Kaspersky Security Center Web コンソールにサインインするための新しいパスワードを設定します。

サインイン後、ダッシュボードが表示されます。言語設定とテーマは、前回使用したものが使用されます。Kaspersky Security Center Web コンソールを操作して、Kaspersky Security Center による処理を実行できます。

サインアウト

Kaspersky Security Center Web コンソールからサインアウトするには：

メインメニューで、アカウント設定に移動して、［**ログアウト**］を選択します。

Kaspersky Security Center Web コンソールが終了し、サインインページが表示されます。

Kaspersky Security Center Web コンソールの Identity and Access Manager

このセクションでは、Identity and Access Manager（IAM とも表記）について説明します。

Identity and Access Manager について

Identity and Access Manager（IAM とも表記）は、Kaspersky Security Center Web コンソールと Kaspersky Industrial CyberSecurity for Networks Web インターフェイス間でシングルサインオン（SSO）を使用できるようにする Kaspersky Security Center Web コンソールのコンポーネントです。IAM は Kaspersky Security Center Web コンソール での Kaspersky Industrial CyberSecurity for Networks の認証に OAuth 2.0 プロトコルを使用します。

この場合、Kaspersky Security Center Web コンソールを経由してアクセスを取得した Kaspersky Industrial CyberSecurity for Networks は *リソースサーバー*になり、Kaspersky Security Center Web コンソールおよび Kaspersky Industrial CyberSecurity for Networks Web インターフェイスは *OAuth 2.0 クライアント*になります。リソースサーバーは複数のユーザーと動作し、認証を必要とするプログラムです。クライアントはリソースサーバーの認証に *トークン*を使用します。トークンは一意なバイト列です。トークンの有効期間が終了すると、自動的に再発行されます。IAM は複数の OAuth 2.0 クライアントに対する単一の認証サーバーとして動作します。

IAM は Kaspersky Security Center Web コンソールのインストール中にインストールできます。Kaspersky Security Center Web コンソールの設定からいつでも有効にできます。Kaspersky Industrial CyberSecurity サーバーまたは Kaspersky Industrial CyberSecurity Web インターフェイスが同一の管理サーバーによって管理されるデバイス上にインストールされている場合、IAM はこのプログラムを検知して Kaspersky Security Center Web コンソール上に通知が表示されます。Kaspersky Industrial CyberSecurity for Networks を登録して、後から Kaspersky Security Center Web コンソールおよび Kaspersky Industrial CyberSecurity for Networks Web インターフェイスの両方に対して SSO を使用することができます。

Kaspersky Security Center Web コンソールからログアウトすると、Kaspersky Industrial CyberSecurity for Networks Web インターフェイスのセッションは終了し、Kaspersky Security Center Web コンソールに再度ログインする必要があります。

Identity and Access Manager を有効にする：シナリオ

必須条件

開始する前に、Kaspersky Industrial CyberSecurity for Networks のバージョン 3.1 以降にアクセスできることを確認してください。

実行するステップ

Identity and Access Manager（IAM とも表記）を有効にするには、次の手順で進めます：

1. **必要なポートの確認**

   Kaspersky Security Center Web コンソールがインストールされているデバイスのポート 3333、4004 および 4444 が開いていることを確認してください。これらのポートは OAuth 2.0 を使用するために必要です。必要であれば既定のポート番号を Kaspersky Security Center Web コンソールの設定ウィンドウで変更することができます。

   ポート 3333、4004 および 4444 のほかに、Kaspersky Security Center Web コンソールは様々な目的でポート 4445、2444 および 2445 も使用します。

2. **Identity and Access Manager のインストール**

   Kaspersky Security Center Web コンソールのインストール中に、Identity and Access Manager をインストールするよう指定します。そうしなかった場合は、Kaspersky Security Center Web コンソールのセットアップウィザードを再度実行してください。

3. **Identity and Access Manager の設定**

   Kaspersky Security Center Web コンソールの設定ウィンドウで、［**Identity and Access Manager（IAM）**］がオンになっていることを確認してください。また、Kaspersky Security Center Web コンソールがインストールされているデバイスの DNS 名を指定してください。クライアントアプリケーションがこのデバイスに接続します。

4. **トークンの設定の指定**

Kaspersky Security Center Web コンソールの設定ウィンドウで、Identity and Access Manager が使用するトークンの有効期間と認証タイムアウトを指定してください。既定値を使用することもできますが、必要に応じて特定の値を指定することも可能です。

5. **証明書の交付**

   管理サーバーにより生成された証明書を使用する場合は、Kaspersky Security Center Web コンソールの設定ウィンドウで IAM によって使用されるポート向けのルート証明書をダウンロードして Kaspersky Security Center Web コンソールのユーザーのワークステーションに配信してください。そうしないと、Kaspersky Security Center Web コンソールに接続しようとする際にユーザーのブラウザーにはエラーメッセージが表示されます。

6. **Kaspersky Industrial CyberSecurity for Networks サーバーおよび Kaspersky Industrial CyberSecurity for Networks Web インターフェイスの登録**

   IAM がインストールされると、Kaspersky Security Center Web コンソールには Industrial CyberSecurity for Networks サーバーおよび 1 つ以上の Kaspersky Industrial CyberSecurity for Networks Web インターフェイスの登録を促すメッセージが表示されます。このメッセージをクリックして Kaspersky Industrial CyberSecurity for Networks サーバー（または複数のサーバー）および Web インターフェイス（または複数の Web インターフェイス）を登録してください。

結果

このシナリオの完了後、Kaspersky Industrial CyberSecurity for Networks および Kaspersky Security Center Web コンソールで SSO および IAM を使用できるようになります。

Kaspersky Security Center Web コンソールでの Identity and Access Manager の設定

必要に応じて Identity and Access Manager を設定するには：

1. メインメニューで、［**設定**］→［**Identity and Access Manager**］に移動します。
2. ［**Identity and Access Manager**］で、Identity and Access Manager が有効になっていることを確認します。
3. ［**Identity and Access Manager デバイスのネットワーク名**］内で［**設定**］をクリックします。
4. Identity and Access Manager をインストールしたデバイスの DNS 名を指定します。クライアントアプリケーションはこのデバイスに接続します。
5. 必要に応じて、関連する設定のグループの下にある［**設定**］をクリックして既定のトークン設定、証明書の設定、ポート番号を変更します。

Identity and Access Manager が有効になり、用途に応じて動作します。

Kaspersky Industrial CyberSecurity for Networks アプリケーションの Kaspersky Security Center Web コンソールでの登録

Kaspersky Security Center Web コンソールを使用して Kaspersky Industrial CyberSecurity for Networks アプリケーションの操作を開始するには、まず Kaspersky Security Center Web コンソールに登録する必要があります。

Kaspersky Industrial CyberSecurity for Networks アプリケーションを登録するには：

1. 次が完了していることを確認してください：

   - Kaspersky Industrial CyberSecurity for Networks Web プラグインのダウンロードとインストール。

     Kaspersky Industrial CyberSecurity for Networks サーバーと管理サーバーの同期の待機中、後で実行することも可能です。

   - シングルサインオン（SSO）テクノロジの使用準備シナリオ。

   - Kaspersky Industrial CyberSecurity for Networks Web インターフェースで必要な設定は、Kaspersky Security Center のページで指定されています。詳細は、Kaspersky Industrial CyberSecurity for Networks のオンラインヘルプを参照してください。

   - Kaspersky Security Center Web コンソールへの管理者アカウントでのログイン。

   - IAM の 設定。

2. Kaspersky Industrial CyberSecurity for Networks サーバーがインストールされているデバイスを、未割り当てのデバイスグループから管理対象デバイスグループに移動します。

   a. メインメニューで、［**検出と製品の導入**］→［**未割り当てデバイス**］の順に選択します。

   b. Kaspersky Industrial CyberSecurity for Networks サーバーがインストールされているデバイスに隣接するチェックボックスをオンにします。

   c. ［**グループへ移動**］をクリックします。

   d. 管理グループの階層で、管理対象デバイスグループに隣接するチェックボックスをオンにします。

   e. ［**移動**］をクリックします。

3. Kaspersky Industrial CyberSecurity for Networks サーバーがインストールされているデバイスのプロパティに進みます。

4. デバイスのプロパティページの［**全般**］セクションで［**管理サーバーから切断しない**］をオンにし、［**保存**］をクリックします。

5. デバイスのプロパティページで、［**アプリケーション**］セクションを選択します。

6. ［**アプリケーション**］セクションで、ネットワークエージェントを選択します。

7. 本製品の現在のステータスが「*停止中*」の場合、「*実行中*」に変更されるまで待機します。

   このプロセスには最大 15 分かかります。Kaspersky Industrial CyberSecurity for Networks Web プラグインをまだインストールしていない場合は、待機中にインストール可能です。

8. メインメニューで、［**設定**］→［**Identity and Access Manager**］に移動します。

   ［**登録リクエスト**］フィールドに、保留中のリクエストが 1 件表示されます。

9. ［**登録リクエスト**］フィールドの下の［**設定**］をクリックします。

10. 登録済みクライアントのリストが開いたら、ステータスが「*保留中*」である Kaspersky Industrial CyberSecurity for Networks サーバーの名前に隣接するチェックボックスをオンにし、［**承認**］をクリックします。

Kaspersky Industrial CyberSecurity for Networks サーバーを登録しない場合は、［承認却下］をクリックして、後でこのリストに戻ることができます。

［**承認**］のクリック後、ステータスが「*承認*」、「*準備完了*」へ遷移します。ステータスが変更されない場合は、［更新］をクリックします。

11. 登録済みクライアントのリストを閉じ、［**登録済みクライアント**］フィールドの値が増えていることを確認します。

12. ダッシュボードに Kaspersky Industrial CyberSecurity for Networks ウィジェットを追加するには：

    a. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］の順に移動します。

    b. ダッシュボードで、［**Web ウィジェットを追加または復元**］をクリックします。

    c. 開いたウィジェットメニューで、［**その他**］を選択します。

    d. Kaspersky Industrial CyberSecurity for Networks ウィジェットを選択します。

    ウィジェットのリンクを使用して、Kaspersky Industrial CyberSecurity for Networks Web インターフェイスに移動できるようになりました。

登録手順の完了後、新しいボタン［**Kaspersky Security Center**］が、Kaspersky Industrial CyberSecurity for Networks Web インターフェイスのログインページに表示されます。このボタンをクリックすると、Kaspersky Security Center の認証情報を使用して Kaspersky Industrial CyberSecurity for Networks Web インターフェイスへログインできます。

Identity and Access Manager のトークンの有効期間と認証タイムアウト

Identity and Access Manager（IAM とも表記）を設定する際、トークンの有効期間と認証タイムアウトを設定する必要があります。既定の設定はセキュリティ標準とサーバーの負荷を反映するよう設計されています。組織のポリシーに従ってこれらの設定を変更することができます。

IAM は有効期間が終了しそうになると、自動的にトークンを再発行します。

以下の表に既定のトークンの有効期間の設定を示します。

トークンの有効期間の設定

トークン	既定の有効期間（秒）	説明
ID トークン（id_token）	86400	認証トークンは OAuth 2.0 クライアント（Kaspersky Security Center Web コンソールまたは Kaspersky Industrial CyberSecurity コンソール）によって使用されます。IAM はユーザーに関する情報（ユーザープロファイル）を含む ID トークンをクライアントに送信します。
アクセストークン（access_token）	86400	IAM で識別されるリソースの所有者の代わりにリソースサーバーにアクセスするために OAuth 2.0 クライアントにより使用されるアクセストークンです。
リフレッシュトークン（refresh_token）	172800	ID トークンおよびアクセストークンの再発行に OAuth 2.0 クライアントが個のトークンを使用します。

以下の表に auth_code および login_consent_request のタイムアウトを示します。

認証タイムアウトの設定

設定	既定のタイムアウト（秒）	説明
認証コード（auth_code）	3600	トークンのコード交換のタイムアウトです。OAuth 2.0 クライアントはこのコードを

		リソースサーバーに送信し、代わりにアクセストークンを取得します。
ログイン同意リクエストのタイムアウト（login_consent_request）	3600	ユーザー権限を OAuth 2.0 クライアントに委任するタイムアウトです。

トークンの詳細は、OAuth の Web サイトを参照してください。

マウスまたはキーボードのアクティビティが検知されないクライアントのタイムアウトを構成するには：

1. Kaspersky Security Center Web コンソールのインストールフォルダーで、config.json ファイルを見つけて開きます。このファイルには、アイドル状態のクライアントのタイムアウトを構成するためのパラメータが含まれています。
2. `clientIdleTimeout` パラメータを使用して、非アクティブなクライアントが警告ポップアップを表示するまでの時間をミリ秒単位で指定します。
3. `clientLogoutTimeout` パラメータを使用して、非アクティブなクライアントの IAM 認証が終了するまでの時間をミリ秒単位で指定します。`clientLogoutTimeout` は `clientIdleTimeout` の後に順次カウントダウンします。

IAM 証明書のダウンロードと配信

既定では、Identity and Access Manager（IAM）は管理サーバーが生成した証明書を使用してブラウザーに Kaspersky Security Center Web コンソールへのアクセス権を付与します。必要に応じてカスタム証明書を使用することができます。どの証明書を使用する場合でも、Kaspersky Security Center Web コンソールのユーザーが Kaspersky Security Center Web コンソールにアクセスするすべてのワークステーションがこの証明書を信頼済みであることを確認してください。

証明書をダウンロードおよび配信するには：

1. メインメニューで、［**設定**］→［**Identity and Access Manager**］に移動します。
2. 各証明書について、関連する設定のグループの下にある［**設定**］をクリックして次のいずれかを実行します：
   - Kaspersky Security Center Web コンソールのインストール中に管理サーバーが生成する証明書を使用する場合：
     1. 表示された証明書のプロパティウィンドウで［**管理サーバーが生成した TLS 証明書**］を選択します。
     2. ［**ダウンロード**］をクリックして証明書をダウンロードします。
     3. Kaspersky Security Center Web コンソールのユーザーが Kaspersky Security Center Web コンソールにアクセスするすべてのワークステーションにダウンロードした証明書を配信します。
   - 使用する証明書がある場合：
     1. 評された証明書のプロパティウィンドウで［**カスタム TLS 証明書**］を選択します。
     2. 証明書ファイルおよび秘密鍵を選択します。
     3. ［**OK**］をクリックします。

4. Kaspersky Security Center Web コンソールまたは Kaspersky Industrial CyberSecurity コンソールにアクセスするすべてのワークステーションに証明書を配信します。

証明書により Kaspersky Security Center Web コンソールおよび Kaspersky Industrial CyberSecurity コンソールにアクセスする権限がユーザーに付与されます。

すべての証明書は、適時に再発行する必要があります。管理サーバーによって生成された証明書は手動で再発行される必要があります。Kaspersky Security Center Web コンソールのインストーラーによって生成された証明書は、インストーラーを使用して再生成される必要があります。

Identity and Access Manager を無効にする

必要に応じて、Identity and Access Manager（IAM とも表記）を無効にできます。

IAM を無効にするには：

1. メインメニューで、［**設定**］→［**連携**］の順にクリックします。
2. **[Identity and Access Manager]** セクションで、［**Identity and Access Manager**］スイッチを無効に切り替えます。

後からいつでも IAM を有効にすることができます。

インストーラーで Kaspersky Security Center Web コンソールをアップデートし、IAM をインストールしない選択をした場合、Kaspersky Security Center Web Console はアップグレードされますが IAM はインストールされません。Kaspersky Industrial CyberSecurity との連携に関するすべての情報、IAM 設定ファイルやログファイルはコンピューターから削除されます。

NTLM および Kerberos プロトコルを使用してドメインの認証を設定する

Kaspersky Security Center 15.1 を使用して、NTLM および Kerberos プロトコルを使用した OpenAPI でのドメイン認証を使用できます。ドメイン認証を使用することで、Windows のユーザーは企業のネットワークのパスワードを再入力することなく Kaspersky Security Center Web コンソールでセキュアな認証を有効にできます（シングルサインオン）。

Kerberos プロトコルを使用した OpenAPI でのドメイン認証には次の制限があります：

- Kaspersky Security Center Web コンソールのユーザーは Kerberos プロトコルを使用して Active Directory で認証されている必要がある。ユーザーは有効な Kerberos Ticket Granting Ticket (TGT とも表記) を持っている必要がある。TGT はドメイン認証時に自動で発行されます。
- ケルベロス認証はブラウザーで設定する必要があります。詳細については、使用しているブラウザーのマニュアルを参照してください。

Kerberos プロトコルを使用したドメイン認証を使用する場合は、ネットワークが次の条件を満たしている必要があります：

- 管理サーバーがドメインアカウント名で実行されている。

- Kaspersky Security Center Web コンソールサーバーが、管理サーバーがインストールされているのと同じデバイスにインストールされている。
- 管理サーバーアカウントに次のサービスプリンシパル名（SPN）が指定されている：
  - "https/<server.fqnd.name>"
  - "https/<server>"

  <server> には管理サーバーデバイスのネットワーク名、<server.fqnd.name> には管理サーバーデバイスの FQDN 名が入ります。
- 管理コンソールまたは Kaspersky Security Center Web コンソールに接続する際に、管理サーバーアドレスとして Service Principal Name (SPN) が登録されたアドレスと完全に同じものを指定する。<server.fqnd.name> または <server> のどちらも指定できます。
- パスワード不要のログインでは、Kaspersky Security Center Web コンソールが開かれるブラウザープロセスはドメインアカウントの下で実行されている必要があります。

Kerberos および NTLM プロトコルは Kaspersky Security Center 15.1 の OpenAPI でのみサポートされています。Kaspersky Security Center Linux の OpenAPI ではサポートされません。

管理サーバーの設定

このセクションでは、Kaspersky Security Center 管理サーバーの設定手順とプロパティについて説明しています。

Kaspersky Security Center Web コンソールから管理サーバーへの接続の設定

管理サーバーへの接続ポートを設定するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**接続ポート**］セクションを選択します。

   選択したサーバーのメインの接続設定が表示されます。

Kaspersky Security Center Web コンソールは、SSL ポート TCP 13299 を介して管理サーバーに接続されます。同じポートを klakaut 自動化オブジェクトも使用できます。

ポート TCP 14000 は、Kaspersky Security Center Web コンソール、ディストリビューションポイント、セカンダリ管理サーバー、klakaut 自動化オブジェクトへの接続とクライアントデバイスからのデータの受信に使用されます。

通常、SSL ポート TCP 13000 は、DMZ 内にあるネットワークエージェント、セカンダリ管理サーバー、プライマリ管理サーバーのみが使用できます。次の場合は、Kaspersky Security Center Web コンソールを SSL ポート 13000 で接続する必要があります：

- Kaspersky Security Center Web コンソールと他の動作（クライアントデバイスからのデータの取得、ディストリビューションポイントへの接続、セカンダリ管理サーバーへの接続）の両方で1つの SSL ポートを使用する可能性がある場合

- klakaut 自動化オブジェクトが管理サーバーに直接ではなく DMZ 内のディストリビューションポイントを介して接続される場合

管理サーバーの接続イベントのログ記録の構成

動作中の管理サーバーへの接続と接続試行の履歴がログファイルに保存されます。ログファイル内の情報により、ネットワークインフラストラクチャ内の接続だけでなく、サーバーに対する不正アクセスの試行についても追跡できます。

管理サーバーへの接続イベントのログを記録するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**接続ポート**］セクションを選択します。
3. ［**管理サーバーへの接続イベントを記録する**］をオンにします。

管理サーバーの受信接続イベント、認証の結果、SSL エラーが「%ProgramData%\KasperskyLab\adminkit\logs\sc.syslog」ファイルに記録されます。

管理サーバーのインターネットアクセスを設定します

Kaspersky Security Network を使用し、Kaspersky Security Center 向けおよび管理対象カスペルスキー製品向けの定義データベースのアップデートをダウンロードするには、インターネットアクセスを設定する必要があります。

管理サーバーのインターネットアクセスを指定するには：

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**インターネットアクセスの設定**］セクションを選択します。
3. インターネットへの接続時にプロキシサーバーを使用する場合は、［**プロキシサーバーを使用する**］をオンにします。このオプションをオンにすると、設定を入力するフィールドが使用可能になります。プロキシサーバーの接続を次のように設定します：

   - **アドレス**

     インターネットへの Kaspersky Security Center の接続に使用するプロキシサーバーのアドレス。

   - **ポート番号**

Kaspersky Security Center でプロキシサーバーへの接続を確立するポートの番号。

- **ローカルアドレスにプロキシサーバーを使用しない**

  ローカルネットワークのデバイスへの接続にプロキシサーバーを使用しません。

- **プロキシサーバー認証**

  このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。
  ［**プロキシサーバーを使用する**］をオンにすると、この入力フィールドが使用可能になります。

- **ユーザー名**

  プロキシサーバーへの接続の確立に使用されるユーザーアカウント（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

- **パスワード**

  プロキシサーバーへの接続の確立に使用されるアカウントのユーザーが設定したパスワード（［**プロキシサーバー認証**］をオンにした場合に有効になります）。
  入力したパスワードを表示するには、確認する間だけ［**入力した文字を表示する**］をクリックしたままにします。

クイックスタートウィザードを使用して、インターネットアクセスを構成することもできます。

イベントのリポジトリに保管できるイベントの最大数の設定

管理サーバーのプロパティウィンドウ内にある［**イベントリポジトリ**］セクションで、管理サーバーデータベース内で保管するイベントの設定を編集できます。編集可能な設定項目は、イベントのレコード数上限やレコードの保管期間があります。保管するイベント数の上限を指定すると、指定した数に応じて必要なディスク容量の概算値が算出されます。データベースのオーバーフローを避けるために十分な空き容量があるかどうかのこの概算値を使用できます。既定の設定では、管理サーバーデータベース内に保管できるイベント数は 400,000 件までとなっています。データベースで推奨される範囲でのイベント数の上限は、45,000,000 件です。

アプリケーションは 10 分ごとにデータベースをチェックします。イベント数が指定された最大値に 10,000 を加えた値に達すると、アプリケーションは最も古いイベントを削除し、指定された最大数のイベントのみが残ります。

管理サーバーが古いイベントを削除する際に、新しいイベントのデータベースへの保存は行えません。この期間、拒否したイベントの情報は Kaspersky イベントログに書き込まれます。新しいイベントはキューに追加され、削除操作が完了した後にデータベースに保存されます。

管理サーバーのイベントリポジトリに保存できるイベント数を制限するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**イベントリポジトリ**］セクションを選択します。データベースに記録するイベント数の上限を指定します。

3. ［**保存**］をクリックします。

さらに、任意のタスクの設定を変更して、タスクの進行状況に関連するイベントを保存したり、タスクの実行結果のみを保存したりできます。それにより、データベース内のイベントの数を削減することで、データベース内のイベントの分析を伴う操作の実行速度を向上し、多数のイベントによって重要なイベントが上書きされる可能性を低下させることができます。

UEFI 保護デバイスの接続設定

*UEFI 保護デバイス*とは、BIOS レベルで統合された UEFI 用のカスペルスキーソリューションまたはアプリケーションを備えたデバイスです。統合された保護により、システムが起動した瞬間からデバイスのセキュリティを確保し、同時に、ソフトウェアが統合されていないデバイスでの保護が、セキュリティ製品の起動後にのみ機能し始めるようにします。Kaspersky Security Center はこれらのデバイスをサポートしています。

UEFI 保護デバイスの接続設定を編集するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（ ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**追加のポート**］セクションを選択します。

3. 目的の設定項目を変更します：

   - **UEFI 保護デバイスおよび KasperskyOS デバイス用のポートを開く**

     UEFI 保護デバイスを管理サーバーに接続できます。

   - **UEFI 保護デバイスおよび KasperskyOS デバイス用のポート**

     ［**UEFI 保護デバイスおよび KasperskyOS デバイス用のポートを開く**］がオンの場合、ポート番号を変更できます。既定のポート番号は 13294 です。

4. ［**保存**］をクリックします。

UEFI 保護デバイスを管理サーバーに接続できる状態になっています。

管理サーバーの階層の作成：セカンダリ管理サーバーの追加

セカンダリ管理サーバーの追加（プライマリ管理サーバーとして指定する管理サーバーで実行）

管理サーバーをセカンダリ管理サーバーとして追加し、プライマリとセカンダリの階層を確立することができます。

Kaspersky Security Center Web コンソールから接続できる管理サーバーをセカンダリ管理サーバーとして追加するには：

1. プライマリ管理サーバーとして指定する管理サーバーのポート 13000 にセカンダリ管理サーバーから接続できることを確認します。
2. プライマリ管理サーバーとして指定する管理サーバーで、［設定］アイコン（  ）をクリックします。
3. 表示されたプロパティページで、［**管理サーバー**］タブを選択します。
4. 管理サーバーを追加する管理グループの名前に隣接するチェックボックスをオンにします。
5. メニューヘッダーから［**セカンダリ管理サーバーの接続**］を選択します。

   セカンダリ管理サーバー追加ウィザードが起動します。［**次へ**］をオンにして、ウィザードに沿って手順を進めます。
6. 次のフィールドに値を入力します：

   - **プライマリ管理サーバーを DMZ 内のセカンダリ管理サーバーに接続する**

     セカンダリ管理サーバーが非武装地帯（DMZ）にある場合は、このオプションをオンにします。

     このオプションをオンにした場合は、**セカンダリサーバーのアドレス**パラメータを指定する必要があります。

     このオプションを選択すると、プライマリ管理サーバーがセカンダリ管理サーバーへの接続を開始します。あるいは、セカンダリ管理サーバーがプライマリ管理サーバーへの接続を開始します。

   - **セカンダリ管理サーバーの表示名**

     階層で表示する、セカンダリ管理サーバーの名前。必要に応じて、IP アドレスを名前として入力するか、「グループ 1 のセカンダリサーバー」などの名前を使用できます。

   - **セカンダリ管理サーバーアドレス（任意）**

     セカンダリ管理サーバーの IP アドレスまたはドメイン名を指定します。

     このパラメータは、［**DMZ のプライマリ管理サーバーをセカンダリ管理サーバーに接続**］オプションが有効になっている場合に必要です。

   - **管理サーバーの SSL ポート**

     プライマリ管理サーバー上の SSL ポート番号を指定します。既定のポート番号は 13000 です。

   - **管理サーバーの API ポート**

     OpenAPI 経由の接続を受信するためのプライマリ管理サーバー上のポート番号を指定します。既定のポート番号は 13299 です。
7. セカンダリ管理サーバーの証明書を指定します。**セカンダリサーバーのアドレス**パラメータを指定した場合は、［**セカンダリ管理サーバーから取得**］をクリックして証明書を取得できます。それ以外の場合は、［**証明書ファイルの参照**］をクリックして証明書ファイルを見つけます。

8. 接続の設定を指定します：

   - 将来のプライマリ管理サーバーのアドレスを入力します。
   - 将来のセカンダリ管理サーバーがプロキシサーバーを使用する場合は、プロキシサーバーのアドレスとユーザー資格情報を入力して、プロキシサーバーに接続します。

9. 将来のセカンダリ管理サーバーへのアクセス権を持つユーザーの資格情報を入力します。

10. 二段階認証が有効になっていて設定済みの場合は、認証アプリによって生成されたセキュリティコードを指定します。

    このアカウントで二段階認証が有効になっている場合は、将来のセカンダリサーバーからのみ階層を作成できます（以下の手順を参照してください）。

接続設定が正しければ、将来のセカンダリサーバーとの接続が確立され、「プライマリ / セカンダリ」階層が構築されます。接続に失敗した場合は、接続設定を確認するか、将来のセカンダリサーバーの証明書を手動で指定します。

プライマリとセカンダリの管理サーバー間の接続は、ポート 13000 で確立されます。プライマリ管理サーバーからのタスクとポリシーが受信および適用されます。プライマリ管理サーバー上の追加先の管理グループにセカンダリ管理サーバーが表示されます。

セカンダリ管理サーバーの追加（セカンダリ管理サーバーとして指定する管理サーバーで実行）

セカンダリ管理サーバーとして指定する管理サーバーが一時的に切断されていた、または使用できなかったため、この管理サーバーに接続できなかった場合も、セカンダリ管理サーバーを追加できます。

Kaspersky Security Center Web コンソールから接続できない管理サーバーをセカンダリ管理サーバーとして追加するには：

1. セカンダリ管理サーバーとして指定する管理サーバーがあるオフィスのシステム管理者に、プライマリ管理サーバーとして指定する管理サーバーの証明書ファイルを渡します（たとえば、フラッシュドライブなどの外部デバイスにファイルを書き込んで送付したり、メールで送信したりできます）。

   証明書ファイルは、プライマリ管理サーバーとして指定する管理サーバーの %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer にあります。

2. セカンダリ管理サーバーとして指定する管理サーバーを担当しているシステム管理者に、次の操作を依頼します：

   a. 設定アイコン（ ）をクリックします。

   b. 表示されるプロパティページで、［**全般**］タブの［**管理サーバーの階層**］セクションに移動します。

   c. ［**この管理サーバーをセカンダリ管理サーバーとして使用する**］を選択します。

   d. ［**プライマリ管理サーバーのアドレス**］に、プライマリ管理サーバーのネットワーク名を入力します。

   e. ［**参照**］をクリックして、プライマリ管理サーバーとして指定する管理サーバーの保存した証明書ファイルを選択します。

   f. 必要に応じて、［**プライマリ管理サーバーを DMZ 内のセカンダリ管理サーバーに接続する**］をオンにします。

g. プロキシサーバーを使用してセカンダリ管理サーバーとして指定する管理サーバーに接続する場合、［**プロキシサーバーを使用する**］をオンにして接続設定を指定します。

h. ［**保存**］をクリックします。

プライマリとセカンダリの階層が構築されます。ポート 13000 を使用して、セカンダリ管理サーバーからプライマリ管理サーバーへの接続が開始されます。プライマリ管理サーバーからのタスクとポリシーが受信および適用されます。プライマリ管理サーバー上の追加先の管理グループにセカンダリ管理サーバーが表示されます。

セカンダリ管理サーバーのリストの表示

セカンダリ管理サーバー（仮想管理サーバーを含む）のリストを表示するには：

メインメニューで、設定アイコン（）の横にある管理サーバーの名前をクリックします。

セカンダリ管理サーバー（仮想管理サーバーを含む）のドロップダウンリストが表示されます。

表示されている管理サーバーの名前をクリックすると、そのサーバーに移動できます。

管理グループも表示されますが、グレーアウトされており、このメニュー内では管理できません。

Kaspersky Security Center Web コンソールでプライマリ管理サーバーに接続しており、セカンダリ管理サーバーによって管理されている仮想管理サーバーに接続できない場合は、次のいずれかの方法を使用できます：

- **Kaspersky Security Center Web コンソールの既存のインストールを変更して、セカンダリサーバーを信頼できる管理サーバーのリストに追加します**。その後、Kaspersky Security Center Web コンソールで仮想管理サーバーに接続できるようになります。

  1. Kaspersky Security Center Web コンソールがインストールされているデバイスで、管理者権限が付与されたアカウントを使用してインストールファイル ksc-web-console-<バージョン番号>.<ビルド番号>.exe を実行します。

     セットアップウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

  2. ［**アップグレード**］をオンにします。

  3. ［**変更の種別**］ステップで、［**接続設定の編集**］を選択します。

  4. ［**信頼済みの管理サーバー**］ステップで、必要なセカンダリ管理サーバーを追加します。

  5. 最後のステップで［**変更**］をクリックし、新しい設定を適用します。

  6. Web コンソールの再設定が正常に完了したら、［**終了**］をクリックします。

- Kaspersky Security Center Web コンソールを使用して、仮想サーバーが作成されたセカンダリ管理サーバーに直接接続します。その後、Kaspersky Security Center Web コンソールで仮想管理サーバーに切り替えられるようになります。

- MMC ベースの管理コンソールを使用して、仮想サーバーに直接接続します。

管理サーバーの階層の削除

管理サーバーの階層構造が不要になった場合は、管理サーバーを階層構造から離脱させることができます。

管理サーバーの階層を削除するには：

1. メインメニューで、プライマリ管理サーバーの名前の横にある設定アイコン（）をクリックします。
2. 表示されたページで、［**管理サーバー**］タブに移動します。
3. セカンダリ管理サーバーを削除する管理グループで、目的のセカンダリ管理サーバーを選択します。
4. メニューヘッダーから［**削除**］を選択します。
5. 表示されるウィンドウで、［**OK**］をクリックし、セカンダリ管理サーバーを削除する処理を確定させます。

プライマリ管理サーバーとして動作していた管理サーバーと、セカンダリ理サーバーとして動作していた管理サーバーは、互いに独立して動作するようになります。これにより、階層構造が解消されます。

管理サーバーのメンテナンス

管理サーバーのメンテナンスにより、管理サーバーのフォルダー内のスペースを解放し、不要になったオブジェクトを削除して定義データベースのサイズを縮小できます。これにより、アプリケーションのパフォーマンスと動作の信頼性が向上します。管理サーバーのメンテナンスは、少なくとも週1回は実施してください。

管理サーバーのメンテナンスは、専用のタスクで実施されます。管理サーバーのメンテナンス時、次の処理が実行されます：

- ストレージフォルダーから不要なフォルダとファイルを削除します。
- テーブルから不要なレコード（「ダングリングポインター」とも呼ばれます）を削除します。
- キャッシュをクリアします。
- 定義データベースを管理します（DBMS として SQL Server または PostgreSQL を使用する場合）：
  - 定義データベースのエラーをチェックします（SQL Server でのみ使用可能）
  - データベースのインデックスを再編成する
  - データベースの統計情報を更新する
  - データベースを縮小する（必要に応じて）

管理サーバーのメンテナンスタスクは、MariaDB バージョン 10.3 以降をサポートします。MariaDB バージョン 10.2 以前を使用する場合、管理者はこの DBMS を独自に維持する必要があります。

管理サーバーのメンテナンスタスクは、Kaspersky Security Center をインストールすると自動的に作成されます。管理サーバーのメンテナンスタスクを削除してしまった場合は、手動で作成することができます。

管理サーバーのメンテナンスを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。
3. ウィザードの［**新規タスク設定**］ウィンドウで、タスク種別に［**管理サーバーのメンテナンス**］を選択し、［**次へ**］をクリックします。
4. 引き続きウィザードの指示に従って操作します。

作成したタスクはタスクリストに表示されます。1台の管理サーバーに対して実行できる管理サーバーのメンテナンスタスクは1つのみです。管理サーバーに対して、既に 管理サーバーのメンテナンス タスクが作成されている場合は、新たに 管理サーバーのメンテナンス タスクを作成することはできません。

インターフェイスの設定

Kaspersky Security Center Web コンソールのインターフェイスを設定して、使用している機能に応じてセクションとインターフェイス要素を表示または非表示にすることができます。

現在使用している機能に基づいて Kaspersky Security Center Web コンソールのインターフェイスを設定するには：

1. メインメニューで、アカウント設定に移動して、［**インターフェイスのオプション**］を選択します。
2. 表示される［**インターフェイスのオプション**］ウィンドウで、必要なオプションをオンまたはオフにします。
3. ［**保存**］をクリックします。

その後、コンソールは有効なオプションに従ってメインメニューにセクションを表示します。たとえば、［**EDR アラートを表示**］をオンにした場合、メイン メニューに［**監視とレポート**］→［**アラート**］セクションが表示されます。

仮想管理サーバーの管理

このセクションでは、仮想管理サーバーを管理する次の操作について説明します：

- 仮想管理サーバーの作成
- 仮想管理サーバーの有効化および無効化
- 仮想管理サーバーの管理者を割り当てる
- クライアントデバイスの管理サーバーの変更
- 仮想管理サーバーの削除

仮想管理サーバーの作成

仮想管理サーバーを作成して、管理グループに追加できます。

仮想管理サーバーを作成して追加するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
2. 表示されるウィンドウで、［**管理サーバー**］タブに移動します。
3. 仮想管理サーバーを追加する管理グループを選択します。
   仮想管理サーバーは選択したグループ（サブグループを含む）からデバイスを管理します。
4. メニューのリストから［**新しい仮想管理サーバー**］を選択します。
5. 表示されるウィンドウで、新しい仮想管理サーバーのプロパティを指定します。
   - **仮想管理サーバー名**
   - **管理サーバー接続用アドレス**
     管理サーバーの名前または IP アドレスを指定できます。
6. ユーザーのリストから、仮想管理サーバーの管理者を選択します。必要に応じて、既存のアカウントを管理者ロールに割り当てる前にこのアカウントを編集したり、新しいアカウントを作成したりできます。
7. ［**保存**］をクリックします。

新しい仮想管理サーバーが作成され、［**管理サーバー**］タブで表示されていた管理グループに追加されます。

Kaspersky Security Center Web コンソールでプライマリ管理サーバーに接続しており、セカンダリ管理サーバーによって管理されている仮想管理サーバーに接続できない場合は、次のいずれかの方法を使用できます：

- **Kaspersky Security Center Web コンソールの既存のインストールを変更して、セカンダリサーバーを信頼できる管理サーバーのリストに追加します**。その後、Kaspersky Security Center Web コンソールで仮想管理サーバーに接続できるようになります。

1. Kaspersky Security Center Web コンソールがインストールされているデバイスで、管理者権限が付与されたアカウントを使用してインストールファイル ksc-web-console-<バージョン番号>.<ビルド番号>.exe を実行します。

   セットアップウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

2. ［**アップグレード**］をオンにします。

3. ［**変更の種別**］ステップで、［**接続設定の編集**］を選択します。

4. ［**信頼済みの管理サーバー**］ステップで、必要なセカンダリ管理サーバーを追加します。

5. 最後のステップで［**変更**］をクリックし、新しい設定を適用します。

6. Web コンソールの再設定が正常に完了したら、［**終了**］をクリックします。

- Kaspersky Security Center Web コンソールを使用して、仮想サーバーが作成されたセカンダリ管理サーバーに直接接続します。その後、Kaspersky Security Center Web コンソールで仮想管理サーバーに切り替えられるようになります。
- MMC ベースの管理コンソールを使用して、仮想サーバーに直接接続します。

仮想管理サーバーの有効化および無効化

新しい仮想管理サーバーを作成すると、既定で有効になります。いつでも無効にしたり、再び有効にできます。仮想管理サーバーの無効化または有効化は、物理管理サーバーをオフまたはオンに切り替えることと同じです。

仮想管理サーバーを有効または無効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。

2. 表示されるウィンドウで、［**管理サーバー**］タブに移動します。

3. 有効または無効にする仮想管理サーバーを選択します。

4. メニューヘッダーで［**仮想管理サーバーの有効化または無効化**］を選択します。

   以前の状態に応じて、仮想管理サーバーの状態が有効または無効に変更されます。管理サーバー名の横にアップデートされた状態が表示されます。

仮想管理サーバーへの管理者の割り当て

組織内で仮想管理サーバーを使用する場合、仮想管理サーバーごとに専任の管理者を割り当てることができます。たとえば、仮想管理サーバーを作成して組織の個別のオフィスや部門を管理する場合や、MSP プロバイダーで仮想管理サーバーを介してテナントを管理する場合に便利です。

仮想管理サーバーを作成すると、プライマリ管理サーバーのユーザーリストとすべてのユーザー権限が継承されます。ユーザーがプライマリサーバーへのアクセス権を持っている場合、このユーザーは仮想サーバーへのアクセス権も持っています。作成後、サーバーへのアクセス権を個別に設定します。仮想管理サーバーのみに管理者を割り当てる場合は、管理者がプライマリ管理サーバーへのアクセス権を持っていないことを確認してください。

仮想管理サーバーへの管理者アクセス権を付与することにより、仮想管理サーバーの管理者を割り当てます。次のいずれかの方法で、必要なアクセス権を付与できます：

- 管理者のアクセス権を手動で設定する
- 管理者に1つ以上のユーザーロールを割り当てる

Kaspersky Security Center Web コンソールにサインインするには、仮想管理サーバーの管理者が仮想管理サーバーの名前、ユーザー名、およびパスワードを指定します。Kaspersky Security Center Web コンソールは管理者を認証し、管理者がアクセス権を持つ仮想管理サーバーを開きます。管理者は、管理サーバーを切り替えることはできません。

必須条件

開始する前に、次の条件が満たされていることを確認してください：

- 仮想管理サーバーが作成されている。
- プライマリ管理サーバーで、仮想管理サーバーに割り当てる管理者のアカウントを作成した。
- ［**一般的な機能**］→［**ユーザーのアクセス許可**］機能領域の**オブジェクト ACL の変更**権限を持っている。

アクセス権の手動設定

仮想管理サーバーの管理者を割り当てるには：

1. メインメニューで、必要な仮想管理サーバーに切り替えます：
   a. シェブロンアイコン（）が現在の管理サーバー名の右側に表示されます。
   b. 必要な管理サーバーを選択します。
2. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
3. ［**アクセス権**］タブで、［**追加**］をクリックします。
   プライマリ管理サーバーと現在の仮想管理サーバーのユーザーの統合リストが表示されます。
4. ユーザーのリストから、仮想管理サーバーに割り当てる管理者のアカウントを選択し、［**OK**］をクリックします。
   選択したユーザーが［**アクセス権**］タブのユーザーリストに追加されます。
5. 追加されたアカウントの横にあるチェックボックスをオンにし、［**アクセス権**］をクリックします。
6. 仮想管理サーバーで管理者が持つ権限を設定します。
   認証が成功するためには、管理者には少なくとも次の権限が必要です：

- **読み取り**権限（［**一般的な機能**］→［**基本機能**］の機能領域）
- **読み取り**権限（［**一般的な機能**］→［**仮想管理サーバー**］の機能領域）

変更されたユーザー権限が管理者アカウントに保存されます。

ユーザーロールの割り当てによるアクセス権の設定

あるいは、ユーザーロールを介して仮想管理サーバー管理者にアクセス権を付与することもできます。たとえば、同じ仮想管理サーバーに複数の管理者を割り当てる場合に便利です。この場合、複数の管理者に同じユーザー権限を構成する代わりに、管理者のアカウントに同じ1つ以上のユーザーロールを割り当てることができます。

ユーザーロールを割り当てて仮想管理サーバーの管理者を割り当てるには：

1. プライマリ管理サーバーで、新しいユーザーロールを作成し、管理者が仮想管理サーバーで持つ必要があるすべてのアクセス権を指定します。たとえば、様々な機能領域へのアクセスを分離する場合は、複数のロールを作成できます。
2. メインメニューで、必要な仮想管理サーバーに切り替えます：
   a. シェブロンアイコン（）が現在の管理サーバー名の右側に表示されます。
   b. 必要な管理サーバーを選択します。
3. 新しいロールまたは複数のロールを管理者アカウントに割り当てます。

ロールが管理者アカウントに割り当てられます。

オブジェクトレベルでのアクセス権の設定

機能領域レベルでのアクセス権の割り当てに加えて、仮想管理サーバー上の特定のオブジェクト（特定の管理グループやタスクなど）へのアクセスを設定できます。これを行うには、仮想管理サーバーに切り替えてから、オブジェクトのプロパティでアクセス権を設定します。

クライアントデバイスの管理サーバーの変更

［**管理サーバーの変更**］タスクを使用して、クライアントデバイスを管理する管理サーバーを別のサーバーに変更できます。タスクの完了後、選択したクライアントデバイスは指定した管理サーバーの管理下に置かれます。

クライアントデバイスを管理する管理サーバーを別のサーバーに変更するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. Kaspersky Security Center アプリケーションで、［**管理サーバーの変更**］タスク種別を選択します。
4. 作成中のタスク名を入力します。

タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

5. タスクを割り当てるデバイスを選択します。
6. 選択したデバイスの管理に使用する管理サーバーを選択します。
7. 次のようにアカウントの設定を指定します。

- **既定のアカウント**

  タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。
  既定では、このオプションがオンです。

- **アカウントの指定**

  ［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

- **アカウント**

  タスクを実行するアカウント。

- **パスワード**

  タスクが実行されるアカウントのパスワード。

8. ［**タスク作成の終了**］ページで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
9. ［**終了**］をクリックします。
   タスクが作成され、タスクリストに表示されます。
10. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。
11. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。
12. ［**保存**］をクリックします。
    タスクが指定した設定で作成されます。
13. 作成したタスクを実行します。

タスクが完了すると、タスクの対象となったクライアントデバイスは、タスク設定で指定した管理サーバーの管理下に置かれます。

仮想管理サーバーの削除

仮想管理サーバーを削除すると、管理サーバーで作成したすべてのオブジェクト（ポリシーとタスクを含む）も削除されます。仮想管理サーバーで管理されていた管理グループの管理対象デバイスは、管理グループから削除されます。Kaspersky Security Center の管理下にあるデバイスを返却するには、ネットワークポーリングを実行してから、見つかったデバイスを[未割り当てのデバイス]グループから管理グループに移動します。

仮想管理サーバーを削除するには：

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
2. 表示されるウィンドウで、［**管理サーバー**］タブに移動します。
3. 削除する仮想管理サーバーを選択します。
4. メニューヘッダーから［**削除**］を選択します。

   仮想管理サーバーが削除されます。

不正な変更からのユーザーアカウントの保護を有効にする

追加のオプションを有効にして不正な変更からのユーザーアカウントの保護を有効にすることができます。このオプションをオンにすると、ユーザーアカウントの編集にはユーザー認証が要求されます。

不正な変更からのユーザーアカウントの保護を有効または無効にする

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に移動します。
2. 不正な変更からの保護を指定する内部ユーザーアカウントの名前をクリックします。
3. ユーザー設定ウィンドウが表示されたら、［**アカウント保護**］を選択します。
4. アカウントの設定が変更または更新された際に毎回ユーザーの資格情報を要求するよう設定するには、［**アカウント保護**］タブで、［**認証を要求してユーザーアカウントの変更権限をチェックする**］を選択します。そうでない場合は、［**追加の認証なしでのこのアカウントの変更をユーザーに対して許可する**］を選択します。
5. ［**保存**］をクリックします。

ユーザーのアカウントに対して、不正な変更からのアカウントの保護が有効になります。

二段階認証

このセクションでは、Kaspersky Security Center Web コンソールへの不正なアクセスのリスクを軽減するために二段階認証を使用する方法について説明します。

シナリオ：すべてのユーザーに対して二段階認証を設定する

このシナリオでは、すべてのユーザーに対して二段階認証を有効にする方法と、二段階認証からユーザーアカウントを除外する方法について説明します。別のユーザーに対する二段階認証を有効にする前に自分のアカウントの二段階認証を有効にしなかった場合、本製品は最初にお使いのアカウントの二段階認証を有効にするウィンドウを開きます。このシナリオでは、自分のアカウントに対して二段階認証を有効にする方法についても説明します。

自分のアカウントの二段階認証を有効にした後、すべてのユーザーに対して二段階認証を有効にする手順に進んでください。

必須条件

開始する前に：

- ご自分のアカウントに、別のユーザーのアカウントのセキュリティ設定を変更するための［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限があることを確認してください。
- 管理サーバーの他のユーザーがデバイス上に認証アプリをインストール済みであることを確認してください。

実行するステップ

すべてのユーザーに対して二段階認証を段階的に有効にするには：

1. **認証アプリをデバイスにインストールする**

   時間ベースのワンタイムパスワードのアルゴリズム（TOTP）をサポートする任意のアプリケーションをインストールできます。たとえば：

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex Key
   - Avanpost Authenticator
   - Aladdin 2FA

   Kaspersky Security Center が使用する認証アプリをサポートしているかどうかを確認するには、すべてのユーザーまたは特定のユーザーに対して二段階認証を有効にします。

   手順の 1 つでは、認証アプリによって生成されたセキュリティコードを指定することを推奨しています。成功すると、Kaspersky Security Center は選択した認証システムをサポートします。

   管理サーバーへの接続が確立されているデバイスと同じデバイスに認証アプリをインストールすることは強く推奨しません。

2. **管理サーバーがインストールされているデバイスの時刻と、認証アプリの時刻を同期する**

   外部時刻ソースを使用して、認証アプリを備えたデバイスの時刻と、管理サーバーを備えたデバイスの時刻が UTC に同期されていることを確認します。そうしないと、認証および二段階認証のアクティブ化中に失敗が発生する可能性があります。

3. **自分のアカウントの二段階認証を有効にし、アカウントの秘密鍵を受け取る**

   実行手順の説明：

   - MMC ベースの管理コンソール：自分のアカウントの二段階認証を有効にする
   - Kaspersky Security Center Web コンソール：自分のアカウントの二段階認証を有効にする

   自分のアカウントの二段階認証を有効にした後、すべてのユーザーに対して二段階認証を有効にできるようになります。

4. **すべてのユーザーに対して二段階認証を有効にする**

   二段階認証を有効にしたユーザーは、管理サーバーにログインする際に二段階認証を使用する必要があります。

   実行手順の説明：

   - MMC ベースの管理コンソール：すべてのユーザーに対して二段階認証を有効にする
   - Kaspersky Security Center Web コンソール：すべてのユーザーに対して二段階認証を有効にする

5. **セキュリティコードの発行元の名前を変更する**

   同じ名前の管理サーバーがある場合は、異なる管理サーバーとして認識できるように、セキュリティコードの発行元の名前を別のものに変更する必要があります。

   実行手順の説明：

   - MMC ベースの管理コンソール：セキュリティコードの発行元の名前を変更する
   - Kaspersky Security Center Web コンソール：セキュリティコードの発行元の名前を変更する

6. **二段階認証を有効にする必要のないユーザーアカウントを除外する**

   必要に応じて、二段階認証からユーザーを除外することができます。アカウントが除外されたユーザーは管理サーバーへのログインの際に二段階認証が不要となります。

   実行手順の説明：

   - MMC ベースの管理コンソール：二段階認証からアカウントを除外する
   - Kaspersky Security Center Web コンソール：二段階認証からアカウントを除外する

7. **自分のアカウントの二段階認証を設定します**

   ユーザーが二段階認証から除外されておらず、アカウントに二段階認証がまだ設定されていない場合は、Kaspersky Security Center にサインインする時に開くウィンドウで設定する必要があります。そうしないと、権限に従って管理サーバーにアクセスできなくなります。

   実行手順の説明：

   - MMC ベースの管理コンソール：自分のアカウントの二段階認証を設定します
   - Kaspersky Security Center Web コンソール：自分のアカウントの二段階認証を設定します

結果

このシナリオの完了時には：

- 自分のアカウントの二段階認証が有効になります。

- 除外したユーザーアカウント以外の管理サーバーのすべてのユーザーアカウントに対して、二段階認証が有効になります。

二段階認証の概要

アカウントの二段階認証が有効になっている場合、管理コンソールまたは Kaspersky Security Center Web コンソールにログインするには、ユーザー名とパスワードに加えて、1回のみ使用するセキュリティコードが必要です。ドメイン認証を有効にすると、ユーザーは1回のみ使用するセキュリティコードを入力するだけで済みます。

二段階認証を使用するには、1回のみ使用するセキュリティコードを生成する認証アプリをモバイルデバイスまたはコンピュータにインストールする必要があります。時間ベースのワンタイムパスワードのアルゴリズム（TOTP）をサポートする任意のアプリケーションを使用できます。たとえば：

- Google Authenticator
- Microsoft Authenticator
- Bitrix24 OTP
- Yandex Key
- Avanpost Authenticator
- Aladdin 2FA

Kaspersky Security Center が使用する認証アプリをサポートしているかどうかを確認するには、すべてのユーザーまたは特定のユーザーに対して二段階認証を有効にします。

手順の1つでは、認証アプリによって生成されたセキュリティコードを指定することを推奨しています。成功すると、Kaspersky Security Center は選択した認証システムをサポートします。

秘密鍵または QR コードを保存し、安全な場所に保管することを強く推奨します。これにより、モバイルデバイスにアクセスできなかった際に Kaspersky Security Center Web コンソールへのアクセスを復元することができます。

Kaspersky Security Center を安全に使用するため、自分のアカウントに対して二段階認証を設定し、すべてのユーザーに対して二段階認証を有効にできます。

二段階認証からアカウントを除外することができます。これは認証のためのセキュリティコードを受信できないサービスアカウントで必要となる場合があります。

ルールと制限事項

すべてのユーザーに対して二段階認証を有効にし、特定のユーザーに対して二段階認証を無効にするには：

- アカウントが［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限を持っていることを確認します。
- アカウントの二段階認証を有効にする。

すべてのユーザーの二段階認証を無効にするには：

- アカウントが［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限を持っていることを確認します。
- 二段階認証を使用して Kaspersky Security Center Web コンソールにログインします。

Kaspersky Security Center 管理サーバーのバージョン 13 以降でユーザーアカウントに二段階認証が有効になっている場合、Kaspersky Security Center Web コンソールのバージョン 12、12.1 または 12.2 にユーザーはログインできません。

秘密鍵の再発行

二段階認証に使用する秘密鍵は、どのユーザーでも再発行できます。ユーザーが再発行された秘密鍵を使用して管理サーバーにログインすると、新しい秘密鍵がユーザーアカウントに保存されます。ユーザーが新しい秘密鍵を誤って入力した場合、新しい秘密鍵は保存されず、現在の秘密鍵は有効なままになります。

セキュリティコードには、*発行元の名前*として参照される識別子があります。セキュリティコードの発行元の名前は、認証アプリの管理サーバーの識別子として使用されます。既定では、セキュリティコードの発行元の名前は管理サーバーの名前と同じです。セキュリティコードの発行元の名前を変更することができます。セキュリティコードの発行元の名前を変更した後は、新しい秘密鍵を発行して認証アプリに渡す必要があります。

自分のアカウントの二段階認証を有効にする

自分のアカウントの二段階認証を有効にすることができます。

アカウントの二段階認証を有効にする前に、お使いのモバイルデバイスに認証アプリがインストールされていることを確認してください。認証アプリと管理サーバーがインストールされているデバイスの時刻が同期されていることを確認します。

ユーザーアカウントの二段階認証を有効にするには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に移動します。
2. 自分のアカウントの名前をクリックします。
3. ユーザー設定ウィンドウが表示されたら、［**認証セキュリティ**］を選択します。
4. ［**認証セキュリティ**］タブ：
   a. ［**ユーザー名、パスワード、セキュリティコードを要求（二段階認証）**］をオンにします。［**保存**］をクリックします。
   b. 開いた［二段階認証］ウィンドウで、［**二段階認証の設定方法を表示する**］をクリックします。
   認証アプリに秘密鍵を入力するか、［**QR コードを表示する**］をクリックして、モバイルデバイス上の認証アプリで QR コードをスキャンして、ワンタイムセキュリティコードを受け取ります。
   c. 二段階認証のウィンドウで、認証アプリが生成したセキュリティコードを入力し、［**チェックして適用**］をクリックします。

5. ［**保存**］をクリックします。

自分のアカウントの二段階認証が有効になります。

全ユーザーに対して二段階認証の有効化

お客様自身のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限があり、二段階認証を使用して認証済みである場合、管理サーバーのすべてのユーザーに対して二段階認証を有効にすることができます。

すべてのユーザーに対して二段階認証を有効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. プロパティウィンドウの［**認証セキュリティ**］タブで、**全ユーザーに対する二段階認証**の切り替えスイッチを有効の位置に移動します。

3. 自分のアカウントの二段階認証を有効にしなかった場合、本製品は最初に自分のアカウントの二段階認証を有効にするウィンドウを開きます。

   a. ［二段階認証］ウィンドウで、［**二段階認証の設定方法を表示する**］をクリックします。

   b. 認証アプリに手動で秘密鍵を入力するか、［**QR コードを表示する**］をクリックして、モバイルデバイス上の認証アプリケーションで QR コードをスキャンして、ワンタイムセキュリティコードを受け取ります。

   c. 二段階認証のウィンドウで、認証アプリが生成したセキュリティコードを入力し、［**チェックして適用**］をクリックします。

すべてのユーザーに対して二段階認証が有効になります。以降、すべてのユーザーに対する二段階認証を有効にする前に追加されたユーザーを含む管理サーバーのユーザーは、アカウントが二段階認証の対象から除外されたユーザー以外全員、アカウントに二段階認証を設定する必要があります。

ユーザーアカウントの二段階認証を無効にする

ご自分のアカウント、または別のユーザーの二段階認証を無効にすることができます。

お客様自身のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限があり、二段階認証を使用して認証済みである場合、他のユーザーアカウントの二段階認証を無効にすることができます。

ユーザーアカウントの二段階認証を無効にするには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に移動します。

2. 二段階認証を無効にする内部ユーザーアカウントの名前をクリックします。この名前は、ご自分のアカウントまたは別のユーザーのアカウントです。

3. ユーザー設定ウィンドウが表示されたら、［**アカウント保護**］を選択します。

4. ［**アカウント保護**］タブで、［**ユーザー名とパスワードのみ要求**］を選択してユーザーアカウントの二段階認証を無効にします。

5. ［**保存**］をクリックします。

このユーザーアカウントの二段階認証が無効になります。

二段階認証を使用して Kaspersky Security Center Web コンソールにログインできないユーザーのアクセスを復元する場合は、このユーザーアカウントの二段階認証を無効にし、上記のように［**ユーザー名とパスワードのみ要求**］をオンにします。その後、二段階認証を無効にしたユーザーアカウントで Kaspersky Security Center Web コンソールにログインし、再度認証を有効にします。

全ユーザーに対して二段階認証の無効化

自分のアカウントで二段階認証が有効になっており、**一般的な機能：ユーザー権限**のオブジェクト ACL の変更権限がある場合にすべてのユーザーに対して必要な二段階認証を無効にすることができます。ご自身のアカウントで二段階認証が有効にされていない場合、すべてのユーザーに対して二段階認証を無効にする前にご自身のアカウントの二段階認証を有効にする必要があります。

すべてのユーザーに対して二段階認証を無効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（ ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. プロパティウィンドウの[**認証セキュリティ**]タブで、**全ユーザーに対する二段階認証**オプションの切り替えスイッチを無効の位置に移動します。

3. 認証ウィンドウでアカウントの認証情報を入力します。

すべてのユーザーに対して二段階認証が無効になります。全ユーザーに対して二段階認証を無効にしても、以前に二段階認証が個別に有効になっていた特定のアカウントには適用されません。

二段階認証からアカウントを除外する

使用中のアカウントに［**一般的な機能：ユーザー権限**］機能領域のオブジェクト ACL の変更権限がある場合は、二段階認証からアカウントを除外することができます。

ユーザーアカウントがすべてのユーザーに対する二段階認証のリストから除外されている場合、このユーザーは二段階認証を使用する必要はありません。

認証中にセキュリティコードをパスできないサービスアカウントの場合、二段階認証からアカウントを除外する必要がある場合があります。

二段階認証から複数のユーザーアカウントを除外する場合：

1. Active Directory のアカウントを除外する場合は、管理サーバーのユーザーのリストを更新するため、Microsoft Active Directory ドメインコントローラーのポーリングを行う必要があります。

2. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（ ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

3. プロパティウィンドウの[**認証セキュリティ**]タブで、二段階認証の除外のテーブルで[**追加**]をクリックします。

4. 表示されたウィンドウで以下を実行します：

   a. 除外するユーザーアカウントを選択します。

   b. ［**OK**］をクリックします。

選択したユーザーアカウントが二段階認証から除外されます。

新しい秘密鍵の作成

使用するアカウントの二段階認証用の新しい秘密鍵は、二段階認証を使用してアカウントが認証された場合のみ生成できます。

ユーザーアカウントに対する新しい秘密鍵を生成するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザー**］の順に移動します。

2. 二段階認証用の新しい秘密鍵を生成するユーザーアカウントの名前をクリックします。

3. ユーザー設定ウィンドウが表示されたら、［**アカウント保護**］を選択します。

4. ［**アカウント保護**］タブで、［**新しい秘密鍵を生成**］をクリックします。

5. 表示された二段階認証ウィンドウで、認証アプリによって作成された新しい秘密鍵を指定します。

6. ［**チェックして適用**］をクリックします。

新しい秘密鍵が生成されました。

モバイルデバイスを紛失した場合は、別のモバイルデバイスに認証アプリをインストールし、新しい秘密鍵を生成して、Kaspersky Security Center Web コンソールへのアクセスを復元できます。

セキュリティコードの発行元の名前を変更する

異なる管理サーバーに対して、複数の識別子（発行元）を設定することができます。別の管理サーバーに同じようなセキュリティコードの発行元の名前が使用されている場合などに、別のセキュリティコードの発行元の名前に変更することができます。既定では、セキュリティコードの発行元の名前は管理サーバーの名前と同じです。

セキュリティコードの発行元の名前を変更した後は、新しい秘密鍵を発行して認証アプリに渡す必要があります。

セキュリティコードの発行元の名前を指定するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ユーザー設定ウィンドウが表示されたら、［**アカウント保護**］を選択します。
3. ［**アカウント保護**］で、［**編集**］リンクをクリックします。
   ［**セキュリティコード発行元の編集**］セクションが開きます。
4. 新しいセキュリティコードの発行元の名前を設定します。
5. ［**OK**］をクリックします。

管理サーバーに新しいセキュリティコードの発行元の名前が設定されます。

自分のアカウントの二段階認証を設定します

二段階認証を有効にした後、初めて Kaspersky Security Center にサインインすると、自分のアカウントの二段階認証を設定するためのウィンドウが開きます。

アカウントの二段階認証を設定する前に、使用中のモバイルデバイスに認証アプリがインストールされていることを確認してください。

外部時刻ソースを使用して、認証アプリを備えたデバイスの時刻と、管理サーバーを備えたデバイスの時刻が UTC に同期されていることを確認します。

アカウントの二段階認証を設定するには：

1. モバイルデバイスの認証アプリを使用して、ワンタイムセキュリティコードを生成します。開くには、次のいずれかの操作を行います：
   - 認証アプリに秘密鍵を手動で入力します。
   - ［**QR コードを表示する**］をクリックし、認証アプリを使用して QR コードをスキャンします。

   モバイルデバイスにセキュリティコードが表示されます。
2. 二段階認証のウィンドウで、認証アプリが生成したセキュリティコードを入力し、［**チェックして適用**］をクリックします。

アカウントには二段階認証が設定されています。自分の権利に従って管理サーバーにアクセスできます。

新規ユーザーが自分で二段階認証を設定することを禁止します

Kaspersky Security Center Web コンソールのアクセスセキュリティをさらに向上させるために、新しいユーザーが自分自身に二段階認証を設定することを禁止できます。

このオプションをオンにする場合、二段階認証が無効になっているユーザー（例：新しいドメイン管理者など）は、自分自身に二段階認証を設定できません。したがって、そのようなユーザーは管理サーバーで認証できず、既に二段階認証を有効にしている別の Kaspersky Security Center 管理者の承認がなければ Kaspersky Security Center Web コンソールにサインインできません。

このオプションは、すべてのユーザーに対して二段階認証が有効になっている場合に使用できます。

新しいユーザーが自分自身に二段階認証を設定することを禁止するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. プロパティウィンドウの［**認証セキュリティ**］タブで、［**新規ユーザーによる二段階認証の設定を禁止する**］スイッチをオンに切り替えます。

このオプションは、二段階認証の除外に追加されたユーザーアカウントには影響しません。

二段階認証が無効になっているユーザーに Kaspersky Security Center Web コンソールへのアクセスを許可するには、［**新規ユーザーによる二段階認証の設定を禁止する**］を一時的にオフにし、ユーザーに二段階認証をオンにするよう依頼してから、オプションをオンに戻します。

管理サーバーデータのバックアップと復元

データバックアップにより、データを失わずに、管理サーバーをデバイス間で移動できます。バックアップを使用すると、管理サーバーのデータベースを別のデバイスに移動した時や、新しいバージョンの Kaspersky Security Center にアップグレードした時に、データを復元できます。

インストールされている管理プラグインはバックアップされないこと留意してください。管理サーバーのデータをバックアップコピーから復元した後で、管理対象アプリケーション用のプラグインをダウンロードして再インストールする必要があります。

管理サーバーのデータをバックアップする前に、仮想管理サーバーが管理グループに追加されているかどうかを確認してください。仮想管理サーバーを追加する場合は、バックアップ前にこの仮想管理サーバーに管理者が割り当てられていることを確認してください。バックアップ後は、仮想管理サーバーへの管理者アクセス権を付与できません。管理者アカウントの資格情報が失われると、仮想管理サーバーに新しい管理者を割り当てることができなくなることに注意してください。

次の方法のいずれかを使用して、管理サーバーデータのバックアップコピーを作成できます。

- 管理コンソールで、データバックアップタスクを作成して実行します。
- 管理サーバーがインストールされているデバイスで klbackup ユーティリティを実行する。このユーティリティは、Kaspersky Security Center の配布キットに含まれています。管理サーバーをインストールすると、このユーティリティは、アプリケーションのインストール時に指定したインストール先フォルダーのルートに格納されます。

次のデータが管理サーバーのバックアップコピー内に保存されます：

- 管理サーバーのデータベース（管理サーバーに保存されているポリシー、タスク、アプリケーション設定、イベント）
- 管理グループとクライアントデバイスの構造についての設定情報

- リモートインストール用アプリケーション配布パッケージのリポジトリ
- 管理サーバー証明書
- ［*アップデート*］フォルダーの内容。

  既定では、フォルダーのパスは C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\ です。

管理サーバーデータを復元するには、klbackup ユーティリティを使用する必要があります。

データバックアップタスクの作成

バックアップタスクは管理サーバーのタスクであり、クイックスタートウィザードで作成されます。クイックスタートウィザードで作成されたバックアップタスクが削除された場合、手動で作成することができます。

管理サーバーのデータバックアップタスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。
3. ウィザードの［**新規タスク設定**］ウィンドウでは［**管理サーバーデータのバックアップ**］タスク種別を選択します。
4. 引き続きウィザードの指示に従って操作します。

［**管理サーバーデータのバックアップ**］タスクは1つのみ作成できます。管理サーバーの管理サーバーデータのバックアップタスクが既に作成されている場合は、管理サーバーのバックアップタスク作成ウィザードのタスク種別選択ウィンドウには表示されません。

管理サーバーデータのバックアップタスクを設定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］に移動し、［**管理サーバーデータのバックアップ**］タスクを選択します。
2. ［**管理サーバーデータのバックアップ**］タスクをクリックします。

   タスクのプロパティウィンドウが開きます。
3. 必要に応じて、一般的なタスク設定を指定します。
4. ［**アプリケーション設定**］セクションで、管理サーバーデータのバックアップコピーを保存するフォルダーへのパスを指定し、バックアップ保護パスワードと、必要に応じてバックアップコピーの数を設定します。
5. ［**保存**］をクリックして変更を適用します。

*管理サーバーデータのバックアップタスク*が設定されました。

管理サーバーの別のデバイスへの移動

新しいデバイスで管理サーバーを使用する必要がある場合は、次のいずれかの方法で移動できます：

- 管理サーバーおよび定義データベースサーバーを新しいデバイスに移動します（定義データベースサーバーは、管理サーバーと一緒に新しいデバイスにインストールすることも、別のデバイスにインストールすることもできます）。
- データベースサーバーを以前のデバイスに保持し、管理サーバーのみを新しいデバイスに移動する。

管理サーバーとデータベースサーバーを新しいデバイスに移動するには：

1. 以前のデバイスで、管理サーバーデータのバックアップを作成します。

   このためには、Kaspersky Security Center Web コンソールからデータバックアップタスクを実行するか、klbackup ユーティリティを実行します。

   > SQL Server を管理サーバーの DBMS として使用している場合、SQL Server から MySQL または MariaDB DBMS へデータを移行できます。これを行うには、klbackup ユーティリティを対話モードで実行して、データバックアップを作成します。バックアップと復元ウィザードの［**バックアップ設定**］ウィンドウで［**MySQL/MariaDB 形式へ移行**］をオンにします。MySQL および MariaDB と互換性があるバックアップが作成されます。その後、データをバックアップから MySQL または MariaDB へ復元することができます。

   > SQL Server から Azure SQL DBMS にデータを移行する場合は、［**Azure 形式へ移行**］オプションをオンにすることもできます。

2. 前のデバイスで、管理サーバーをネットワークから切断します。

3. 管理サーバーをインストールする新しいデバイスを選択します。選択したデバイスのハードウェアとソフトウェアが、管理サーバー、Kaspersky Security Center Web コンソール、およびネットワークエージェントの要件を満たしていることを確認してください。また、管理サーバーで使用されるポートが使用可能であることを確認してください。

4. 新しいデバイスに同じアドレスを割り当てます。

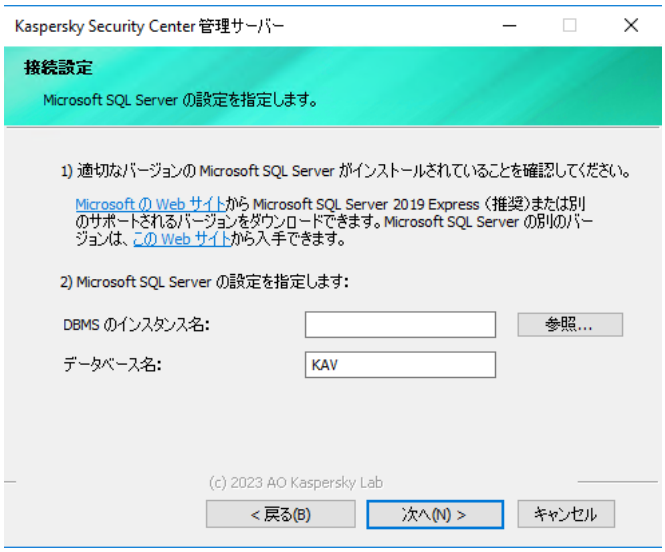
   新しい管理サーバーに NetBIOS 名、FQDN、および固定 IP アドレスを割り当てることができます。これは、ネットワークエージェントが導入された時にネットワークエージェントのインストールパッケージで設定された管理サーバーのアドレスによって異なります。あるいは、ネットワークエージェントが接続する管理サーバーを決定する接続アドレスを使用することもできます（管理対象デバイスでこのアドレスを取得するには、klnagchk ユーティリティを使用します）。

5. 必要に応じて、別のデバイスに管理サーバーが使用するデータベース管理システム（DBMS）をインストールします。

   定義データベースは、管理サーバーと一緒に新しいデバイスにインストールすることも、別のデバイスにインストールすることもできます。このデバイスがハードウェアおよびソフトウェアの要件を満たしていることを確認してください。DBMS を選択する際は、管理サーバーが対応するデバイスの数を考慮してください。

6. 新しいデバイスで管理サーバーのインストールを実行します。

7. 管理サーバーのインストール中に、定義データベースサーバーの接続設定を構成します。



Microsoft SQL Server の［接続設定］ウィンドウの例

データベースサーバーを配置する必要がある場所に応じて、次のいずれかを実行します：

- **データベースサーバーを以前のデバイスに保持する**

  1. ［**DBMS のインスタンス名**］の横にある［**参照**］をクリックし、表示されるリストで以前のデバイスの名前を選択します。

     新しい管理サーバーに接続するためには、以前のデバイスを使用できる必要があります。

  2. ［**データベース名**］に以前のデータベース名を入力します。

- **定義データベースサーバーを新しいデバイスに移動する**

  1. ［**DBMS のインスタンス名**］の横にある［**参照**］をクリックし、表示されるリストで新しいデバイス名を選択します。

  2. ［**データベース名**］に新しいデータベース名を入力します。

     なお、新しいデータベース名は、以前のデバイスのデータベース名と一致している必要があります。管理サーバーのバックアップを使用できるように、データベースの名前は同一である必要があります。既定のデータベース名は *KAV* です。

8. インストールが完了したら、klbackup ユーティリティを使用して、新しいデバイスで管理サーバーのデータを復元します。

   以前のデバイスと新しいデバイスで SQL Server を DBMS として使用する場合、新しいデバイスにインストールされている SQL Server のバージョンは、以前のデバイスにインストールされている SQL Server のバージョンと同じかそれ以降である必要があります。それ以外のバージョンの場合、新しいデバイスで管理サーバーのデータを復元できません。

9. Kaspersky Security Center Web コンソールを開き、管理サーバーに接続します。
10. すべての管理対象デバイスが管理サーバーに接続されていることを確認します。
11. 以前のデバイスから管理サーバーとデータベースサーバーをアンインストールします。

管理コンソールを使用して、管理サーバーとデータベースサーバーを別のデバイスに移動することもできます。

Kaspersky Security Center Web コンソールの初期設定

このセクションでは Kaspersky Security Center Web コンソールのインストール後に初期セットアップを実行するために必要となる手順について説明します。

クイックスタートウィザード（Kaspersky Security Center Web コンソール）

このセクションでは、管理サーバークイックスタートウィザードについて説明します。

ウィザードでは、インターネットにアクセスできる必要があります。管理サーバーがインターネットにアクセスできない場合は、Kaspersky Security Center Web コンソールのインターフェイスを使用して、ウィザードのすべての手順を手動で実行してください。

Kaspersky Security Center では、セキュリティ上の脅威から社内ネットワークを保護するための一元的な管理システムを構築する上で調整が必要な最小限の設定項目が選定されており、これらの設定を編集してセキュリティ管理システムを構築できます。この設定は、クイックスタートウィザードを使用して行います。ウィザードの実行中、次の変更をアプリケーションに対して行うことができます：

- 管理グループ内のデバイスに自動配信可能なライセンス情報ファイルを追加するか、アクティベーションコードを入力します。
- Kaspersky Security Network（KSN）との対話を設定します。KSN を使用可能にした場合、ウィザードは、KSN とデバイスの間の接続を確保する KSN プロキシサーバーサービスを有効にします。
- 管理サーバーと管理対象アプリケーションの動作中に発生したイベントを通知するメール配信を設定します（通知が正しく送信されるようにするには、管理サーバーとすべての受信側デバイスで Messenger サービスが稼働している必要があります）。
- 管理対象デバイスの最上位階層で、ワークステーションとサーバーの保護ポリシー、およびマルウェアスキャンタスク、アップデートのダウンロードタスク、データバックアップタスクを作成します。

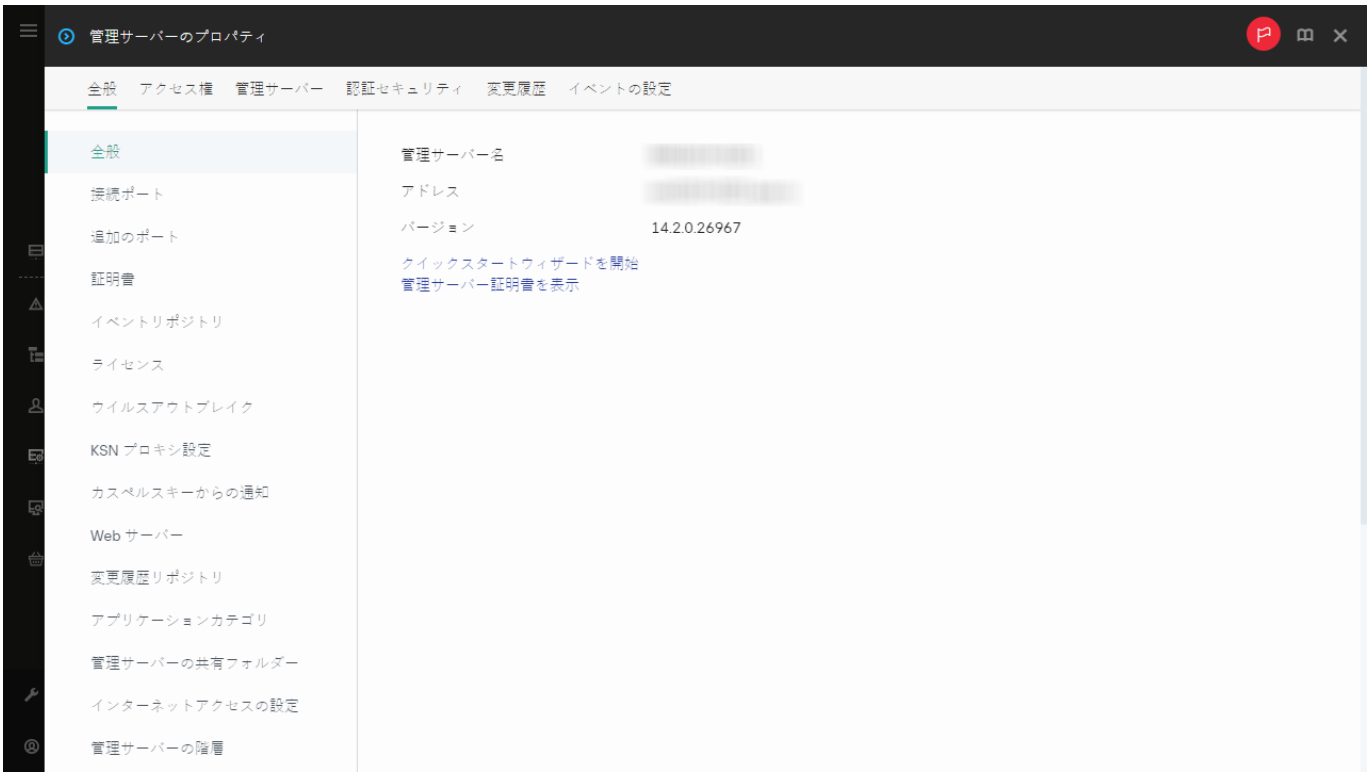
  クイックスタートウィザードでは、［**管理対象デバイス**］フォルダーにポリシーがないアプリケーションに対してのみポリシーが作成されます。管理対象デバイスの最上位階層で同じ名前のタスクが作成済みの場合、クイックスタートウィザードではタスクが作成されません。

管理サーバーのインストール後に初めて接続すると、クイックスタートウィザードを実行することを指示するメッセージが自動的に表示されます。また、クイックスタートウィザードはいつでも手動で起動できます。

クイックスタートウィザードを手動で起動するには：

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（ ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**全般**］セクションを選択します。



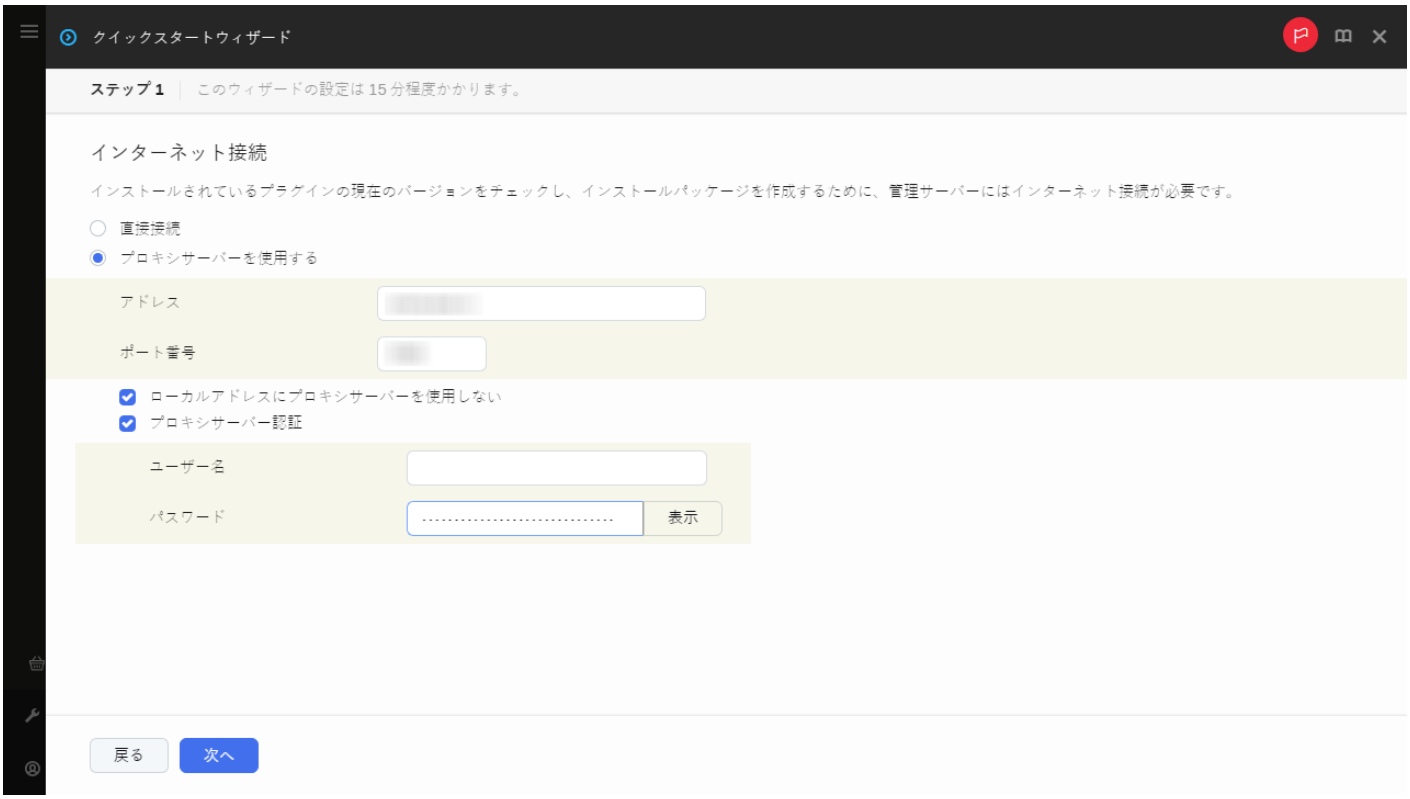
管理サーバーのプロパティウィンドウ

3. ［**クイックスタートウィザードを開始**］をクリックします。

管理サーバーの初期設定を実行するように指示されます。ウィザードの指示に従ってください。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

ステップ1：インターネット接続設定の指定

管理サーバーのインターネットアクセスを設定します。Kaspersky Security Network を使用し、Kaspersky Security Center 向けおよび管理対象カスペルスキー製品向けの定義データベースのアップデートをダウンロードするには、インターネットアクセスを設定する必要があります。



インターネット接続設定

インターネットへの接続時にプロキシサーバーを使用する場合は、［**プロキシサーバーを使用する**］をオンにします。このオプションをオンにすると、設定を入力するフィールドが使用可能になります。プロキシサーバーの接続を次のように設定します：

- **アドレス**

  インターネットへの Kaspersky Security Center の接続に使用するプロキシサーバーのアドレス。

- **ポート番号**

  Kaspersky Security Center でプロキシサーバーへの接続を確立するポートの番号。

- **ローカルアドレスにプロキシサーバーを使用しない**

  ローカルネットワークのデバイスへの接続にプロキシサーバーを使用しません。

- **プロキシサーバー認証**

  このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。
  ［**プロキシサーバーを使用する**］をオンにすると、この入力フィールドが使用可能になります。

- **ユーザー名**

  プロキシサーバーへの接続の確立に使用されるユーザーアカウント（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

- **パスワード**

  プロキシサーバーへの接続の確立に使用されるアカウントのユーザーが設定したパスワード（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

  入力したパスワードを表示するには、確認する間だけ［**入力した文字を表示する**］をクリックしたままにします。

クイックスタートウィザードを使用せずに、後からインターネットアクセスを設定することもできます。

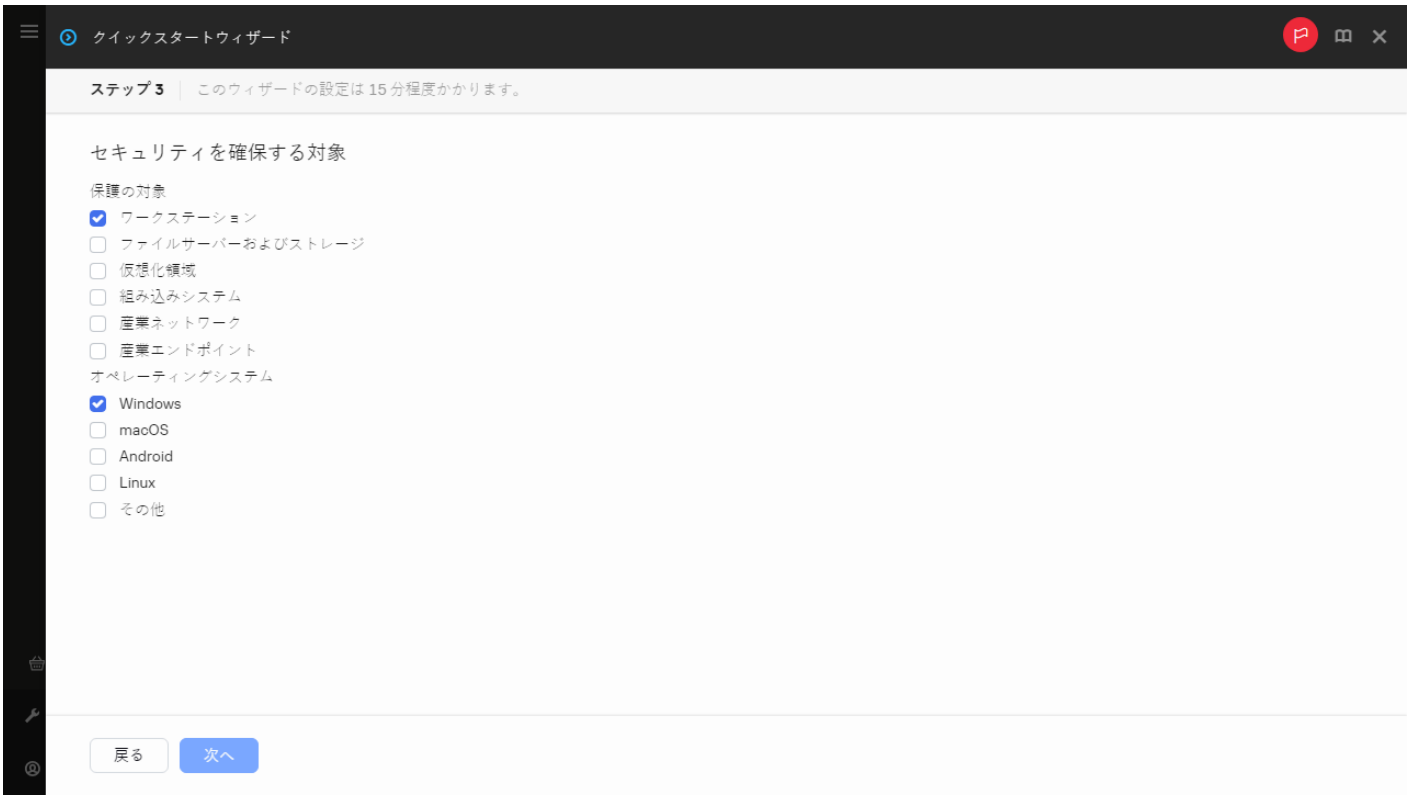
ステップ 2：必要なアップデートのダウンロード

必要なアップデートはカスペルスキーのアップデートサーバーから自動的にダウンロードされます。

必要なアップデートのダウンロード

ステップ 3：保護する資産の選択

所属組織のネットワークで保護対象範囲とオペレーティングシステムを選択します。これらの項目を選択することによって、ネットワーク内のクライアントデバイスにインストールするためにカスペルスキーのサーバーからダウンロードできる管理プラグインと配布パッケージが絞り込まれます。



保護する資産の選択

オプションを選択します：

- **保護の対象**

次の保護領域を選択できます：

- **ワークステーション**：組織ネットワーク内のワークステーションを保護する場合はこのオプションをオンにします。既定では、［ワークステーション］はオンです。
- **ファイルサーバーおよびストレージ**：組織ネットワーク内のファイルサーバーを保護する場合はこのオプションをオンにします。
- **モバイルデバイス**：会社所有または従業員所有のモバイルデバイスを保護する場合はこのオプションをオンにします。モバイルデバイス管理機能をサポートするライセンスを追加していない状態でこのオプションを選択した場合、モバイルデバイス管理機能をサポートするライセンスを追加する必要性を通知するメッセージが表示されます。ライセンスを追加しない場合、モバイルデバイス機能を使用することはできません。
- **仮想化領域**。組織ネットワーク内の仮想マシンを保護する場合はこのオプションをオンにします。
- **Kaspersky Anti-Spam**：メールサーバーをスパムや詐欺、マルウェアから保護する場合はこのオプションを選択します。
- **組み込みシステム**。Automated Teller Machine（ATM）などの Windows ベースの組み込みシステムを保護する場合は、このオプションをオンにします。
- **産業ネットワーク**。産業用ネットワーク全体およびカスペルスキー製品によって保護されているネットワークエンドポイントからのセキュリティデータを監視する場合は、このオプションをオンにします。
- **産業エンドポイント**。産業用ネットワーク内の個々のノードを保護する場合は、このオプションをオンにします。

- **オペレーティングシステム**

次のプラットフォームを選択できます：

- Microsoft Windows
- macOS
- Android
- Linux
- その他

サポートされているオペレーティングシステムの詳細は、「Kaspersky Security Center Web コンソールのシステム要件」を参照してください。

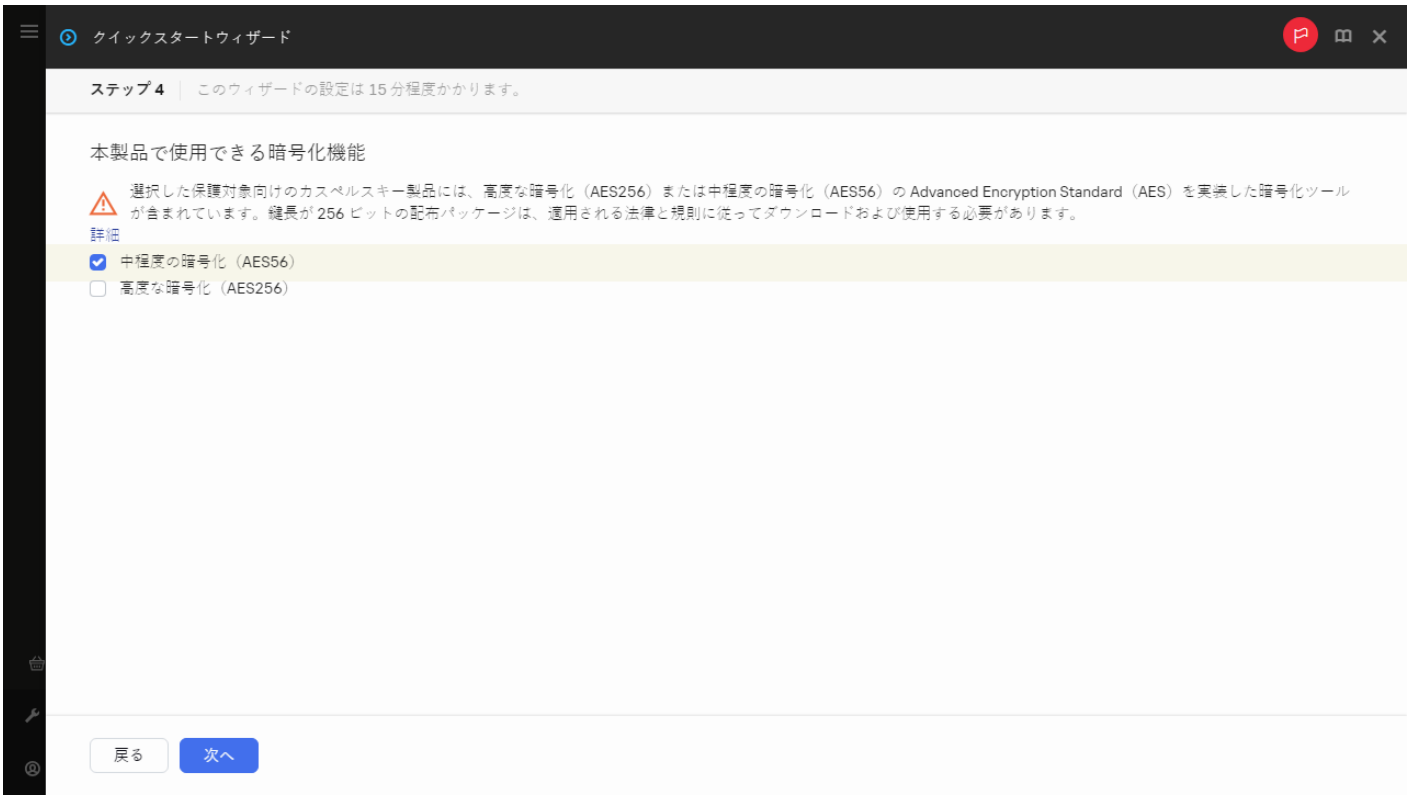
クイックスタートウィザードを使用せずに、後からカスペルスキー製品パッケージを使用可能なパッケージのリストから選択できます。必要なパッケージを検索しやすくするために、さまざまな基準に従って使用可能なパッケージのリストをフィルタリングできます。

ステップ 4：ソリューションでの暗号化の選択

［**本製品で使用できる暗号化機能**］ウィンドウは、保護範囲として［**ワークステーション**］を選択した場合にのみ表示されます。

Kaspersky Endpoint Security for Windows は、Windows ベースのクライアントデバイスに保存されている情報を暗号化する機能を備えています。これには、256 ビットまたは 56 ビットの鍵長を実装した Advanced Encryption Standard（AES）を備えた暗号化ツールが含まれます。

256 ビットの鍵長を持つ配布パッケージのダウンロードと使用は、適用法令および規制に従って実行する必要があります。組織のニーズに合致した Kaspersky Endpoint Security for Windows の配布パッケージをダウンロードするには、組織内のクライアントデバイスの所在地における法令などを確認してください。



ソリューションでの暗号化の選択

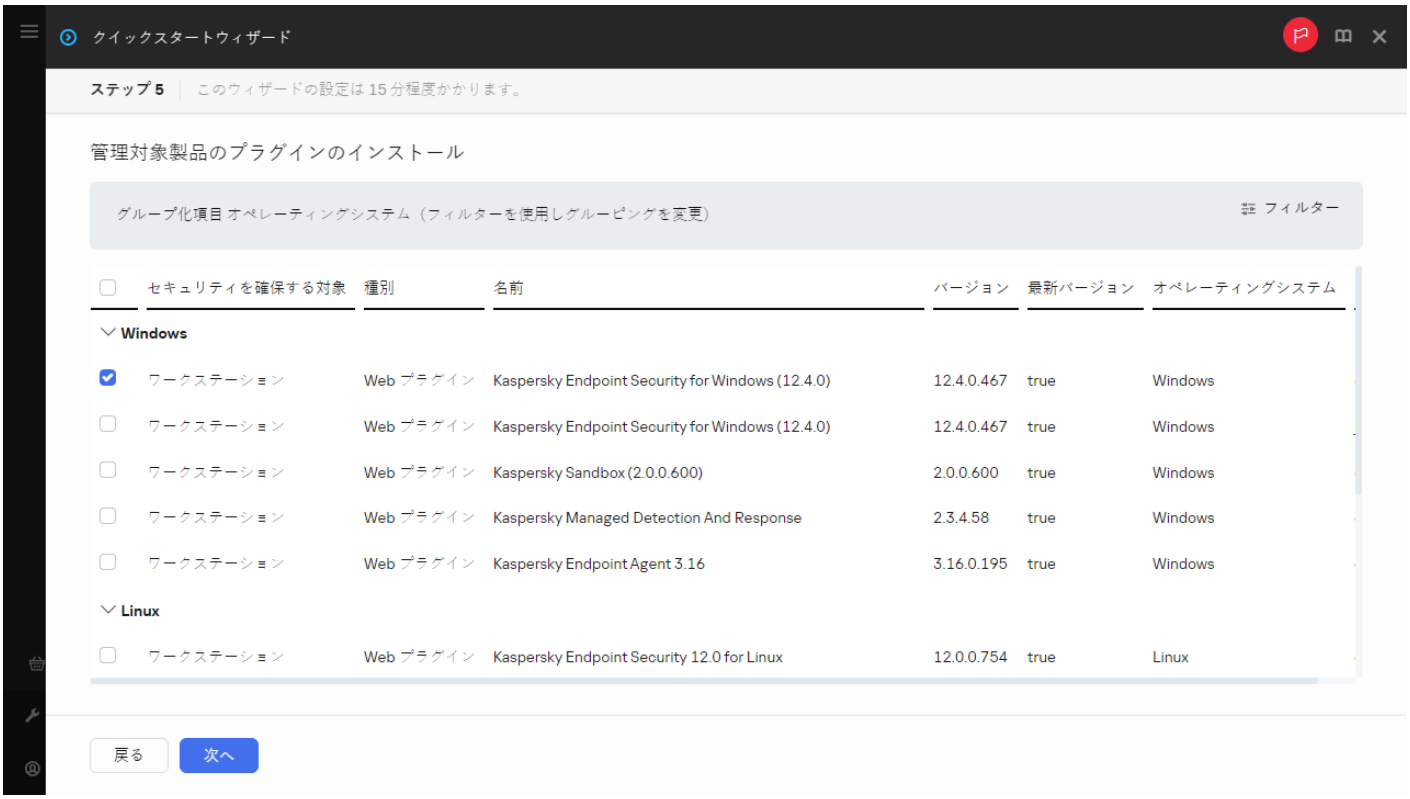
［**本製品で使用できる暗号化機能**］ウィンドウで、次のいずれかの暗号化種別を選択します：

- 中程度の暗号化。この暗号化種別では、56 ビットの鍵長が使用されます。
- 高度な暗号化。この暗号化種別では、256 ビットの鍵長が使用されます。

Kaspersky Endpoint Security for Windows の配布パッケージは、後でクイックスタートウィザードとは別に、必要な暗号化タイプで選択できます。

ステップ 5：管理対象製品のプラグインのインストールの設定

インストールする管理対象製品のプラグインを選択します。カスペルスキーのサーバーから利用できるプラグインのリストが表示されます。リストは、ウィザードの前のステップで選択されたオプションに従ってフィルタリングされます。既定では、このリストではプラグインのすべての言語バージョンが表示されます。特定の言語バージョンのみを対象にプラグインを表示するには、フィルターを使用します。



管理対象製品のプラグインのインストール

プラグインのリストには次の列が含まれます：

- **セキュリティを確保する対象**

  保護するために選択された領域がこの列に表示されます。

- **種別**

  プラグインの種類がこの列に表示されます。

- **名前**

  前のステップで選択した保護領域とプラットフォームに応じて、対応するプラグインが選択されています。

- **バージョン**

  リストには、カスペルスキーのサーバーから利用できるすべてのバージョンのプラグインが含まれています。既定では、最新バージョンのプラグインが選択されています。

- **最新バージョン**

  この列は、プラグインのバージョンが最新かどうかを示します。**true** 値が表示されている場合、対応するプラグインは最新バージョンです。**false** 値が表示された場合、対応するプラグインのバージョンが新しいことを示しています。

- **オペレーティングシステム**

この列には、プラグインのオペレーティングシステムが表示されます。

- **言語**

  既定では、インストール時に選択した Kaspersky Security Center の言語に応じてプラグインのローカリゼーション言語も選択されます。［**管理コンソールの言語または次の言語で表示**］ドロップダウンリストで、その他の言語を指定することもできます。

プラグインを選択したら、［**次へ**］をクリックしてインストールを開始します。

クイックスタートウィザードとは別に、カスペルスキー製品の管理プラグインを手動でインストールできます。

クイックスタートウィザードは、選択したプラグインを自動的にインストールします。一部のプラグインのインストールでは使用許諾契約書に同意する必要があります。使用許諾契約書の内容を確認し、同意する場合は［**Kaspersky Security Network への参加に同意する**］をオンにして［**インストール**］をクリックします。使用許諾契約書の条項に同意しない場合、プラグインはインストールされません。

選択したすべてのプラグインがインストールされると、クイックスタートウィザードが自動的に次のステップに進みます。

ステップ 6.選択したプラグインのインストール

クイックスタートウィザードは、前のステップで選択したプラグインを自動的にインストールします。一部のプラグインのインストールでは使用許諾契約書に同意する必要があります。使用許諾契約書の内容を確認し、同意する場合は［**Kaspersky Security Network への参加に同意する**］をオンにして［**インストール**］をクリックします。使用許諾契約書の条項に同意しない場合、プラグインはインストールされません。

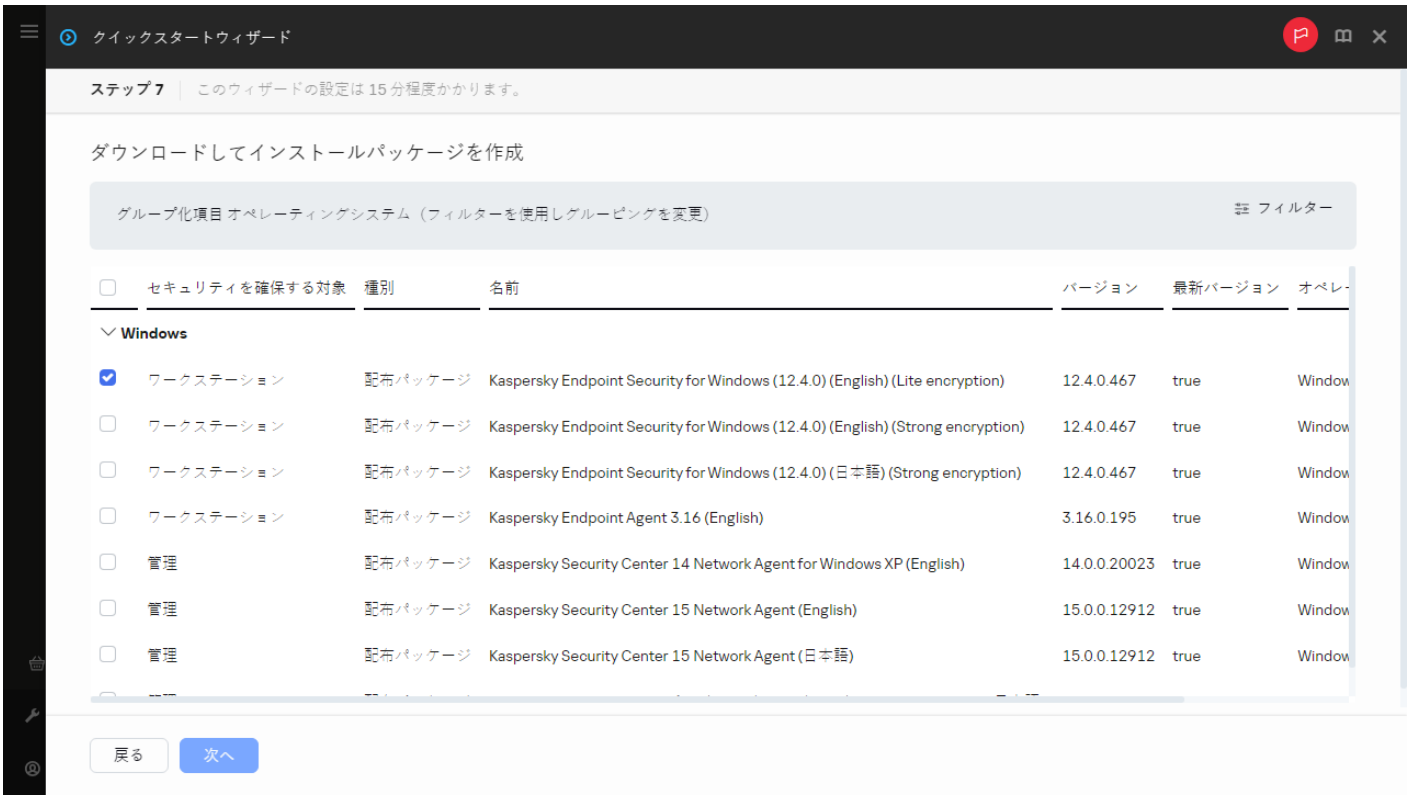
選択したすべてのプラグインがインストールされると、クイックスタートウィザードが自動的に次のステップに進みます。

ステップ 7：配布パッケージのダウンロードとインストールパッケージの作成

ダウンロードする配布パッケージを選択します。

管理対象製品の配布パッケージには、Kaspersky Security Center の特定の最小バージョンをインストールする必要がある場合があります。

Kaspersky Endpoint Security for Windows の暗号化種別を選択すると、両方の暗号化種別のバージョンの配布パッケージのリストが表示されます。選択した暗号化種別の配布パッケージがリストで選択されています。任意の暗号化種別の配布パッケージを選択できます。配布パッケージの言語は Kaspersky Security Center の言語に対応するものが選択されます。Kaspersky Security Center の言語に対応する Kaspersky Endpoint Security for Windows の配布パッケージが存在しない場合、英語版の配布パッケージが選択されます。



配布パッケージのダウンロードとインストールパッケージの作成

一部の配布パッケージのダウンロードを完了させるには、使用許諾契約書に同意する必要があります。［**同意する**］をクリックすると、使用許諾契約書の条項が表示されます。ウィザードの次のステップに進むには、使用許諾契約書の条項とカスペルスキーのプライバシーポリシーの条項に同意する必要があります。パッケージのダウンロードに必要な条項に同意しない場合、パッケージのダウンロードはキャンセルされます。

使用許諾契約書の条項とカスペルスキーのプライバシーポリシーの条項への同意が完了すると、配布パッケージのダウンロードが引き続き実行されます。インストールパッケージを使用して、後でカスペルスキー製品をクライアントデバイスに導入できます。

クイックスタートウィザードとは別に、配布パッケージをダウンロードして、後でインストールパッケージを作成できます。

ステップ 8：Kaspersky Security Network の設定

Kaspersky Security Center の動作に関する情報を Kaspersky Security Network ナレッジベースに転送する設定を指定します。

Kaspersky Security Network の設定

次のいずれかのオプションをオンにします：

- **Kaspersky Security Network への参加に同意する**

  Kaspersky Security Center とクライアントデバイスにインストールされている管理対象製品は、自動的に動作情報を Kaspersky Security Network に送信します。Kaspersky Security Network への参加により、ウイルスなどの脅威に関する情報を含んだデータベースのアップデートをより迅速に入手できるため、セキュリティへの緊急の脅威にすぐに対応できます。

- **Kaspersky Security Network への参加に同意しない**

  Kaspersky Security Center と管理対象製品は、Kaspersky Security Network に対して情報を提供しません。
  このオプションをオンにすると、Kaspersky Security Network の使用がオフになります。

クイック スタート ウィザードとは別に、後で Kaspersky Security Network（KSN）へのアクセスを設定できます。

ステップ 9：アプリケーションのアクティベート方法の選択

Kaspersky Security Center のアクティベーションオプションのいずれかを選択します：

- **アクティベーションコードを入力**

*アクティベーションコード*は、英数字 20 文字の一意な並びで構成されます。アクティベーションコードを入力すると、Kaspersky Security Center をアクティベートするライセンス情報を追加することができます。アクティベーションコードは、Kaspersky Security Center を購入すると、指定したメールアドレスに届きます。

アクティベーションコードを使用して製品をアクティベートするには、カスペルスキーのアクティベーションサーバーと接続を確立するためのインターネット接続が必要です。

このアクティベーションオプションを選択すると、［**管理対象デバイスにライセンスを自動配信する**］を有効にできます。

このオプションを有効にすると、ライセンスが管理対象デバイスに自動的に適用されます。

このオプションが無効になっている場合、管理コンソールツリーの［**カスペルスキーのライセンス**］フォルダーで、後で管理対象デバイスにライセンスを適用できます。

- **ライセンス情報ファイルを指定**

*ライセンス情報ファイル*は、拡張子「key」のファイルであり、カスペルスキーから提供されます。ライセンス情報ファイルを製品に追加し、製品をアクティベートする目的で作成されています。

ライセンス情報ファイルの取得方法については、次の［ライセンス情報ファイルについて］セクションで説明します。

ライセンス情報ファイルでのアクティベーション時には、カスペルスキーのアクティベーションサーバーへの接続は必要ありません。

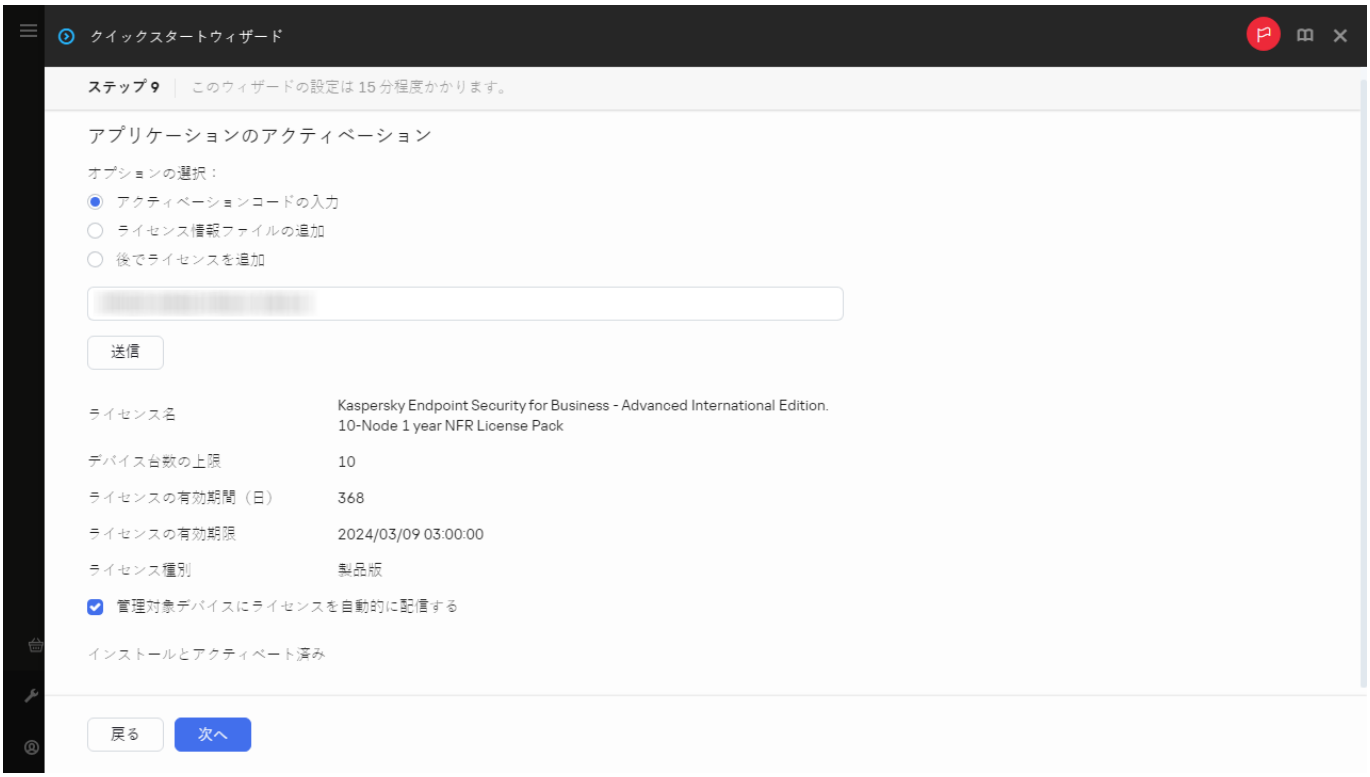
このアクティベーションオプションを選択すると、［**管理対象デバイスにライセンスを自動配信する**］を有効にできます。

このオプションを有効にすると、ライセンスが管理対象デバイスに自動的に適用されます。

このオプションが無効になっている場合、管理コンソールツリーの［**カスペルスキーのライセンス**］フォルダーで、後で管理対象デバイスにライセンスを適用できます。

- **アプリケーションのアクティベーションを後で実行**

アプリケーションは基本機能のみが使用できる状態で動作し、モバイルデバイス管理および脆弱性とパッチ管理機能は利用できません。



アプリケーションのアクティベート方法の選択

アプリケーションのアクティベーションを延期する場合は、メニューの［**操作**］→［**ライセンス管理**］を選択して後でいつでもライセンスを追加できます。

有料 AMI または月単位の従量課金の SKU から導入した Kaspersky Security Center で作業を行う場合は、ライセンス情報ファイルを指定したりアクティベーションコードを入力することはできません。

ステップ 10：ステップ 9：サードパーティ製品のアップデート管理設定の指定

脆弱性とパッチ管理が使用可能なライセンスをお持ちでなく、［*脆弱性とアプリケーションのアップデートの検索*］タスクが既に存在している場合、このステップは表示されません。

サードパーティ製品のアップデート管理設定

サードパーティ製ソフトウェアのアップデートの場合は、次のいずれかのオプションを選択します：

- **必要なアップデートの検索**

  *脆弱性とアプリケーションのアップデートの検索*タスクがない場合は、自動的に作成されます。
  既定ではこのオプションが選択されます。

- **必要なアップデートの検索とインストール**

  ［*脆弱性とアプリケーションのアップデートの検索*］タスクと［*アップデートのインストールと脆弱性の修正*］タスクがまだ作成されていない場合は、自動的に作成されます。

  この機能は、脆弱性とパッチ管理が使用可能なライセンスでのみ使用できます。

Windows Update 更新プログラムの場合は、次のオプションのいずれかを選択します：

- **ドメインポリシーで定義されたアップデート元を使用する**

  クライアントデバイスは、ドメインポリシー設定に従って Windows Update 更新プログラムをダウンロードします。ネットワークエージェントポリシーがまだ作成されていない場合は、自動的に作成されます。

- **管理サーバーを WSUS サーバーとして使用する**

  クライアントデバイスは、管理サーバーから Windows Update 更新プログラムをダウンロードします。［*Windows Update の同期の実行*］タスクとネットワークエージェントポリシーがまだ作成されていない場合は、自動的に作成されます。

  この機能は、脆弱性とパッチ管理が使用可能なライセンスでのみ使用できます。

クイックスタートウィザードとは別に、［*脆弱性と必要な更新プログラムの検索*］および［*必要な更新プログラムのインストールと脆弱性の修正*］タスクを作成できます。管理サーバーを WSUS サーバーとして使用するには、［*Windows Update の同期の実行*］タスクを作成してから、ネットワークエージェントのポリシーで［**管理サーバーを WSUS サーバーとして使用する**］をオンにする必要があります。

ステップ 11：基本的なネットワーク保護の設定情報の作成

作成されたポリシーとタスクのリストを確認できます。

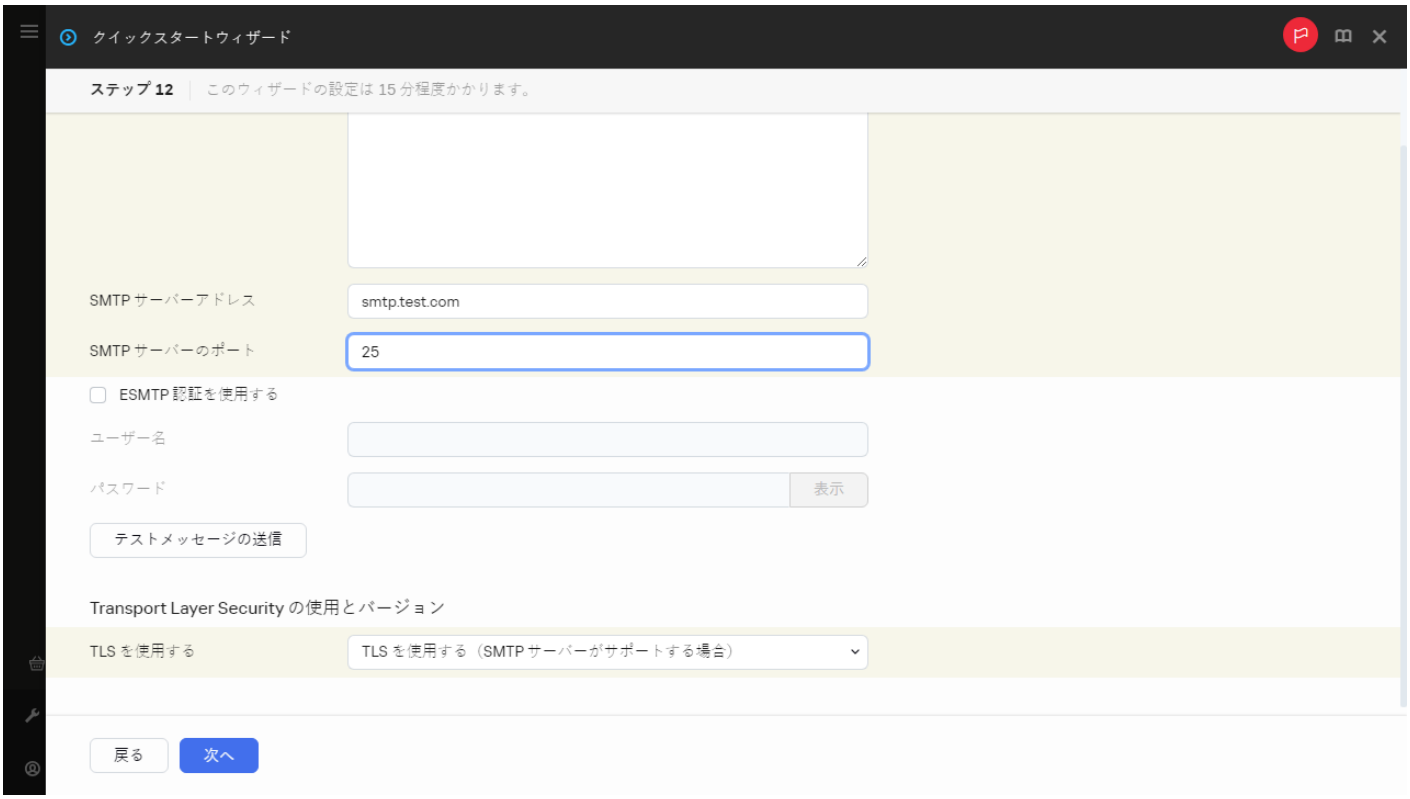
ポリシーとタスクの作成が完了してから、ウィザードの次のステップに進んでください。

基本的なネットワーク保護の設定情報の作成

クイックスタートウィザードを使用せずに、必要なタスクとポリシーを後で作成することもできます。

ステップ 12：メール通知の設定

クライアントデバイス上のカスペルスキー製品の実行中に登録されたイベントに関する通知の配信方法を設定します。この設定は、アプリケーションポリシーの既定の設定として使用されます。



メール通知の設定

カスペルスキー製品で発生したイベントに関する通知の配信を設定するには、次の設定を使用します：

- **受信者（メールアドレス）**

  通知が送られるユーザーのメールアドレスです。1つ以上のアドレスを入力できます。複数のアドレスを入力する場合はセミコロンで区切ってください。

- **SMTP サーバーアドレス**

  組織のメールサーバーのアドレスです。
  複数のアドレスを入力する場合はセミコロンで区切ってください。次の値を使用できます：
  - IPv4 / IPv6 アドレス
  - デバイスの Windows ネットワーク名（NetBIOS 名）
  - SMTP サーバーの DNS 名

- **SMTP サーバーのポート**

  SMTP サーバーの通信ポート番号。複数の SMTP サーバーを使用する場合、それらサーバーへの接続は指定された通信ポートを介して確立されます。既定のポート番号は 25 です。

- **ESMTP 認証を使用する**

  ESMTP 認証のサポートを有効にします。チェックボックスをオンにすると、［**ユーザー名**］と［**パスワード**］で ESMTP 認証を設定できます。既定では、このチェックボックスはオフです。

- **TLS を使用する**

  SMTP サーバーとの接続の TLS 設定を指定できます：

  - **TLS を使用しない**

    メールの暗号化を無効にする場合に、このオプションを選択できます。

  - **TLS を使用する（SMTP サーバーがサポートする場合）**

    SMTP サーバーに TLS 接続を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは TLS を使用せずに SMTP サーバーへ接続します。

  - **TLS を常に使用し、サーバー証明書の有効性をチェックする**

    TLS 認証設定を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは SMTP サーバーへ接続できません。

    > SMTP サーバーの接続の保護をより強化する目的で、このオプションを使用することを推奨します。このオプションを選択すると、TLS 接続の認証設定を指定できます。

    ［**TLS を常に使用し、サーバー証明書の有効性をチェックする**］の値を選択する場合は、SMTP サーバーの認証用の証明書を指定し、TLS の任意のバージョンを介した通信を有効にするか、TLS 1.2 以降のバージョンのみを介した通信を有効にするかを選択できます。また、SMTP サーバーでクライアント認証に使用する証明書を指定することもできます。

  ［**証明書を指定**］をクリックして TLS 接続用の証明書を指定できます。

  - SMTP サーバーの証明書ファイルを参照します：

    信頼できる証明書認証局から証明書のリストを含むファイルを受け取り、ファイルを管理サーバーへアップロードできます。Kaspersky Security Center は、SMTP サーバーの証明書も信頼できる証明書認証局によって署名されているかどうかをチェックします。信頼できる証明書認証局から SMTP サーバーの証明書を受け取っていない場合、Kaspersky Security Center は SMTP サーバーに接続できません。

  - クライアント証明書ファイルを参照します：

    信頼できる認証局など、任意の発行元から受け取った証明書を使用できます。次のいずれかの証明書タイプを使用して、証明書とその秘密鍵を指定する必要があります：

    - X-509証明書：

      証明書を含むファイルと秘密鍵を含むファイルを指定する必要があります。両方のファイルは相互に依存せず、ファイルを読み込む順序は重要ではありません。両方のファイルを読み込む時は、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

    - pkcs12 コンテナー：

      証明書とその秘密鍵を含む単一のファイルをアップロードする必要があります。ファイルの読み込み時に、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

［**テストメッセージの送信**］をクリックして、新しいメール通知設定をテストできます。

クイックスタートウィザードを使用せずに、後からイベント通知を設定することもできます。

ステップ 13：ネットワークポーリングの実行

管理サーバーが最初のポーリングを実行します：ポーリングの実行中、進捗バーが表示されます。ポーリングが完了すると、［**検出されたデバイスの表示**］が利用可能になります。このリンクをクリックすると、管理サーバーによって検出されたネットワークデバイスを表示できます。クイックスタートウィザードに戻るには、**Escape** キーを押します。

クイックスタートウィザードを使用せずに、後からネットワークのポーリングを行うこともできます。Kaspersky Security Center Web コンソールを使用して、ドメインコントローラー、Windows ドメイン、IP 範囲、および IPv6 ネットワークのポーリングを設定します。

ステップ 14：クイックスタートウィザードの終了

ネットワーク内のデバイスへのアンチウイルス製品またはネットワークエージェントの自動インストールを開始する場合は、クイックスタートウィザードの完了ウィンドウで［**製品導入ウィザードを開始する**］をオンにします。

クイックスタートウィザードの最終手順

ウィザードを終了するには、［**終了**］をクリックします。

モバイルユーザーデバイスの接続

このセクションでは、モバイルユーザーデバイス（メインネットワークの外部にある管理対象デバイス）を管理サーバーに接続する方法について説明します。

シナリオ：接続ゲートウェイを使用したモバイルユーザーデバイスの接続

このシナリオでは、メインネットワークの外部にある管理対象デバイスを管理サーバーに接続する方法について説明します。

必須条件

シナリオには次の前提条件があります：

- 非武装地帯（DMZ）が組織のネットワークに編成されていること。
- Kaspersky Security Center 管理サーバーが企業ネットワークに導入されていること。

実行するステップ

このシナリオは段階的に進行します：

1. **DMZ 内のクライアントデバイスの選択**

   このデバイスは接続ゲートウェイとして使用されます。選択するデバイスは、接続ゲートウェイの要件を満たしている必要があります。

2. **接続ゲートウェイのロールへのネットワークエージェントのインストール**

   ローカルインストールを使用して、選択したデバイスにネットワークエージェントをインストールすることを推奨します。

   既定では、インストールファイルは次の場所にあります：\\<サーバー名>\KLSHARE\PkgInst\NetAgent_<バージョン番号>

   ネットワークエージェントのセットアップウィザードの［**接続ゲートウェイ**］ウィンドウで、［**DMZ 内でネットワークエージェントを接続ゲートウェイとして使用する**］を選択します。このモードは同時に接続ゲートウェイのロールをアクティブにし、管理サーバーからの接続を待機するようにネットワークエージェントに指示します。管理サーバーへの接続の確立は指示しません。

   または、Linux デバイスにネットワークエージェントをインストールし、ネットワークエージェントを接続ゲートウェイとして動作するように設定することも可能です。ただし、Linux デバイスで実行されるネットワークエージェントの制限事項のリストを確認しておく必要があります。

3. **接続ゲートウェイのファイアウォールにおける接続の許可**

   管理サーバーが実際に DMZ の接続ゲートウェイに接続できることを確認するには、管理サーバーと接続ゲートウェイの間のすべてのファイアウォールで TCP ポート 13000 への接続を許可します。

   接続ゲートウェイがインターネット上に実際の IP アドレスを持たず、ネットワークアドレス変換（NAT）を使用している場合は、NAT を介して接続を転送するルールを設定します。

4. **外部デバイスの管理グループの作成**

   管理対象デバイスグループの下に新しいグループを作成します。この新しいグループには、外部の管理対象デバイスを含めます。

5. **接続ゲートウェイの管理サーバーへの接続**

設定した接続ゲートウェイは、管理サーバーからの接続を待機しています。ただし、管理サーバーは、管理対象デバイス間の接続ゲートウェイを使用するデバイスを一覧表示しません。これは、接続ゲートウェイが管理サーバーへの接続確立を試行していないためです。したがって、管理サーバーが接続ゲートウェイへの接続を開始するようにするには、特別な手順が必要です。

次の手順に従います：

1. 接続ゲートウェイをディストリビューションポイントとして追加します。
2. **未割り当てデバイス**から、外部デバイス用に作成したグループに接続ゲートウェイを移動します。

接続ゲートウェイが接続および設定されます。

6 管理サーバーへの外部デスクトップコンピューターの接続

通常、外部デスクトップコンピューターは境界の内側に移動されません。したがって、ネットワークエージェントのインストール時に、ゲートウェイを介して管理サーバーに接続するように設定する必要があります。

7 外部デスクトップコンピューターのアップデートの設定

セキュリティ製品のアップデートが管理サーバーからダウンロードされるように設定されている場合、外部コンピューターは接続ゲートウェイを介してアップデートをダウンロードします。この方法には、2 つの欠点があります：

- これは不要なトラフィックであり、会社のインターネット通信チャネルの帯域幅を占有します。
- この方法により、アップデートの取得が必ずしも最速になるとは限りません。外部コンピューターがカスペルスキーのアップデートサーバーからアップデートを取得する方が、低コストで高速である可能性があります。

次の手順に従います：

1. 前の手順で作成した別の管理グループにすべての外部コンピューターを移動します。
2. 外部デバイスを含むグループをアップデートタスクから除外します。
3. 外部デバイスを含むグループ用に個別のアップデートタスクを作成します。

8 移動中のノート PC の管理サーバーへの接続

移動中のノート PC は、ネットワーク内に存在する場合もあれば、ネットワーク外に存在する場合もあります。効果的に管理するには、場所に応じて異なる方法で管理サーバーに接続する必要があります。トラフィックを効率的に使用するには、場所に応じて異なるアップデート元からアップデートを受信することも必要です。

次のモバイルユーザー向けのルールを設定する必要があります：接続プロファイルとネットワークロケーション記述。各ルールは、移動するノート PC が場所に応じて接続する必要がある管理サーバーのインスタンスと、アップデートの受信元とする必要がある管理サーバーのインスタンスを定義します。

シナリオ：DMZ 内のセカンダリ管理サーバーを介した社外デバイスの接続

メインネットワークの外側にある管理対象デバイスを管理サーバーに接続する場合は、非武装地帯（DMZ）にあるセカンダリ管理サーバーを使用して接続できます。

必須条件

導入を開始する前に、次が完了していることを確認してください：

- DMZ が組織内のネットワークに編成されていること。
- Kaspersky Security Center 管理サーバーが組織の内部ネットワークに導入されていること。

実行するステップ

このシナリオは段階的に進行します：

1. **DMZ 内のクライアントデバイスの選択**

   DMZ で、セカンダリ管理サーバーとして使用されるクライアントデバイスを選択します。

2. **Kaspersky Security Center 管理サーバーのインストール**

   Kaspersky Security Center 管理サーバーをクライアントデバイスにインストールします。

3. **管理サーバーの階層の作成**

   セカンダリ管理サーバーを DMZ に配置する場合、セカンダリ管理サーバーはプライマリ管理サーバーからの接続を受け取る必要があります。新規管理サーバーをセカンダリとして追加し、プライマリ管理サーバーからセカンダリ管理サーバーへポート 13000 で接続できます。2 つの管理サーバーを 1 つの階層内で組み合わせる時は、ポート 13299 が両方の管理サーバーで開放されていることを確認してください。
   Kaspersky Security Center Web コンソールは、ポート 13299 を介して管理サーバーに接続されます。

4. **社外の管理対象デバイスをセカンダリ管理サーバーに接続します**

   管理サーバーとメインネットワークにある管理対象デバイスとの間で接続を確立するのと同じ方法で、社外のデバイスを DMZ 内の管理サーバーに接続できます。社外の管理対象デバイスは、ポート 13000 を通じて接続を開始します。

モバイルユーザーデバイスの接続

一部の管理対象デバイスは、常にメインネットワークの外部に配置されています（たとえば、会社の支社にあるコンピューター、売店、ATM、様々な販売拠点に設置されている端末、従業員のホームオフィスにあるコンピューターなど）。また、一部のデバイスは、ネットワークの外部を不定期に移動しています（たとえば、支社や顧客オフィスを訪問するユーザーのノート PC など）。

モバイルユーザーデバイスの保護について、引き続き監視および管理する必要があります。保護ステータスに関する実際の情報を受け取り、デバイスのセキュリティ製品を最新の状態に保ちます。たとえば、そのようなデバイスがメインネットワークから離れている際にセキュリティ侵害を受けた場合、メインネットワークに接続するとすぐに脅威を伝播するプラットフォームになる可能性があるため、これは必要です。モバイルユーザーデバイスを管理サーバーへ接続する方法は、次の 2 つがあります：

- 非武装地帯（DMZ）にある接続ゲートウェイ

  データトラフィックのスキーム：LAN 上の管理サーバー、インターネット上の管理対象デバイス、使用中の接続ゲートウェイ

- DMZ 内の管理サーバー

  データトラフィックのスキーム：DMZ 内の管理サーバー、インターネット上の管理対象デバイス

DMZ 内の接続ゲートウェイ

モバイルユーザーデバイスから管理サーバーへの接続で推奨される方法は、DMZ を組織内に構築し、接続ゲートウェイを DMZ 内に実装することです。外部デバイスは接続ゲートウェイに接続し、ネットワーク内の管理サーバーは接続ゲートウェイを介してデバイスへの接続を開始します。

その他の方法と比較すると、この方法はより安全です。

- ネットワーク外部からの管理サーバーへのアクセスを許可する必要がありません。
- 接続ゲートウェイが攻撃された場合でも、ネットワーク上のデバイスに深刻な危険が及ぶ可能性がありません。接続ゲートウェイ自身は実際は何も管理しておらず、接続を確立することもありません。

また、接続ゲートウェイに必要なハードウェアリソースも少量です。

ただし、この方法には複雑な設定編集の手順が必要です：

- デバイスを DMZ 内で接続ゲートウェイとして動作するように設定するには、ネットワークエージェントのインストールと管理サーバーへの接続を、特定の方法で実行する必要があります。
- 同一のアドレスを、管理サーバーへの接続用に使用することができません。ネットワーク境界の外部から、異なるアドレス（接続ゲートウェイアドレス）を使用するだけでなく、接続方法も変更する必要があります：接続ゲートウェイを介した方法。
- 異なる場所にあるノート PC 用に、別の接続設定を指定する必要もあります。

以前に構成したネットワークに接続ゲートウェイを追加するには、次の手順を実行します：

1. ネットワークエージェントを接続ゲートウェイモードでインストールします。
2. 新しく追加した接続ゲートウェイに接続するデバイスにネットワークエージェントを再インストールします。

DMZ 内の管理サーバー

もう 1 つの方法は、単一の管理サーバーの DMZ 内へのインストールです。

前述の方法よりも、設定の安全性が低くなります。この方法で外部のノート PC を管理するには、インターネット上の任意のアドレスからの接続を管理サーバーが許可する必要があります。内部ネットワークのデバイスをすべて管理することも可能ですが、DMZ からの管理となります。したがって、発生の可能性は低いと言えますが、サーバーが攻撃された場合、結果として甚大な被害が発生する可能性があります。

DMZ 内の管理サーバーが内部ネットワークのデバイスを管理しない場合、この危険性は大幅に低減されます。この設定は、たとえば、顧客デバイスを管理するサービスプロバイダーなどが使用する可能性があります。

この方法の使用が検討されるのは、次のような場合があります：

- 管理サーバーのインストールと設定を熟知しており、接続ゲートウェイを別の方法でインストール、設定したくない場合。
- 管理対象デバイスの数が多い場合。管理サーバーで管理可能な台数は 100,000 台、接続ゲートウェイは 10,000 台です。

この方法には、次の欠点もあります：

- 管理サーバーに必要なハードウェアリソースが増大し、データベースも 1 個追加する必要があります。

- デバイスに関する情報が、互いに関連付けられていない 2 つのデータベースに保管されるので（ネットワーク内の管理サーバーと DMZ）、監視が困難になります。

- デバイスをすべて管理するには、管理サーバーが階層構造に属する必要があります。これにより、監視と管理の両方が複雑化されます。セカンダリ管理サーバーのインスタンスがある場合、管理グループで構築可能な構造が制限されます。タスクとポリシーを選択し、セカンダリ管理サーバーのインスタンスへの導入方法を決定する必要があります。

- DMZ 内の管理サーバーを外部から使用し、プライマリ管理サーバーを内部で使用するように外部デバイスを設定するのは、接続ゲートウェイへの接続条件を満たして使用するように設定するよりも難易度が高くなります。

- セキュリティ上の高い危険性。管理サーバーのインスタンスが攻撃されると、管理対象のノート PC をより簡単に攻撃できるようになります。この攻撃が発生すると、ノート PC のうち 1 台が企業ネットワーク内に復帰するまで待機するだけで、ローカルエリアネットワークへの攻撃を継続することが可能になります。

管理サーバーへの外部デスクトップコンピューターの接続

常にメインネットワークの外部にあるデスクトップコンピューター（たとえば、会社の支社にあるコンピューター、売店、ATM、様々な販売拠点に設置されている端末、従業員のホームオフィスにあるコンピューター）は、管理サーバーに直接接続できません。非武装地帯（DMZ）にインストールされている接続ゲートウェイを介して管理サーバーに接続する必要があります。この設定は、これらのコンピューターにネットワークエージェントをインストールする時に行われます。

外部デスクトップコンピューターを管理サーバーに接続するには：

1. ネットワークエージェントの新規インストールパッケージを作成します。

2. 作成したインストールパッケージのプロパティを開き、［**設定**］→［**詳細**］の順に選択し、［**接続ゲートウェイを使用して管理サーバーに接続する**］をオンにします。

   ［**接続ゲートウェイを使用して管理サーバーに接続する**］設定は［**DMZ 内でネットワークエージェントを接続ゲートウェイとして使用する**］設定と互換性がありません。これらの設定の両方を同時に有効にすることはできません。

3. ［**接続ゲートウェイアドレス**］フィールドで、接続ゲートウェイのパブリックアドレスを指定します。

   接続ゲートウェイがネットワークアドレス変換（NAT）の背後にあり、独自のパブリックアドレスがない場合は、接続をパブリックアドレスから接続ゲートウェイの内部アドレスに転送するための NAT ゲートウェイルールを設定します。

4. 作成したインストールパッケージに基づいて、スタンドアロンインストールパッケージを作成します。

5. スタンドアロンインストールパッケージを電子送信により、またはリムーバブルドライブによりターゲットコンピューターに配信します。

6. スタンドアロンパッケージからネットワークエージェントをインストールします。

外部デスクトップコンピューターが管理サーバーに接続されます。

モバイルユーザー用の接続プロファイルの概要

モバイルユーザー用のノートPC（以降「デバイス」とも表記）では、企業ネットワーク内でのデバイスの現在位置によっては、管理サーバーへの接続方法を変更する、または管理サーバーを切り替える必要があります。

接続プロファイルは、Windowsおよびmacosを実行しているデバイスでのみサポートされます。

単一の管理サーバーに対する異なるアドレスの使用

ネットワークエージェントがインストールされたデバイスは、組織の社内ネットワークかイントラネット経由で管理サーバーに接続できます。そのため、ネットワークエージェントは異なるアドレスを使用して管理サーバーに接続することが必要になる場合があります。つまり、インターネット経由で接続された場合は外部管理サーバーアドレス、社内ネットワーク経由で接続された場合は内部管理サーバーアドレスが使用されます。

ネットワークエージェントのポリシーのプロパティで、インターネット経由で管理サーバーに接続するプロファイルを追加します（［**アプリケーション設定**］→［**接続**］→［**接続プロファイル**］→［**管理サーバー接続プロファイル**］セクション）。次に、プロファイル作成ウィンドウで、［**アップデートの受信にのみ使用する**］をオフにし、［**このプロファイルで指定された管理サーバー設定と接続設定を同期する**］がオンになっていることを確認します。接続ゲートウェイを使用して管理サーバーにアクセスする場合（たとえば、「インターネットアクセス：DMZ内でネットワークエージェントを接続ゲートウェイとして使用する」で説明されているようなKaspersky Security Centerの設定の場合）、接続プロファイルの該当フィールドで、接続ゲートウェイのアドレスを指定する必要があります。

現在のネットワークに応じた管理サーバーの切り替え

企業に、異なる管理サーバーを使用する複数のオフィスがあり、ネットワークエージェントがインストールされた一部のデバイスが管理サーバー間を移動している場合、現在のデバイスがあるオフィスのローカルネットワークの管理サーバーに、ネットワークエージェントを接続する必要があります。

この場合、各オフィスにおいて、ネットワークエージェントのポリシーのプロパティに、管理サーバーへの接続用プロファイルを作成する必要があります。ただし、独自のホーム管理サーバーがあるホームオフィスは除きます。接続プロファイルで管理サーバーのアドレスを指定し、次のように、［**アップデートの受信にのみ使用する**］をオンまたはオフにする必要があります：

- ローカルサーバーをアップデートのダウンロードのためだけに使用する間、ネットワークエージェントをホーム管理サーバーと同期する必要がある場合は、このオプションをオンにします。
- ネットワークエージェントをローカル管理サーバーで完全に管理する必要がある場合は、このオプションをオフにします。

その後、新たに作成したプロファイルに切り替える条件を設定します。ホームオフィスを除いて、オフィスごとに少なくとも1つの条件を設定する必要があります。各条件は、オフィスのネットワーク環境特有の項目を検出することを目的とします。条件が真の場合、対応するプロファイルがアクティブになります。いずれの条件も真でない場合、ネットワークエージェントはホーム管理サーバーに切り替わります。

モバイルユーザー用の接続プロファイルの作成

管理サーバーの接続プロファイルは、Windowsおよびmacosを実行しているデバイスでのみ使用できます。

ネットワークエージェントのモバイルユーザー用管理サーバー接続プロファイルを作成するには：

1. 管理対象デバイスのグループに対して接続プロファイルを作成する場合は、このグループのネットワークエージェントのポリシーを開きます。次の操作を実行します：

   a. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。

   b. 現在のパスのリンクをクリックします。

   c. 表示されるウィンドウで、対象の管理グループを選択します。

   その後、現在のパスが変更されます。

   d. 管理対象デバイスのグループにネットワークエージェントのポリシーを追加します。すでに作成済みの場合は、ポリシーのプロパティを開くためにネットワークエージェントのポリシーの名前をクリックします。

2. 特定の管理対象デバイスに対して接続プロファイルを作成する場合は、次の操作を実行します：

   a. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

   b. 管理対象デバイスの名前をクリックします。

   c. 管理対象デバイスのプロパティウィンドウが表示されたら、［**アプリケーション**］タブをクリックします。

   d. 選択した管理対象デバイスにのみ適用するネットワークエージェントのポリシーの名前をクリックします。

3. 表示されるプロパティウィンドウで、［**アプリケーション設定**］→［**接続**］→［**接続プロファイル**］の順に選択します。

4. ［**管理サーバー接続プロファイル**］セクションで、［**追加**］をクリックします。

   既定では、接続プロファイルのリストには <オフラインモード> プロファイルと <ホーム管理サーバー> プロファイルが含まれています。プロファイルの編集や削除はできません。

   <オフラインモード> プロファイルでは接続するサーバーが指定されていません。したがって、このプロファイルに切り替わると、クライアントデバイスにインストールされたアプリケーションがモバイルユーザーポリシー下で実行されている場合、ネットワークエージェントは管理サーバーへの接続を行いません。<オフラインモード> プロファイルは、デバイスがネットワークから切断された場合に使用できます。

   <ホーム管理サーバー> プロファイルは、ネットワークエージェントのインストール中に選択された管理サーバーの接続を指定します。<ホーム管理サーバー> プロファイルは、しばらく外部ネットワークで動作していたデバイスが、ホーム管理サーバーに再接続された時に適用されます。

5. ［**プロファイルの設定**］ウィンドウが開いたら、接続プロファイルを設定します：

   - **プロファイル名**

     この入力フィールドでは、接続プロファイル名を表示または変更できます。

   - **管理サーバーアドレス**

     プロファイルの有効化時にクライアントデバイスが接続する管理サーバーのアドレス。

   - **ポート番号**

接続に使用されるポート番号。

- **SSL ポート**

  SSL プロトコルを使用する接続のポート番号。

- **SSL 接続を使用する**

  このオプションをオンにすると、SSL プロトコルを使用してセキュアなポート経由で接続が確立されます。

  既定では、このオプションはオンです。セキュアな接続を保つために、このオプションを無効にしないことを推奨します。

- インターネットへの接続時にプロキシサーバーを使用する場合は、［**プロキシサーバーを使用する**］をオンにします。このオプションをオンにすると、設定を入力するフィールドが使用可能になります。プロキシサーバーの接続を次のように設定します：

  - **アドレス**

    インターネットへの Kaspersky Security Center の接続に使用するプロキシサーバーのアドレス。

  - **ポート番号**

    Kaspersky Security Center でプロキシサーバーへの接続を確立するポートの番号。

  - **プロキシサーバー認証**

    このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。

  - **ユーザー名**

    プロキシサーバーへの接続の確立に使用されるユーザーアカウント（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

  - **パスワード**

    プロキシサーバーへの接続の確立に使用されるアカウントのユーザーが設定したパスワード（［**プロキシサーバー認証**］をオンにした場合に有効になります）。

    入力したパスワードを表示するには、確認する間だけ［**表示**］をクリックしたままにします。

- **接続ゲートウェイアドレス**

  クライアントデバイスが管理サーバーに接続する場合に使用するゲートウェイのアドレス。

- **管理サーバーが使用できない時にモバイルユーザーモードを有効にする**

このチェックボックスをオンにすると、クライアントデバイスにインストールされているアプリケーションは、管理サーバーが使用できない場合の接続試行で、モバイルユーザーモードのデバイス向けのポリシーのプロファイル、およびモバイルユーザー用ポリシーを使用できます。モバイルユーザーポリシーがアプリケーションに対して定義されていない場合は、アクティブポリシーが使用されます。

このオプションを無効にすると、アプリケーションはアクティブポリシーを使用します。

既定では、このチェックボックスはオフです。

- **アップデートの受信にのみ使用する**

  このオプションをオンにすると、クライアントデバイスにインストールされているアプリケーションによってアップデートがダウンロードされる場合にのみプロファイルが使用されます。その他の処理では、ネットワークエージェントのインストール時に定義された初期接続設定で管理サーバーへの接続が確立されます。

  既定では、このオプションはオンです。

- **このプロファイルで指定された管理サーバー設定と接続設定を同期する**

  このオプションをオンにすると、ネットワークエージェントはプロファイルのプロパティで指定された設定を使用して管理サーバーに接続します。

  このオプションをオフにすると、ネットワークエージェントはインストール時に指定された元の設定を使用して管理サーバーに接続します。

  このオプションは、［**アップデートの受信にのみ使用する**］を無効にすると使用可能になります。

  既定では、このオプションはオフです。

ネットワークエージェントを管理サーバーに接続する、モバイルユーザー用のプロファイルが作成されます。ネットワークエージェントがこのプロファイルを使用して管理サーバーに接続すると、クライアントデバイスにインストールされたアプリケーションは、モバイルユーザーモードのデバイス用のポリシーまたはモバイルユーザーポリシーを使用します。

ネットワークエージェントの別の管理サーバーへの切り替えについて

Kaspersky Security Center では、次のネットワーク設定が変更された場合、クライアントデバイスのネットワークエージェントを別の管理サーバーに切り替えることができます：

- **DHCP サーバーアドレスの条件** – ネットワークの DHCP（Dynamic Host Configuration Protocol）サーバーの IP アドレスが変更された場合。
- **デフォルト接続ゲートウェイアドレスの条件** – メインネットワークゲートウェイのアドレスが変更された場合。
- **DNS ドメインの条件** – サブネットの DNS サフィックスが変更された場合。
- **DNS サーバーアドレスの条件** – ネットワークの DNS サーバーの IP アドレスが変更された場合。
- **WINS サーバーアドレスの条件** – ネットワークの WINS サーバーの IP アドレスが変更された場合。この設定は Windows を実行しているデバイスでのみ使用可能です。

- **名前解決の条件** – クライアントデバイスの DNS または NetBIOS 名が変更された場合。
- **サブネットの条件** – サブネットアドレスとマスクが変更された場合。
- **Windows ドメインのアクセス可否の条件** – クライアントデバイスが接続している Windows ドメインのステータスが変更された場合。この設定は Windows を実行しているデバイスでのみ使用可能です。
- **SSL 接続アドレスのアクセス可否の条件** – クライアントデバイスは、（選択したオプションによって）指定されたサーバー（name：port）との SSL 接続を確立できる場合とできない場合があります。サーバーごとに、SSL 証明書を追加で指定できます。この場合、ネットワークエージェントは、SSL 接続の機能をチェックすることに加えて、サーバー証明書を検証します。証明書が一致しない場合、接続は失敗します。

この機能は、Windows または macOS を実行しているデバイスにインストールされているネットワークエージェントでのみサポートされます。

ネットワークエージェントから管理サーバーへの接続の既定の設定は、ネットワークエージェントのインストール時に定義されます。その後、ネットワークエージェントを他の管理サーバーに切り替えるルールが作成されると、次のようにネットワークエージェントがネットワーク設定の変更に対応します：

- 作成されたルールの 1 つをネットワーク設定が満たす場合、ネットワークエージェントはそのルールで指定された管理サーバーに接続します。クライアントデバイスにインストールされたアプリケーションは、モバイルユーザーポリシーへの切り替えがルールで認められている場合、モバイルユーザーポリシーに切り替わります。
- どのルールも満たされなくなった場合、ネットワークエージェントはインストール時に指定された管理サーバーへの既定の接続設定に戻します。クライアントデバイスにインストールされたアプリケーションは、アクティブポリシーに戻ります。
- 管理サーバーに接続できない場合、ネットワークエージェントはモバイルユーザーポリシーを使用します。

ネットワークエージェントがモバイルユーザーポリシーに切り替わるのは、［**管理サーバーが使用できない時にモバイルユーザーモードを有効にする**］がネットワークエージェントのポリシー設定でオンになっている場合のみです。

ネットワークエージェントの管理サーバーへの接続設定は接続プロファイルに保存されます。接続プロファイルでは、クライアントデバイスをモバイルユーザーポリシーに切り替えるルールを作成したり、プロファイルをアップデートのダウンロード専用に設定したりすることができます。

ネットワークの場所によるネットワークエージェント切り替えルールの作成

ネットワークロケーションに基づくネットワークエージェント切り替えは、Windows または macOS を実行しているデバイスでのみ使用できます。

ネットワーク設定が変更された場合に、ある管理サーバーから別の管理サーバーにネットワークエージェントを切り替えるルールを作成するには：

1. 管理対象デバイスのグループに対してルールを作成する場合は、このグループのネットワークエージェントのポリシーを開きます。次の操作を実行します：

a. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。

b. 現在のパスのリンクをクリックします。

c. 表示されるウィンドウで、対象の管理グループを選択します。

その後、現在のパスが変更されます。

d. 管理対象デバイスのグループにネットワークエージェントのポリシーを追加します。すでに作成済みの場合は、ポリシーのプロパティを開くためにネットワークエージェントのポリシーの名前をクリックします。

2. 特定の管理対象デバイスに対してルールを作成する場合は、次の操作を実行します：

a. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

b. 管理対象デバイスの名前をクリックします。

c. 管理対象デバイスのプロパティウィンドウが表示されたら、［**アプリケーション**］タブをクリックします。

d. 選択した管理対象デバイスにのみ適用するネットワークエージェントのポリシーの名前をクリックします。

3. 表示されるプロパティウィンドウで、［**アプリケーション設定**］→［**接続**］→［**接続プロファイル**］の順に選択します。

4. ［**ネットワークロケーションの設定**］セクションで、［**追加**］をクリックします。

5. プロパティウィンドウが表示されたら、ネットワークロケーションの説明と切り替えルールを設定します。次のネットワークロケーションの説明に関する設定を指定します：

- **説明**

  ネットワークロケーションの説明の名前は 255 字以内とし、特殊文字（例：`"*<>?\/:|`）を含むことはできません。

- **接続プロファイルの使用**

  このドロップダウンリストで、ネットワークエージェントが管理サーバーへの接続に使用する接続プロファイルを指定できます。ネットワークロケーションの説明の条件が一致すると、このプロファイルが使用されます。この接続プロファイルには、ネットワークエージェントから管理サーバーへの接続に関する設定が含まれ、クライアントデバイスがモバイルユーザーポリシーに切り替える条件も定義されています。このプロファイルは、アップデートをダウンロードする場合にのみ使用されます。

- **記述を有効にする**

  チェックボックスをオンにして新しいネットワークロケーションの説明を使用できるようにします。

6. ネットワークエージェント切り替えルールの条件を選択します：

- **DHCP サーバーアドレスの条件** – ネットワークの DHCP（Dynamic Host Configuration Protocol）サーバーの IP アドレスが変更された場合。
- **デフォルト接続ゲートウェイアドレスの条件** – メインネットワークゲートウェイのアドレスが変更された場合。
- **DNS ドメインの条件** – サブネットの DNS サフィックスが変更された場合。
- **DNS サーバーアドレスの条件** – ネットワークの DNS サーバーの IP アドレスが変更された場合。
- **WINS サーバーアドレスの条件** – ネットワークの WINS サーバーの IP アドレスが変更された場合。この設定は Windows を実行しているデバイスでのみ使用可能です。
- **名前解決の条件** – クライアントデバイスの DNS または NetBIOS 名が変更された場合。
- **サブネットの条件** – サブネットアドレスとマスクが変更された場合。
- **Windows ドメインのアクセス可否の条件** – クライアントデバイスが接続している Windows ドメインのステータスが変更された場合。この設定は Windows を実行しているデバイスでのみ使用可能です。
- **SSL 接続アドレスのアクセス可否の条件** – クライアントデバイスは、（選択したオプションによって）指定されたサーバー（name：port）との SSL 接続を確立できる場合とできない場合があります。サーバーごとに、SSL 証明書を追加で指定できます。この場合、ネットワークエージェントは、SSL 接続の機能をチェックすることに加えて、サーバー証明書を検証します。証明書が一致しない場合、接続は失敗します。

ルールに複数の条件がある場合、論理演算子「AND」を使用して組み合わせられます。ネットワークロケーションの記述により切り替えルールを適合させるには、すべてのルール切り替え条件を満たす必要があります。

7. 条件セクションで、ネットワークエージェントを別の管理サーバーに切り替える時間を指定します。このため、［**追加**］をクリックして条件の値を設定します。

   また、［**リストにある値のいずれかと一致する**］オプションは既定でオンになっています。条件がすべての指定した値と一致する必要がある場合はこのオプションをオフにしてください。

8. 変更を保存します。

ネットワークロケーションの記述ごとに新しい切り替えルールが作成されます。ルールの条件が満たされるたびに、ネットワークエージェントはルールで指定された接続プロファイルを使用して管理サーバーに接続します。

製品導入ウィザード

カスペルスキー製品をインストールするには、製品導入ウィザードを使用できます。製品導入ウィザードにより、専用に作成されたインストールパッケージを使用するか、または配布パッケージから直接、アプリケーションをリモートインストールすることができます。

製品導入ウィザードにより、次の操作が実行できます：

- アプリケーションをインストールするためのインストールパッケージをダウンロードします（まだ作成されていない場合）。［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移

動すると、インストールパッケージにアクセスできます。今後アプリケーションをインストールする時に、このインストールパッケージを使用できます。

- 特定のデバイスまたは管理グループに対するリモートインストールタスクを作成して実行します。新しく作成されたリモートインストールタスクは、［**タスク**］セクションに保存されます。このタスクは後から手動で開始できます。タスクの種別は［**アプリケーションのリモートインストール**］になります。

SUSE Linux Enterprise Server 15 オペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントの設定前に、insserv-compat パッケージをインストールします。

製品導入ウィザードの開始

製品導入ウィザードを手動で起動するには：

メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**製品導入ウィザード**］の順に移動します。

製品導入ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

ステップ 1：インストールパッケージの選択

インストールする製品のインストールパッケージを選択します。

目的の製品のインストールパッケージがリストに含まれていない場合、［**追加**］をクリックしてリストから製品を選択します。

ステップ 2：ライセンス情報ファイルまたはアクティベーションコードの配信方法の選択

ライセンス情報ファイルまたはアクティベーションコードの配信方法を選択します：

- **インストールパッケージにライセンスを含めない**

  次の条件を満たす場合、ライセンスは互換性のあるすべてのデバイスへ自動的に配信されます：
  - ライセンスのプロパティで［自動配信］が有効になっている場合。
  - ［**ライセンスの追加**］タスクが作成されている場合。

- **インストールパッケージにライセンスを含める**

ライセンスはインストールパッケージと共にデバイスへ配信されます。

共有読み取りアクセス権がインストールパッケージのリポジトリに対して有効になっているため、この方法はできるだけ使用しないでください。

インストールパッケージに既にライセンス情報ファイルまたはアクティベーションコードが含まれる場合も、同様のウィンドウが表示されますが、ライセンスの情報のみが表示されます。

ステップ 3：ネットワークエージェントのバージョンの選択

ネットワークエージェント以外の製品のインストールパッケージを選択した場合でも、各製品と Kaspersky Security Center 管理サーバーとを接続するために、ネットワークエージェントのインストールが必要になります。

最新バージョンのネットワークエージェントを選択してください。

ステップ 4：デバイスの選択

アプリケーションをインストールするデバイスを指定します。

- **管理対象デバイスにインストール**

  このオプションをオンにすると、デバイスのグループに対してリモートインストールタスクが作成されます。

- **インストールするデバイスの選択**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

ステップ 5：リモートインストールタスクの設定

［**リモートインストールタスク設定**］ウィンドウで、アプリケーションのリモートインストール設定を指定します。

［**インストールパッケージの強制ダウンロード**］セクションで、アプリケーションのインストールに必要なファイルをクライアントデバイスに配布する方法を指定します。

- **ネットワークエージェントを使用する**

このオプションをオンにすると、インストールパッケージのクライアントデバイスへの配布は、クライアントデバイスにインストールされたネットワークエージェントによって行われます。

このオプションをオフにすると、インストールパッケージはクライアントデバイスのオペレーティングシステムのツールを使用して配信されます。

ネットワークエージェントがインストールされたデバイスにタスクが割り当てられている場合は、このチェックボックスをオンにすることを推奨します。

既定では、このオプションはオンです。

- **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**

このオプションをオンにすると、ディストリビューションポイントがオペレーティングシステムのツールを使用してインストールパッケージをクライアントデバイスに送信します。この機能が使用できるのは、ネットワークに少なくとも1つのディストリビューションポイントがある場合です。

［**ネットワークエージェントを使用する**］をオンにすると、ネットワークエージェントのツールが使用できない場合に限り、ファイルがオペレーティングシステムのツールで配布されます。

既定では、仮想管理サーバーで作成されたリモートインストールタスクに対して、このオプションはオンです。

- **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**

このオプションをオンにすると、管理サーバーを通じてクライアントデバイスのオペレーティングシステムツールを使用してクライアントデバイスにファイルが送信されます。このオプションは、クライアントデバイスにネットワークエージェントがインストールされていないものの、クライアントデバイスが管理サーバーと同じネットワークに存在する場合にオンにできます。

既定では、このオプションはオンです。

詳細設定を行います：

- **アプリケーションが既にインストールされている場合再インストールしない**

このオプションをオンにすると、選択したアプリケーションがクライアントデバイスに既にインストールされていた場合、インストールされません。

このオプションをオフにすると、アプリケーションは常にインストールされます。

既定では、このオプションはオンです。

- **Active Directory のグループポリシーにパッケージのインストールを割り当てる**

このオプションをオンにすると、Active Directory のグループポリシーを使用してインストールパッケージがインストールされます。

このオプションは、ネットワークエージェントのインストールパッケージが選択されている場合に使用可能になります。

既定では、このオプションはオフです。

ステップ 6：再起動の設定

アプリケーションの使用中、インストール中、アンインストール中にオペレーティングシステムの再起動が必要になった場合に行う動作を指定します。

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

  - **通知の繰り返し間隔（分）**

    このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

    既定では、このオプションはオンです。既定の間隔は 5 分です。1分から 1,440 分までの値を指定できます。

    このオプションをオフにすると、確認メッセージは1回だけ表示されます。

  - **再起動するまでの時間（分）**

    ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

    既定では、このオプションはオンです。既定の間隔は 30 分です。1分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

既定では、このオプションはオフです。

ステップ 7：インストール前に競合アプリケーションを削除する

この手順の実施ウィンドウは、インストール対象の製品に既知の競合アプリケーションが存在する場合にのみ表示されます。

インストール対象の製品と互換性がないアプリケーションを自動的に削除するには、オプションをオンにします。

互換性がない競合アプリケーションのリストも表示されます。

このオプションをオフにした場合、インストール対象の製品は、競合アプリケーションがインストールされていないデバイスにのみインストールされます。

ステップ 8：管理対象デバイスへのデバイスの移動

ネットワークエージェントのインストール後に、デバイスを管理グループに移動するかどうかを指定します。

- **デバイスを移動しない**

  デバイスは、現在配置されているグループから移動しません。どのグループにも割り当てられていないデバイスは、未割り当てのままとなります。

- **未割り当てデバイスをグループへ移動**

  指定した管理グループにデバイスが移動されます。

既定では［**デバイスを移動しない**］がオンになっています。セキュリティ上の理由のため、場合によってはデバイスを手動で移動する必要があります。

ステップ 9：デバイスにアクセスするアカウントの選択

必要に応じて、リモートインストールタスクの開始に使用するアカウントを追加できます：

- **アカウントが不要（ネットワークエージェントインストール済み）**

  このオプションをオンにすると、アプリケーションのインストーラーを実行するアカウントを指定する必要はありません。タスクは管理サーバーのサービスを実行しているアカウントで実行されます。

  クライアントデバイスにネットワークエージェントがインストールされていない場合、このオプションは使用できません。

- **アカウントが必要（ネットワークエージェントの使用なし）**

  リモートインストールタスクを割り当てるデバイスにネットワークエージェントがインストールされていない場合は、このオプションをオンにします。この場合、ユーザーアカウントを指定して、アプリケーションをインストールできます。

  アプリケーションインストーラーを実行するユーザーアカウントを指定するには、［**追加**］をクリックし、［**ローカルアカウント**］を選択して、ユーザーアカウントの資格情報を指定します。

  タスクを割り当てるすべてのデバイスで必要なすべての権限をどのアカウントも持たない場合などのために、複数のユーザーアカウントを追加できます。この場合、追加されたすべてのアカウントが上から下へ順番に使用され、タスクが実行されます。

ステップ 10：インストールの開始

このウィンドウがこのウィザードでの最後のステップです。このステップを完了すると、**リモートインストールタスク**の作成と設定が完了します。

既定では、［**ウィザードの終了後にタスクを実行**］はオフになっています。このオプションをオンにすると、ウィザードの完了後すぐに**リモートインストールタスク**が開始されます。このオプションをオフにすると、**リモートインストールタスク**は開始されません。このタスクは後から手動で開始できます。

製品導入ウィザードを完了するには、［OK］をクリックします。

カスペルスキー製品：Kaspersky Security Center Web コンソールを使用した導入

このセクションでは、Kaspersky Security Center Web コンソールを使用して、企業ネットワーク内のクライアントデバイスにカスペルスキー製品を導入する方法について説明しています。

シナリオ：Kaspersky Security Center Web コンソールを使用したカスペルスキー製品の導入

このシナリオは、Kaspersky Security Center Web コンソールを使用したカスペルスキー製品の導入方法を説明しています。導入には、クイックスタートウィザードと製品導入ウィザードを使用する方法と、すべての必要なステップを手動で完了させる方法があります。

次の製品は、Kaspersky Security Center Web コンソールを使用して導入できます：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

実行するステップ

カスペルスキー製品の導入シナリオは、以下の手順で進みます：

1. **アプリケーションの管理プラグインのダウンロード**

   このステップはクイックスタートウィザードの一部として実行できます。ウィザードを実行しない場合は、Kaspersky Endpoint Security for Windows のプラグインを手動でダウンロードします。

   企業のモバイルデバイスを管理する場合は、Kaspersky Security for Mobile のヘルプの手順に従って Kaspersky Endpoint Security for Android の管理プラグインをダウンロードしインストールしてください。

2. **インストールパッケージのダウンロードと作成**

   このステップはクイックスタートウィザードの一部として実行できます。

   クイックスタートウィザードを使用すると、管理プラグインと一緒にインストールパッケージをダウンロードできます。ウィザードの実行中にこのオプションを選択しない場合は、手動でパッケージをダウンロードする必要があります。

   Kaspersky Security Center を使用してカスペルスキー製品をインストールできないデバイスがある場合（リモートワークで働く従業員のデバイスなど）、製品のスタンドアロンインストールパッケージを作成できます。スタンドアロンパッケージを使用してカスペルスキー製品をインストールする場合、リモートインストールタスクを作成して実行したり、Kaspersky Endpoint Security for Windows のタスクを作成、設定したりする必要はありません。

3. **リモートインストールタスクの作成、設定、実行**

   Kaspersky Endpoint Security for Windows では、この段階は製品導入ウィザードの一部となっており、クイックスタートウィザードの終了後に自動的に開始されます。製品導入ウィザードを実行しない場合は、手動でこのタスクを作成して設定する必要があります。

   異なる管理グループや異なるデバイスの抽出を対象に、複数のリモートインストールタスクを手動で作成することもできます。これらのタスクでは、同一製品の異なるバージョンを導入できます。

   ネットワーク上ですべてのデバイスが検出済みであることを確認してから、リモートインストールタスクを実行します。

   > SUSE Linux Enterprise Server 15 オペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントの設定前に、insserv-compat パッケージをインストールします。

4. **管理対象アプリケーションのタスクの作成と設定**

   Kaspersky Endpoint Security for Windows の *アップデートインストールタスク*を設定する必要があります。

   この段階はクイックスタートウィザードの一部です：既定の設定を使用してタスクは自動的に作成、設定されます。ウィザードを実行しない場合は、手動でこのタスクを作成して設定する必要があります。クイックスタートウィザードを使用する場合、タスクのスケジュールが要件を満たすことを確認してください（既定では、タスクの実行予定は［**手動**］に設定されていますが、別のオプションも選択できます）。

   他のカスペルスキー製品には、別の既定のタスクがある場合があります。詳細については、該当する製品のドキュメントを参照してください。

   作成した各タスクのスケジュールがお客様の要件に合致しているかを確認します。

5. **Kaspersky Security for Mobile のインストール（省略可能）**

企業のモバイルデバイスを管理する場合は、Kaspersky Security for Mobile のヘルプの手順に従って Kaspersky Endpoint Security for Android を導入してください。

6. **ポリシーの作成**

   アプリケーションごとに手動または（Kaspersky Endpoint Security for Windows の場合）クイックスタートウィザードを使用してポリシーを作成します。ポリシーは既定の設定を使用できます。また、いつでも必要に応じてポリシーの既定の設定を変更できます。

7. **結果の検証**

   導入が正しく完了しているかの確認：アプリケーションごとにポリシーとタスクが設定済みで、これらのアプリケーションが管理対象デバイスにインストールされていることを確認します。

結果

これらのステップがすべて完了すると、次の状態を実現できます：

- すべての必要なポリシーとタスクが、選択したアプリケーションに対して作成されている。
- タスクのスケジュールが必要に応じて設定されている。
- 指定したデバイス上で、選択したアプリケーションが導入されているか、導入スケジュールが設定されている。

カスペルスキー製品のプラグインの取得

Kaspersky Endpoint Security for Windows などのカスペルスキー製品を導入するには、製品の管理プラグインをダウンロードする必要があります。

カスペルスキー製品の管理プラグインをダウンロードするには：

1. メインメニューで［**設定**］→［**Web プラグイン**］の順に移動します。

2. ウィンドウが表示されたら、［**追加**］をクリックします。
   使用可能なプラグインのリストが表示されます。

3. 使用可能なプラグインのリストから、プラグイン名（「Kaspersky Endpoint Security 11 for Windows」など）をクリックしてダウンロードするプラグインを選択します。
   プラグインの説明ページが表示されます。

4. プラグインの説明ページで、［**プラグインのインストール**］をクリックします。

5. インストールが完了したら、［**OK**］をクリックします。

管理プラグインが既定の設定でダウンロードされ、管理プラグインのリストに表示されます。

ファイルからプラグインを追加したり、ダウンロードされたプラグインをアップデートすることができます。管理プラグインと Web 管理プラグインは、Kaspersky のテクニカルサポートサイトウェブページからダウンロードできます。

ファイルからプラグインをダウンロードまたはアップデートするには：

1. メインメニューで［**設定**］→［**Web プラグイン**］の順に移動します。

2. 次のいずれかの手順を実行します：

   - ［**ファイルから追加**］をクリックしてファイルからプラグインをダウンロードします。

   - ［**ファイルからアップデート**］をクリックしてファイルからプラグインのアップデートをダウンロードします。

3. ファイルおよびファイルの署名を指定します。

4. 指定したファイルをダウンロードします。

管理プラグインがファイルからダウンロードされ、管理プラグインのリストに表示されます。

カスペルスキー製品のインストールパッケージのダウンロードおよび作成

管理サーバーがインターネットにアクセスできる場合、カスペルスキーの Web サーバーからカスペルスキー製品のインストールパッケージを作成できます。

カスペルスキー製品のインストールパッケージのダウンロードと作成を実行するには：

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に選択します。

   - メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

画面表示による通知のリストでも、カスペルスキー製品の新しいパッケージに関する通知を確認できます。新しいパッケージに関する通知が表示されている場合、通知に隣接するリンクをクリックし、使用可能なインストールパッケージのリストを表示できます。

管理サーバーで利用可能なインストールパッケージのリストが表示されます。

2. ［**追加**］をクリックします。

新規パッケージウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ［**カスペルスキー製品のインストールパッケージを作成する**］を選択します。

カスペルスキーの Web サーバーで使用可能なインストールパッケージのリストが表示されます。リストには、Kaspersky Security Center の現在のバージョンと互換性のあるアプリケーションのインストールパッケージのみが含まれています。

4. インストーパッケージの名前（たとえば「Kaspersky Endpoint Security for Windows (11.1.0)」など）をクリックします。

インストールパッケージに関する情報を確認できるウィンドウが表示されます：

> 適用法令および規則に準拠している場合、高度な暗号化を実装する暗号化ツールを含むインストールパッケージをダウンロードして使用できます。組織のニーズに合致した Kaspersky Endpoint Security for Windows のインストールパッケージをダウンロードするには、組織内のクライアントデバイスの所在地における法令などを確認してください。

5. 情報を確認し、［**ダウンロードしてインストールパッケージを作成**］をクリックします。

配布パッケージをインストールパッケージに変換できない場合、［**配布パッケージをダウンロード**］の代わりに［**ダウンロードしてインストールパッケージを作成**］が表示されます。

インストールパッケージ（または配布パッケージ）の管理サーバーへのダウンロードが開始されます。ウィザードのウィンドウを閉じるか、手順の次のステップに進むことができます。ウィザードのウィンドウを閉じると、ダウンロードプロセスはバックグラウンドモードで続行されます。

インストールパッケージのダウンロードプロセスを追跡する場合：

a. メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］→［**実行中**（）］の順に選択します。

b. 操作の進捗状況を表の［**ダウンロードの進行状況**］列と［**ダウンロード状況**］列で追跡します。

プロセスが完了すると、インストールパッケージが［**ダウンロード済み**］タブのリストに追加されます。ダウンロードプロセスが停止し、ダウンロードの状況が［**使用許諾契約書に同意する**］に切り替わったら、インストールパッケージ名をクリックして、手順の次のステップに進みます。

> 選択した配布パッケージ内のデータサイズが現在の上限を超えている場合、エラーメッセージが表示されます。上限の値を変更し、インストールパッケージの作成に進んでください。

6. 一部のカスペルスキー製品では、ダウンロードプロセスの途中で［**使用許諾契約書を表示**］が表示されます。この場合は、次の操作を実行します：

a. ［**使用許諾契約書を表示**］をクリックし、使用許諾契約書（EULA）の内容を確認します。

b. 画面に表示された EULA の内容を確認し、［**同意する**］をクリックします。

使用許諾契約書に同意するとダウンロードを進めることができます。［**同意しない**］をクリックすると、ダウンロードが中止されます。

7. ダウンロードが完了したら、［**閉じる**］をクリックします。

選択したインストールパッケージが管理サーバーの共有フォルダーのパッケージ用サブフォルダーにダウンロードされます。ダウンロード後、インストールパッケージがインストールパッケージのリストに表示されます。

カスタムインストールパッケージのデータサイズの上限の変更

カスタムインストールパッケージの作成中に展開されるデータサイズの総量には上限があります。既定の制限は 1 GB です。

現在設定されている上限値を超えるサイズのデータが含まれる圧縮ファイルをアップロードしようとすると、エラーメッセージが表示されます。サイズが大きい配布パッケージからインストールパッケージを作成する場合は、上限値を増やす必要が生じる場合があります。

カスタムインストールパッケージのサイズの上限値を変更するには：

1. 管理サーバーデバイスで、管理サーバーのインストールに使用したアカウントでコマンドプロンプトを実行します。
2. カレントディレクトリを Kaspersky Security Center のインストールフォルダ（通常は <ディスク>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center）に変更します。
3. 管理サーバーのインストールの種別に応じて、管理者権限を使用して次のいずれかのコマンドを入力します：

   - 通常のローカルインストール：

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <バイト数>
     ```

   - Kaspersky Security Center のフェールオーバークラスターのインストール：

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <バイト数> --stp klfoc
     ```

   - Windows Server のフェールオーバークラスターへのインストール：

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <バイト数> --stp cluster
     ```

   <バイト数> は、16 進数または 10 進数形式のバイト数です。

   たとえば、必要な制限が 2 GB の場合、10 進値 2147483648 または 16 進値 0x80000000 を指定できます。この場合、管理サーバーのローカルインストールでは、次のコマンドを使用できます：

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

カスタムインストールパッケージのデータサイズの上限が変更されます。

カスペルスキー製品の配布パッケージのダウンロード

Kaspersky Security Center Web コンソールを使用して、カスペルスキー製品の配布パッケージをダウンロードし、保存できます。配布パッケージを使用すると、Kaspersky Security Center を使用せずに手動でカスペルスキー製品をインストールできます。

カスペルスキー製品の配布パッケージをダウンロードして保存するには：

1. メインメニューで、［**操作**］→［**カスペルスキー製品**］→［**現在の製品バージョン**］の順に移動します。

   使用可能な配布パッケージ、プラグイン、パッチのリストが表示されます。Kaspersky Security Center は、現在のバージョンと互換性のある項目のみを表示します。

2. ダウンロードするパッケージの名前をクリックします。

   パッケージの説明が表示されます。

3. 説明内容を確認し、［**ダウンロードしてインストールパッケージを作成**］をクリックします。

   配布パッケージをインストールパッケージに変換できない場合、［**配布パッケージをダウンロード**］のかわりに［**ダウンロードしてインストールパッケージを作成**］が表示されます。

   インストールパッケージ（または配布パッケージ）の管理サーバーへのダウンロードが開始されます。

選択したインストールパッケージ（または配布パッケージ）が管理サーバーの共有フォルダーのパッケージ用サブフォルダーにダウンロードされます。ダウンロード後、インストールパッケージがインストールパッケージのリストに表示されます。

Kaspersky Endpoint Security が正常に導入されたことを確認する

Kaspersky Endpoint Security などのカスペルスキー製品を意図した通りに導入できているかを確認するには：

1. Kaspersky Security Center Web コンソールを使用して、次のオブジェクトが存在することを確認します：

   - 使用しているカスペルスキー製品（Kaspersky Endpoint Security など）のポリシー。
   - Kaspersky Endpoint Security for Windows のタスク：*簡易スキャンタスクとアップデートのインストール*タスク（Kaspersky Endpoint Security for Windows を使用している場合）。
   - 使用しているその他のカスペルスキー製品のタスク。

2. インストール対象として選択した管理対象デバイスのうち1台で、次のことを確認します：

   - インストール対象として選択した Kaspersky Endpoint Security またはその他のカスペルスキー製品がインストールされている。
   - Kaspersky Endpoint Security のファイル脅威対策、ウェブ脅威対策、メール脅威対策の設定が、該当デバイスを対象とするポリシーの設定と一致する。
   - Kaspersky Endpoint Security サービスを手動で停止したり起動できる。
   - グループタスクを手動で停止したり起動できる。

スタンドアロンインストールパッケージの作成

組織内の管理者とユーザーがデバイスに手動でアプリケーションをインストールするために、スタンドアロンインストールパッケージを使用できます。

スタンドアロンパッケージは実行ファイル形式（installer.exe）で、Web サーバーや共有フォルダーへの配置などによりクライアントデバイスに受け渡すことができます。クライアントデバイスで受け取った実行ファイルをローカルで起動することで、Kaspersky Security Center を使用せずにアプリケーションをインストールすることが可能となります。カスペルスキー製品および Windows、macOS、Linux プラットフォーム用のサードパーティ製品のスタンドアロンインストールパッケージを作成できます。サードパーティ製品のインストールパッケージを作成するには、カスタムインストールパッケージを作成する必要があります。

スタンドアロンインストールパッケージは、権限のないユーザーからアクセスできないようにしてください。

スタンドアロンインストールパッケージを作成するには：

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に選択します。
   - メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

   管理サーバーで利用可能なインストールパッケージのリストが表示されます。

2. インストールパッケージのリストでインストールパッケージを選択し、リストの上にある［**製品の導入**］をクリックします。

3. ［**スタンドアロンパッケージを使用**］を選択します。

   スタンドアロンインストールパッケージ作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

4. 選択したアプリケーションとネットワークエージェントを合わせてインストールする場合、［**このアプリケーションと同時にネットワークエージェントをインストールする**］がオンになっていることを確認します。

   既定では、このオプションはオンです。デバイスにネットワークエージェントがインストール済みかどうかが不明な場合は、このオプションをオンにすることを推奨します。ネットワークエージェントがデバイスにインストールされている場合、ネットワークエージェントを含めたスタンドアロンインストールパッケージのインストール後に、ネットワークエージェントが新しいバージョンにアップデートされます。

   このオプションがオフの場合、デバイスにはネットワークエージェントはインストールされず、デバイスは管理対象外のデバイスになります。

   選択したアプリケーションのスタンドアロンインストールパッケージが既に管理サーバー上に存在する場合、ウィザードに通知が表示されます。この場合、次のいずれかのオプションを選択する必要があります：

   - **スタンドアロンインストールパッケージの作成**：新しいバージョンのアプリケーションのスタンドアロンインストールパッケージを新規に作成し、なおかつ以前のバージョンのアプリケーションで作成したスタンドアロンインストールパッケージも保持する場合などにこのオプションをオンにします。新しいスタンドアロンインストールパッケージは別のフォルダーに配置されます。
   - **既存のスタンドアロンインストールパッケージを使用**：既存のスタンドアロンインストールパッケージを使用する場合は、このオプションをオンにします。パッケージの作成プロセスは開始されません。
   - **既存のスタンドアロンインストールパッケージを再構築**：同じアプリケーションのインストールパッケージを再作成する場合、このオプションを選択します。スタンドアロンインストールパッケージは、同じフォルダーに保存されます。

5. ［**管理対象デバイスのリストへ移動**］ステップで、既定では［**デバイスを移動しない**］がオンになっています。ネットワークエージェントのインストール後にクライアントデバイスをどの管理グループにも移動

させたくない場合は、このオプションをオンのままにします。

ネットワークエージェントのインストール後にクライアントデバイスを移動したい場合は、［**未割り当てデバイスをこのグループへ移動**］を選択し、クライアントデバイスの移動先の管理グループを指定します。既定では、デバイスは［**管理対象デバイス**］グループに移動されます。

6. スタンドアロンインストールパッケージの作成プロセスが完了したら、［**完了**］をクリックします。

［Stand-alone Installation Package Creation Wizard］が閉じます。

スタンドアロンインストールパッケージが作成され、管理サーバーの共有フォルダーのパッケージ用のサブフォルダーにダウンロードされます。インストールパッケージのリストの上にある［**スタンドアロンパッケージリストの表示**］をクリックすると、スタンドアロンパッケージのリストを確認できます。

スタンドアロンインストールパッケージのリストの表示

スタンドアロンインストールパッケージのリストを表示し、それぞれのスタンドアロンインストールパッケージのプロパティを確認できます。

すべてのインストールパッケージについて、対応するスタンドアロンインストールパッケージのリストを表示するには：

リストの上にある［**スタンドアロンパッケージリストの表示**］をクリックします。

スタンドアロンインストールパッケージのリストで、パッケージのプロパティが次のように表示されます。

- **パッケージ名**：パッケージに含まれるアプリケーション名とバージョン番号を組み合わせて自動的に作成されるスタンドアロンインストールパッケージの名前。
- **アプリケーション名**：スタンドアロンインストールパッケージに含まれるアプリケーションの名前。
- **アプリケーションのバージョン**。
- **ネットワークエージェントのインストールパッケージ名**。このプロパティは、スタンドアロンインストールパッケージにネットワークエージェントが含まれる場合にのみ表示されます。
- **ネットワークエージェントのバージョン**。このプロパティは、スタンドアロンインストールパッケージにネットワークエージェントが含まれる場合にのみ表示されます。
- **サイズ**：ファイルのサイズ（MB 単位）。
- **グループ**：ネットワークエージェントのインストール後にクライアントデバイスが移動する管理グループの名前。
- **作成日時**：スタンドアロンインストールパッケージが作成された日時。
- **変更日時**：スタンドアロンインストールパッケージが変更された日時。
- **パス**：スタンドアロンインストールパッケージが保存されているフォルダーのパス。
- **URL**：スタンドアロンインストールパッケージをダウンロードできる URL。
- **ファイルのハッシュ**：このプロパティは、スタンドアロンインストールパッケージが第三者による改竄を受けておらず、管理者が作成してユーザーに送信したのと同じファイルがユーザーの手元にあるかどうか

を検証するために使用します。

特定のインストールパッケージについて、対応するスタンドアロンインストールパッケージのリストを表示するには：

リストからインストールパッケージを選択し、リストの上にある［**スタンドアロンパッケージリストの表示**］をクリックします。

スタンドアロンインストールパッケージのリストを使用して、次の操作を実行できます：

- ［**公開**］をクリックして、スタンドアロンインストールパッケージを Web サーバーに公開する。スタンドアロンインストールパッケージへのリンクを管理者から受け取ったユーザーは、公開されたスタンドアロンインストールパッケージをダウンロードできます。
- ［**公開の取り消し**］をクリックして、スタンドアロンインストールパッケージの Web サーバーへの公開を中止する。公開を取り消したスタンドアロンインストールパッケージは、取り消し操作を行った管理者およびその他の管理者しかダウンロードできません。
- ［**ダウンロード**］をクリックして、スタンドアロンインストールパッケージを操作中のデバイスにダウンロードする。
- ［**メールで送信**］をクリックして、スタンドアロンインストールパッケージへのリンクをメールで送信する。
- ［**削除**］をクリックして、スタンドアロンインストールパッケージを削除する。

カスタムインストールパッケージの作成

以下のような用途でカスタムインストールパッケージを使用できます：

- タスクなどを使用して、サードパーティ製を含む任意のアプリケーション（例：テキストエディター）をクライアントデバイスにインストールするため。
- スタンドアロンインストールパッケージを作成するため。

カスタムインストールパッケージは、複数のファイルを含んだフォルダーです。カスタムインストールパッケージは、*圧縮ファイル*を元に作成します。圧縮ファイルには、カスタムインストールパッケージに含める必要のあるファイルが含まれているようにします。カスタムインストールパッケージを作成するときに、コマンドラインのパラメータを指定できます（例：製品をサイレントモードでインストールするためのパラメータ）。

脆弱性とパッチ管理（VAPM）機能の有効なライセンスをお持ちの場合は、関連するカスタムインストールパッケージの既定のインストール設定を変換し、カスペルスキーのエキスパートが推奨する値を使用できます。対応する実行ファイルが、サードパーティ製品の定義データベースに含まれている場合にのみ、カスタムインストールパッケージの作成中に設定が自動的に変換されます。

カスタムインストールパッケージを作成するには：

1. 次のいずれかの手順を実行します：
   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動します。

- メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

管理サーバーで利用可能なインストールパッケージのリストが表示されます。

2. ［**追加**］をクリックします。

新規パッケージウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ［**インストールパッケージをファイルから作成する**オンにします。

4. パッケージ名を指定して、［**参照**］をクリックします。

ブラウザーで Windows 標準の［**ファイルを開く**］ウィンドウが開き、インストールパッケージを作成するファイルを選択できます。

5. 事前に準備しておいた圧縮ファイルを選択します。

ZIP、CAB、TAR、または TAR.GZ ファイルをアップロードできます。インストールパッケージを SFX ファイル（自己解凍型の圧縮ファイル）から作成することはできません。

パッケージのインストール中に設定が変換されるようにする場合は、［**ウィザードの終了後、Kaspersky Security Center で認識されたアプリケーションの設定値を推奨値に変換する**］をオンにして、［**次へ**］をクリックします。

Kaspersky Security Center 管理サーバーへのファイルのアップロードが開始されます。

推奨インストール設定の使用を有効にした場合、Kaspersky Security Center 15.1 は実行ファイルがサードパーティ製品の定義データベースに含まれているかどうかをチェックします。チェックが成功すると、ファイルが認識されたことを知らせる通知が表示されます。設定が変換され、カスタムインストールパッケージが作成されます。追加の操作は必要ありません。［**終了**］をクリックしてウィザードを終了します。

6. 指定された圧縮ファイルから展開されたファイルのリストから実行ファイルを選択し、実行ファイルのコマンドラインパラメータを指定します。

インストールパッケージから製品をサイレントモードでインストールするためのコマンドラインのパラメータを指定できます。コマンドラインのパラメータの指定は省略可能です。

カスタムインストールパッケージを作成するプロセスが開始されます。

プロセスが終了すると、ウィザードで通知されます。

インストールパッケージが作成されなかった場合も、メッセージで通知されます。

7. ［**終了**］をクリックしてウィザードを終了します。

作成したインストールパッケージは、管理サーバーの共有フォルダーのパッケージ用のサブフォルダーにダウンロードされます。ダウンロード後、インストールパッケージがインストールパッケージのリストに表示されます。

管理サーバーで利用できるインストールパッケージのリストで、カスタムインストールパッケージの名前をクリックすることで次の操作を実行できます：

- インストールパッケージのプロパティとして以下の情報を表示する：
  - **名前**：カスタムインストールパッケージの名前。

- **ソース**：アプリケーションの開発元の名前。
- **アプリケーション**：カスタムインストールパッケージに含まれるアプリケーションの名前。
- **バージョン**：アプリケーションのバージョン。
- **言語**：カスタムインストールパッケージに含まれるアプリケーションの言語。
- **サイズ（MB）**：インストールパッケージのサイズ。
- **オペレーティングシステム**：インストールパッケージが対象とするオペレーティングシステムの種別。
- **作成**：インストールパッケージの作成日時。
- **変更**：インストールパッケージの変更日時。
- **種別**：インストールパッケージの種別。

- パッケージ名とコマンドラインのパラメータを変更する。この操作は、カスペルスキー製品以外を対象に作成したインストールパッケージでのみ実行できます。

カスタムパッケージの作成中にパッケージのインストール設定を推奨値に変換した場合は、［**設定**］と［**インストール手続き**］の 2 つの追加セクションが、カスタムインストールパッケージのプロパティの［**設定**］タブに表示される場合があります。

［**設定**］セクションには、表に示す次のプロパティが表示されます：

- **名前**：この列には、インストールパラメータに割り当てられた名前が表示されます。
- **種別**：この列には、インストールパラメータの種別が表示されます。
- **値**：この列には、インストールパラメータで定義されたデータの種別（［ブール］、［ファイルパス］、［数値］、［パス］、または［文字列］）が表示されます。

［**インストール手続き**］セクションには、カスタムインストールパッケージに含まれているアップデートの次のプロパティを指定する表が表示されます：

- **名前**：アップデートの名前。
- **説明**：アップデートの説明。
- **ソース**：アップデート元、つまり、Microsoft または別のサードパーティ開発元のいずれによってリリースされたものであるか。
- **種別**：アップデートの種別、つまり、対象とするのがドライバーまたはアプリケーションのいずれであるか。
- **カテゴリ**：Microsoft のアップデート（緊急更新プログラム、定義更新プログラム、ドライバー、機能パック、セキュリティ更新プログラム、サービスパック、ツール、更新プログラムロールアップ、更新プログラム、またはアップグレード）に対して表示される Windows Server Update Services（WSUS）カテゴリ。
- **MSRC による重要度**：Microsoft Security Response Center（MSRC）によって定義されたアップデートの重要度。
- **重要度**：カスペルスキーによって定義されたアップデートの重要度。

- **パッチ重要度（カスペルスキー製品向けのパッチ）**：カスペルスキー製品を対象とする場合のパッチの重要度。
- **記事**：アップデートについて説明するナレッジベースの記事の識別子（ID）。
- **セキュリティ情報**：アップデートについて説明するセキュリティ情報の ID。
- **インストール用に未割り当て**：アップデートのステータスが「インストール用に未割り当て」であるかどうかを表示します。
- **インストール予定**：アップデートのステータスが「インストール予定」であるかどうかを表示します。
- **インストール中**：アップデートのステータスが「インストール中」であるかどうかを表示します。
- **インストール済み**：アップデートのステータスが「インストール済み」であるかどうかを表示します。
- **失敗**：アップデートのステータスが「失敗」であるかどうかを表示します。
- **再起動が必要**アップデートのステータスが「再起動が必要」であるかどうかを表示します。
- **登録時刻**：アップデートが登録された日時を表示します。
- **対話モードでのインストール**：アップデートのインストール中にユーザーとの対話が必要であるかどうかを表示します。
- **取り消し**：アップデートが取り消された日時を表示します。
- **アップデート承認の状況**：アップデートのインストールが承認済みであるかどうかを表示します。
- **リビジョン**：アップデートの現在のリビジョン番号を表示します。
- **アップデート ID**：アップデートの ID を表示します。
- **アプリケーションのバージョン**。アプリケーションのアップデート後のバージョン番号を表示します。
- **より古い**：該当するアップデートを置換できる他のアップデートを表示します。
- **より新しい**：このアップデートで置換できる他のアップデートを表示します。
- **使用許諾契約書に同意する**：アップデート時に使用許諾契約書（EULA）への同意が必要であるかどうかを表示します。
- **製造元**：アップデートの製造元の名前を表示します。
- **アプリケーションファミリー**：アップデートが属するアプリケーションファミリーの名前を表示します。
- **アプリケーション**：アップデートが属するアプリケーションの名前を表示します。
- **言語**：アップデートの言語を表示します。
- **新しいバージョンのインストール用に未割り当て**：アップデートのステータスが「新しいバージョンのインストール用に未割り当て」であるかどうかを表示します。
- **必須コンポーネントのインストールが必要**：アップデートのステータスが「必須コンポーネントのインストールが必要」であるかどうかを表示します。

- **ダウンロード方法**：アップデートのダウンロード方法を表示します。
- **パッチ**：アップデートがパッチであるかどうかを表示します。
- **未インストール**：アップデートのステータスが「未インストール」であるかどうかを表示します。

セカンダリ管理サーバーへのインストールパッケージの配布

Kaspersky Security Center を使用すると、カスペルスキー製品およびサードパーティ製品のインストールパッケージを作成したり、インストールパッケージをクライアントデバイスに配布したり、パッケージからアプリケーションをインストールしたりできます。プライマリ管理サーバーの負荷を最適化するために、インストールパッケージをセカンダリ管理サーバーに配布できます。その後、セカンダリサーバーがパッケージをクライアントデバイスに送信すると、クライアントデバイスでアプリケーションのリモートインストールを実行できます。

セカンダリ管理サーバーにインストールパッケージを配布するには：

1. セカンダリ管理サーバーがプライマリ管理サーバーに接続されていることを確認します。
2. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
   タスクのリストが表示されます。
3. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
4. ［**新規タスク設定**］ページの［**アプリケーション**］ドロップダウンリストで、**Kaspersky Security Center** を選択します。次に、［**タスク種別**］ドロップダウンリストから［**インストールパッケージの配布**］を選択し、タスク名を指定します。
5. ［**タスク範囲**］ページで、次のいずれかの方法で、タスクが割り当てられるデバイスを選択します。
   - 特定の管理グループ内のすべてのセカンダリ管理サーバー用のタスクを作成する場合は、そのグループを選択して、グループタスクを作成します。
   - 特定のセカンダリ管理サーバー用のタスクを作成する場合は、それらのサーバーを選択して、タスクを作成します。
6. ［**配布したインストールパッケージ**］ページで、セカンダリ管理サーバーにコピーするインストールパッケージを選択します。
7. *インストールパッケージの配布*タスクを実行するアカウントを指定します。自身のアカウントを使用して、［**既定のアカウント**］**オプションをオンのままにすることもできます。**または、必要なアクセス権を持つ別のアカウントを指定してタスクを実行することもできます。この場合は［**アカウントの指定**］をオンにしてそのアカウントの資格情報を入力してください。
8. ［**タスク作成の終了**］ページで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにして、タスクのプロパティウィンドウを開き、既定のタスク設定を変更できます。変更しない場合は、後でいつでもタスク設定を変更できます。
9. ［**終了**］をクリックします。
   セカンダリ管理サーバーにインストールパッケージを配布するために作成されたタスクが、タスクリストに表示されます。

10. 手動でタスクを実行するか、タスク設定で指定したスケジュールに基づいてタスクが起動するのを待つことができます。

タスクが完了すると、選択したインストールパッケージが、指定したセカンダリ管理サーバーにコピーされます。

リモートインストールタスクを使用したアプリケーションのインストール

Kaspersky Security Center では、リモートインストールタスクを使用してデバイスにアプリケーションをリモートインストールできます。このタスクは、専用のウィザードを使用して作成しデバイスに割り当てます。タスクを簡単にデバイスに割り当てるには、次のいずれかの方法を使用し、ウィザードウィンドウでデバイス（最大 1000 台）を指定できます：

- **ネットワークの管理サーバーによって検出されたデバイスを選択する**：この場合、タスクを特定のデバイスに割り当てます。特定のデバイスには、管理グループに属するデバイスと管理グループが割り当てられていないデバイスの両方を含めることができます。
- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**：タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。
- **デバイスの抽出にタスクを割り当てる**：この場合、既に作成された抽出に属するデバイスにタスクを割り当てます。事前定義の抽出または作成済みのカスタム抽出を指定できます。
- **管理グループにタスクを割り当てる**：この場合、既に作成された管理グループに属するデバイスにタスクを割り当てます。

ネットワークエージェントがインストールされていないデバイスでリモートインストールを正常に行うには、次のポートを開いておく必要があります：TCP 139 および 445、UDP 137 および 138。既定では、これらのポートはドメイン内のすべてのデバイスで開いています。これらは、リモート導入準備ユーティリティによって自動的に開かれます。

アプリケーションのリモートインストール

このセクションでは、管理グループ、特定の IP アドレスを持つデバイス、またはさまざまな管理対象デバイスにアプリケーションをリモートインストールする方法について説明します。

アプリケーションを特定のデバイスにインストールするには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。
3. ［**タスク種別**］で、［**アプリケーションのリモートインストール**］を選択します。
4. 次のいずれかのオプションをオンにします：
   - **管理グループにタスクを割り当てる**

任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

  タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

  特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

- **デバイスの抽出にタスクを割り当てる**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

指定したデバイスに対して、*アプリケーションのリモートインストール*タスクが作成されます。［**管理グループにタスクを割り当てる**］オプションを選択した場合、タスクはグループ1になります。

5. ［**タスク範囲**］ステップで、管理グループ、特定のアドレスを持つデバイス、またはデバイスの抽出を指定します。

   使用可能な設定は、前のステップでオンにしたオプションによって異なります。

6. ［**インストールパッケージ**］ステップで、次の設定を指定します：

   - ［**インストールパッケージの選択**］で、インストールするアプリケーションのインストールパッケージを選択します。
   - ［**インストールパッケージの強制ダウンロード**］セクションで、アプリケーションのインストールに必要なファイルをクライアントデバイスに配布する方法を指定します。

     - **ネットワークエージェントを使用する**

       このオプションをオンにすると、インストールパッケージのクライアントデバイスへの配布は、クライアントデバイスにインストールされたネットワークエージェントによって行われます。

       このオプションをオフにすると、インストールパッケージはクライアントデバイスのオペレーティングシステムのツールを使用して配信されます。

       ネットワークエージェントがインストールされたデバイスにタスクが割り当てられている場合は、このチェックボックスをオンにすることを推奨します。

       既定では、このオプションはオンです。

     - **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**

このオプションをオンにすると、ディストリビューションポイントがオペレーティングシステムのツールを使用してインストールパッケージをクライアントデバイスに送信します。この機能が使用できるのは、ネットワークに少なくとも1つのディストリビューションポイントがある場合です。

［**ネットワークエージェントを使用する**］をオンにすると、ネットワークエージェントのツールが使用できない場合に限り、ファイルがオペレーティングシステムのツールで配布されます。

既定では、仮想管理サーバーで作成されたリモートインストールタスクに対して、このオプションはオンです。

- **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**

  このオプションをオンにすると、管理サーバーを通じてクライアントデバイスのオペレーティングシステムツールを使用してクライアントデバイスにファイルが送信されます。このオプションは、クライアントデバイスにネットワークエージェントがインストールされていないものの、クライアントデバイスが管理サーバーと同じネットワークに存在する場合にオンにできます。

  既定では、このオプションはオンです。

- ［**同時ダウンロード数の上限**］で、管理サーバーが同時にファイルを送信できるクライアントデバイスの最大許容数を指定します。

- ［**インストール試行回数の上限**］で、インストーラーの最大許容実行回数を指定します。

  試行回数がこのパラメータで指定された回数を超えると、Kaspersky Security Center はこのデバイスでインストーラーを起動しなくなります。*アプリケーションのリモートインストール*タスクを再開するには、［**インストール試行回数の上限**］パラメータの値を増やしてタスクを開始します。または、*アプリケーションのリモートインストール*タスクを新規作成することもできます。

- あるカスペルスキー製品から別のアプリケーションに移行する場合、現在のアプリケーションがパスワードで保護されているときは、［**現在のカスペルスキー製品をアンインストールするためのパスワード**］フィールドにパスワードを入力します。移行中は、現在の Kaspersky アプリケーションがアンインストールされることに注意してください。

  ［**現在のカスペルスキー製品をアンインストールするためのパスワード**］フィールドは、［**インストールパッケージの強制ダウンロード**］設定グループで［**ネットワークエージェントを使用する**］をオンにした場合にのみ使用できます。

  アンインストールパスワードは、*アプリケーションをリモートでインストールする*タスクを使用して Kaspersky Endpoint Security for Windows をインストールする場合、Kaspersky Security for Windows Server から Kaspersky Endpoint Security for Windows への移行シナリオでのみ使用できます。他のコンポーネントをインストールする時にアンインストールパスワードを使用すると、インストールエラーが発生する可能性があります。

  移行シナリオを正常に完了するには、次の前提条件が満たされていることを確認してください：

  - Kaspersky Security Center ネットワークエージェント 14.2 for Windows 以降を使用しています。
  - Windows を実行しているデバイスにアプリケーションをインストールしています。

- 詳細設定を行います：

  - **アプリケーションが既にインストールされている場合再インストールしない**

このオプションをオンにすると、選択したアプリケーションがクライアントデバイスに既にインストールされていた場合、インストールされません。

このオプションをオフにすると、アプリケーションは常にインストールされます。

既定では、このオプションはオンです。

- **ダウンロード前に OS の種別を確認する**

  ファイルをクライアントデバイスに送信する前に、Kaspersky Security Center Linux はインストールユーティリティの設定がクライアントデバイスのオペレーティングシステムに適用可能であるかどうかを確認します。設定を適用できない場合、Kaspersky Security Center はファイルを送信せず、アプリケーションのインストールを試行しません。たとえば、様々なオペレーティングシステムを実行しているデバイスが存在する管理グループのデバイスにアプリケーションをインストールするには、インストールタスクを管理グループに割り当ててから、このオプションをオンにして、必要なオペレーティングシステム以外を実行しているデバイスをスキップできます。

- **Active Directory のグループポリシーにパッケージのインストールを割り当てる**

  このオプションをオンにすると、Active Directory のグループポリシーを使用してインストールパッケージがインストールされます。

  このオプションは、ネットワークエージェントのインストールパッケージが選択されている場合に使用可能になります。

  既定では、このオプションはオフです。

- **実行中のアプリケーションを終了するよう告知する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

- 本製品をインストールするデバイスを選択します：

  - **全デバイスにインストール**

    他の管理サーバーで管理されているクライアントデバイスにもアプリケーションがインストールされます。

    既定ではこのオプションが選択されます。ネットワーク内に管理サーバーが1台しかない場合は、この設定を変更する必要はありません。

  - **この管理サーバーで管理されているデバイスにのみインストール**

アプリケーションはこの管理サーバーによって管理されているデバイスにのみインストールされます。ネットワーク内に複数の管理サーバーがあり、管理サーバー間での競合を回避したい場合は、このオプションを選択してください。

- インストール後に、デバイスを管理グループに移動するかどうかを指定します：
  - **デバイスを移動しない**

    デバイスは、現在配置されているグループから移動しません。どのグループにも割り当てられていないデバイスは、未割り当てのままとなります。

  - **未割り当てデバイスを選択したグループへ移動する（選択できるグループは1つのみ）**

    指定した管理グループにデバイスが移動されます。

  既定では［**デバイスを移動しない**］がオンになっています。セキュリティ上の理由のため、場合によってはデバイスを手動で移動する必要があります。

7. ウィザードのこのステップでは、アプリケーションのインストール中にデバイスを再起動する必要があるかどうかを指定します。
   - **デバイスを再起動しない**

     操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

   - **デバイスを再起動する**

     インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

   - **ユーザーに処理を確認する**

     手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

     既定では、このオプションがオンです。

     - **通知の繰り返し間隔（分）**

このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

既定では、このオプションはオンです。既定の間隔は 5 分です。1分から1,440 分までの値を指定できます。

このオプションをオフにすると、確認メッセージは1回だけ表示されます。

- **再起動するまでの時間（分）**

  ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

  既定では、このオプションはオンです。既定の間隔は 30 分です。1分から1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

8. 必要に応じて、［**デバイスにアクセスするアカウントの選択**］ステップで、*アプリケーションのリモートインストール*タスクを開始するために使用されるアカウントを追加します。

- **アカウントが不要 (ネットワークエージェントインストール済み)**

  このオプションをオンにすると、アプリケーションのインストーラーを実行するアカウントを指定する必要はありません。タスクは管理サーバーのサービスを実行しているアカウントで実行されます。

  クライアントデバイスにネットワークエージェントがインストールされていない場合、このオプションは使用できません。

- **アカウントが必要（ネットワークエージェントの使用なし）**

  リモートインストールタスクを割り当てるデバイスにネットワークエージェントがインストールされていない場合は、このオプションをオンにします。この場合、ユーザーアカウントを指定して、アプリケーションをインストールできます。

  アプリケーションインストーラーを実行するユーザーアカウントを指定するには、［**追加**］をクリックし、［**ローカルアカウント**］を選択して、ユーザーアカウントの資格情報を指定します。

  タスクを割り当てるすべてのデバイスで必要なすべての権限をどのアカウントも持たない場合などのために、複数のユーザーアカウントを追加できます。この場合、追加されたすべてのアカウントが上から下へ順番に使用され、タスクが実行されます。

9. ［**タスク作成の終了**］ステップで、［**終了**］をクリックしてタスクを作成し、ウィザードを終了します。

   ［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスク設定ウィンドウが表示されます。このウィンドウでは、必要に応じて、タスクのパラメータの確認と変更、またはタスクの開始スケジュールの設定を行うことができます。

10. タスクリストで、作成したタスクを選択し、［**開始**］をクリックします。

    または、タスク設定で指定したスケジュールに従ってタスクが起動するまで待ちます。

リモートインストールタスクが完了すると、指定したデバイスに選択したアプリケーションがインストールされます。

Active Directory グループポリシーを使用したアプリケーションのインストール

Kaspersky Security Center では、Active Directory グループポリシーを使用して、管理対象デバイスにカスペルスキー製品をインストールできます。

Active Directory グループポリシーを使用したインストールは、ネットワークエージェントを含むインストールパッケージからのみ可能です。

Active Directory グループポリシーを使用してアプリケーションをインストールするには：

1. 製品導入ウィザードを実行します。ウィザードの指示に従ってください。

2. 製品導入ウィザードの［**リモートインストールタスク設定**］ウィンドウで、［**Active Directory のグループポリシーにパッケージのインストールを割り当てる**］オプションをオンにします。

3. ［**デバイスにアクセスするアカウントの選択**］ウィンドウで、［**アカウントが必要（ネットワークエージェントの使用なし）**］オプションをオンにします。

4. Kaspersky Security Center をインストールするデバイスの管理者権限があるアカウントまたは Group Policy Creator Owners ドメイングループに含まれるアカウントを追加します。

5. 選択したアカウントに権限を付与するには：

   a. ［**コントロールパネル**］→［**管理ツール**］の順に選択し、［**グループポリシーの管理**］を開きます。

   b. 必要なドメインのフォルダーをクリックします。

   c. ［**委任**］セクションをクリックします。

   d. ［**権限**］のドロップダウンリストから［**GPO をリンク**］を選択します。

   e. ［**追加**］をクリックします。

   f. 開いた［**ユーザー、コンピューター、またはグループの選択**］ウィンドウで、必要なアカウントを選択します。

   g. ［OK］をクリックして、［**ユーザー、コンピューター、またはグループの選択**］ウィンドウを閉じます。

h. ［**グループとユーザー**］の一覧で、先ほど追加したアカウントを選択して、［**詳細**］→［**詳細**］の順にクリックします。

i. ［**権限エントリ**］リストで、追加したアカウントをダブルクリックします。

j. 次の権限を付与します：

- **グループオブジェクトの作成**
- **グループオブジェクトの削除**
- **グループポリシーコンテナーオブジェクトの作成**
- **グループポリシーコンテナーオブジェクトの削除**

k. ［**OK**］をクリックして変更内容を保存します。

6. ウィザードの指示に従って、他の設定を定義します。

7. 作成されたリモートインストールタスクを手動で実行するか、スケジュール済みの開始まで待機します。

リモートインストールが次の順番で開始されます：

1. タスクの実行時に、指定したすべてのクライアントデバイスが属する各ドメインに次の項目が作成されます：
   - ［**Kaspersky_AK{GUID}**］という名前のグループポリシーオブジェクト（GPO）。
   - GPO に対応するセキュリティグループこのセキュリティグループには、タスクが適用されるクライアントデバイスが含まれます。セキュリティグループの内容によって、GPO の範囲が定義されます。
2. Kaspersky Security Center は、選択されたカスペルスキー製品を、本製品の共有ネットワークフォルダー「Share」から直接クライアントデバイスにインストールします。Kaspersky Security Center のインストールフォルダーでは、アプリケーションをインストールするための MSI ファイルを含む補助的なサブフォルダーが作成されます。
3. 新しいデバイスをタスク範囲に追加すると、次回のタスク開始時に、新しいデバイスがセキュリティグループに追加されます。タスクスケジュールで［**未実行のタスクを実行する**］をオンにしていると、デバイスはすぐにセキュリティグループに追加されます。
4. デバイスがタスク範囲から削除されると、次回のタスク開始時にセキュリティグループからも削除されます。
5. タスクを Active Directory から削除すると、GPO、GPO へのリンクおよび対応するセキュリティグループも削除されます。

Active Directory を使用して別のインストールスキームを適用する場合は、必要な設定を手動で指定できます。手動での設定が必要な可能性がある場合は次の通りです：

- アンチウイルスによる保護の管理者が一部のドメインの Active Directory で変更権限を持っていない場合
- 元のインストールパッケージを別のネットワークリソースに保存する必要がある場合
- 特定の Active Directory ユニットに GPO をリンクする場合

Active Directory で別のインストールスキームのオプションは次の通りです：

- インストールが Kaspersky Security Center の共有フォルダーから直接実行される場合、GPO プロパティで、目的のアプリケーションのインストールパッケージフォルダーのサブフォルダー exec にある MSI ファイルを指定する必要があります。

- インストールパッケージを別のネットワークリソースに配置する必要がある場合は、フォルダー exec の内容全部をネットワークリソースにコピーする必要があります。これは、このフォルダーには MSI ファイルの他に、パッケージの作成時に生成された構成ファイルが含まれているためです。アプリケーションと同時にライセンスをインストールするには、ライセンス情報ファイルもこのフォルダーにコピーします。

セカンダリ管理サーバーへのアプリケーションのインストール

セカンダリ管理サーバーにアプリケーションをインストールするには：

1. 目的のセカンダリ管理サーバーを制御する管理サーバーとの接続を確立します。

2. インストールするアプリケーションに対応するインストールパッケージが、選択したそれぞれのセカンダリ管理サーバー上で使用可能であるか確認してください。セカンダリサーバーのいずれにもインストールパッケージが見つからない場合は、配布します。この目的のために、タスク種別［**インストールパッケージの配布**］でタスクを作成します。

3. セカンダリ管理サーバーでリモートアプリケーションのインストール用のタスクを作成します。タスク種別として［**セカンダリ管理サーバーへのアプリケーションのリモートインストール**］を選択します。

   新規タスクウィザードは、ウィザードで選択したアプリケーションを特定のセカンダリ管理サーバーにリモートインストールするタスクを作成します。

4. 手動でタスクを実行するか、タスク設定で指定したスケジュールに基づいてタスクが起動するのを待ちます。

リモートインストールタスクが完了すると、選択したアプリケーションがセカンダリ管理サーバーにインストールされます。

Unix デバイスのリモートインストールを設定する

リモートインストールタスクを使用して Unix デバイスにアプリケーションをインストールする際、タスクに Unix 固有の設定を指定することができます。これらの設定はタスクが作成された後にタスクのプロパティで利用できるようになります。

Unix 固有の設定をリモートインストールタスクで指定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

2. Unix 固有の設定を指定するリモートインストールタスクの名前をクリックします。

   タスクのプロパティウィンドウが開きます。

3. ［**アプリケーション設定**］→［**Unix 固有の設定**］の順に移動します。

4. 次の設定を指定します：

   - **root アカウントのパスワードを設定する（SSH での導入時のみ）**

パスワードを指定しないと対象のデバイスで sudo コマンドが使用できない場合、このオプションを選択してルートアカウントのパスワードを指定します。Kaspersky Security Center は対象デバイスにパスワードを暗号化して転送し、復号化してからこのパスワードを使用してルートアカウントに代わってインストール手順を開始します。

Kaspersky Security Center は SSH 接続を作成するためにユーザーアカウントや指定したパスワードを使用しません。

- **ターゲットデバイスへの実行権限がある一時ディレクトリへのパスを指定する（SSH での導入時のみ）**

  対象デバイスの /tmp ディレクトリに実行権限がない場合、このオプションを選択してから実行権限のあるディレクトリへのパスを指定します。Kaspersky Security Center は SSH 経由でアクセスする一時ディレクトリとして指定されたディレクトリを使用します。アプリケーションはインストールパッケージをそのディレクトリに配置し、インストールプロセスを実行します。

5. ［**保存**］をクリックします。

   指定したタスク設定が保存されます。

カスペルスキー製品の起動および停止

管理対象デバイスでカスペルスキー製品を起動および停止するには、*アプリケーションの開始または停止*タスクを使用できます。

アプリケーションの開始または停止タスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. ［**アプリケーション**］ドロップダウンリストで、タスクを作成するアプリケーションを選択します。
   以前にこれらのアプリケーションの管理 Web プラグインを追加している場合は、カスペルスキー製品がリストに表示されます。
4. ［**タスク種別**］リストから、［**アプリケーションのアクティベーション**］タスクを選択します。
5. ［**タスク名**］フィールドに、新しいタスクの名前を指定します。
   タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
6. ［タスクを割り当てるデバイス］を選択します。
7. ［**アプリケーション**］ウィンドウで、次のように操作します：
   - タスクを作成するアプリケーションの名前の横にあるチェックボックスをオンにします。
   - ［**アプリケーションの開始**］または［**アプリケーションの停止**］オプションを選択します。

8. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ステップで、［**タスクの作成が完了したらタスクの詳細を表示する**］オプションを有効にします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

9. ［**終了**］をクリックします。
   タスクが作成され、タスクリストに表示されます。

10. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

11. タスクのプロパティウィンドウで、必要性に応じて一般的なタスク設定を指定し、設定を保存します。

    タスクが指定した設定で作成されます。

タスクを実行するには、タスクリストで目的のタスクを選択し、［**開始**］をクリックします。

モバイルデバイス管理

Kaspersky Security Center からのモバイルデバイス保護の管理は、専用のライセンスを使用して利用できるモバイルデバイス管理機能を使用して行われます。自社の従業員が使用しているモバイルデバイスを管理する場合は、モバイルデバイス管理を有効にして設定してください。

モバイルデバイス管理を使用して、従業員の Android デバイスを管理できます。デバイスにインストールされた Kaspersky Endpoint Security for Android を使用して保護します。このモバイルアプリケーションにより、モバイルデバイスを Web の脅威やウイルス、その他の脅威をもたらすプログラムから保護します。Kaspersky Security Center Web コンソールを使用した一元管理のため、Kaspersky Security Center Web がインストールされたデバイスに次の Web 管理プラグインをインストールする必要があります：

- Kaspersky Security for Mobile プラグイン
- Kaspersky Endpoint Security for Android プラグイン

モバイルデバイスへの保護の導入および管理の詳細については、Kaspersky Security for Mobile のヘルプを参照してください。

Kaspersky Security Center Web コンソールにおけるモバイルデバイス管理設定の変更

モバイルデバイス管理設定を変更するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（ ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**追加のポート**］セクションを選択します。

3. 目的の設定項目を変更します：

   - **モバイルデバイス用ポートを開く**

このスイッチをオンにすると、管理サーバー上でモバイルデバイス用ポートが開かれます。
モバイルデバイス用ポートを使用できるのは、モバイルデバイス管理がインストールされている場合のみです。
このスイッチをオフにした場合、管理サーバー上のモバイルデバイスのポートは使用されません。
既定では、このスイッチはオフです。

- **モバイルデバイスとの同期用のポート**

  モバイルデバイスと管理サーバーとの接続に使用するポートの番号。既定のポート番号は 13292 です。
  レコードには 10 進法が使用されます。

- **モバイルデバイスのアクティベーション用のポート**

  Kaspersky Endpoint Security for Android をカスペルスキーのアクティベーションサーバーに接続するポートです。
  既定のポート番号は 17100 です。

4. ［**保存**］をクリックします。

モバイルデバイスを管理サーバーに接続できる状態になっています。

サードパーティのセキュリティ製品からの移行とアンインストールの実施

カスペルスキーのセキュリティ製品を Kaspersky Security Center を使用してインストールする場合、インストールするアプリケーションと競合するサードパーティ製ソフトウェアを削除しなければならない場合があります。Kaspersky Security Center では、サードパーティ製品を削除する複数の方法が用意されています。

競合するアプリケーションをインストーラーを使用して削除

この方法は MMC ベースの管理コンソールでのみ利用できます。

競合するアプリケーションをインストーラーを使用して削除する方法は、様々なインストールでサポートされています。セキュリティ製品のインストールパッケージのプロパティウィンドウ（［**競合アプリケーション**］セクション）で、［**競合アプリケーションを自動的にアンインストールする**］がオンになっている場合、セキュリティ製品がインストールされる前に、すべての競合アプリケーションが自動的に削除されます。

競合するアプリケーションの削除をアプリケーションのリモートインストールの設定時に指定

セキュリティ製品のリモートインストールの設定時に［**競合アプリケーションを自動的にアンインストールする**］をオンにできます。MMC ベースの管理コンソールでは、リモートインストールウィザードでこのオプションを設定できます。Kaspersky Security Center Web コンソールでは、製品導入ウィザードでこのオプションを設定できます。このオプションをオンにすると、管理対象デバイスにセキュリティ製品をインストールする前に、Kaspersky Security Center は競合するアプリケーションを削除します。

実行手順の説明：

- 管理コンソール：リモートインストールウィザードを使用した競合アプリケーションの削除
- Kaspersky Security Center Web コンソール：セキュリティ製品をインストールする前に競合するアプリケーションを削除

専用タスクを使用した競合アプリケーションの削除

競合アプリケーションを削除するには、**アプリケーションのリモートアンインストール**タスクを使用します。このタスクは、セキュリティ製品のインストールタスクの前にデバイスで実行する必要があります。たとえば、インストールタスクのスケジュール種別として［**他のタスクが完了次第**］を選択し、条件の対象となるタスクとして［**アプリケーションのリモートアンインストール**］を指定できます。

このアンインストール方法は、セキュリティ製品のインストーラーでは競合アプリケーションを適切に削除できない場合に有用です。

管理コンソールの使用方法：タスクの作成

ネットワーク接続されたデバイスの検出

このセクションでは、ネットワーク接続されたデバイスを検出するプロセスについて説明します。

Kaspersky Security Center では、条件を指定してデバイスを検索できます。検索結果をテキストファイルに保存できます。

デバイスの検出機能により、次のデバイスを見つけることができます：

- Kaspersky Security Center の管理サーバーとセカンダリ管理サーバーの管理グループに属する管理対象デバイス
- Kaspersky Security Center の管理サーバーとセカンダリ管理サーバーで管理される未割り当てデバイス

ネットワーク接続されたデバイスの検出シナリオ

セキュリティ製品のインストール前にデバイスの検索を実行する必要があります。管理サーバーは、検出されたデバイスに関する情報を受け取り、ポリシーを通じてデバイスを管理することができるようにします。ネットワークで使用可能なデバイスのリストを更新するには、定期的なネットワークポーリングが必要です。

ネットワークポーリングを開始する前に、SMB プロトコルが有効になっていることを確認してください。有効でない場合、Kaspersky Security Center はポーリングされたネットワークでデバイスを検出できません。SMB プロトコルを有効にするには、オペレーティングシステムの指示に従ってください。

ネットワーク接続されたデバイスの検出は、次の手順で進行します：

1. **デバイスの検出**

   クイックスタートウィザードの説明に従って最初のデバイス検出を実行すると、コンピューター、タブレット、スマートフォンなどのネットワーク接続されたデバイスが検出されます。デバイスの検出は手動でも実行できます。

2. **ポーリングスケジュールを設定**

   どのポーリングタイプを定期的に使用するかを決定します。目的のタイプを有効にして、ポーリングスケジュールを自由に設定することができます。「ネットワークポーリングの頻度に関する推奨事項」を参照してください。

3. **検出されたデバイスを管理グループに追加するルールの設定（任意）**

   ネットワーク内に新しいデバイスが追加された場合、これらのデバイスは定期的なポーリング中に検出され、［**未割り当てデバイス**］グループに含まれます。デバイスの移動ルールを設定することで、［管**管理対象デバイス**グループへのデバイスの割り当てを自動化することができます。また、［保持ルール］を確立することもできます。

   手順 3 をスキップすると、新しく検出されたデバイスは［**未割り当てデバイス**］グループに割り当てられます。必要に応じて、これらのデバイスを［**管理対象デバイス**］グループに手動で移動できます。デバイスを［**管理対象デバイス**］グループに手動で移動する場合、各デバイスの情報を分析し、管理グループに移動するかどうかや具体的にどの管理グループに移動するかを決定することができます。

結果

これらのステップがすべて完了すると、次の状態を実現できます：

- Kaspersky Security Center 管理サーバーがネットワーク内のデバイスを検出し、その情報を利用できるようになります。
- ポーリングのスケジュールが設定され、指定したスケジュールに従ってポーリングが実行されます。
- 新しく検出されたデバイスは、設定されたルールに従って配置されます（または、ルールが設定されていない場合、デバイスは［**未割り当てデバイス**］グループに割り当てられたままになります）。

デバイスの検索

Kaspersky Security Center で利用できるデバイスの検索方法の種別と、それぞれの方法の使用方法を説明しています。

管理サーバーは、ネットワークの構造およびネットワーク上のデバイスに関する情報を定期的なポーリングによって取得します。情報は管理サーバーのデータベースに保存されます。管理サーバーが実行可能なポーリングの種類は、次の通りです：

- **Windows ネットワークのポーリング**：管理サーバーでは、簡易ポーリングと完全ポーリングの 2 種類の Windows ネットワークポーリングを実行できます。簡易ポーリングでは管理サーバーが、すべてのネットワークドメインとワークグループ内のデバイスの NetBIOS 名リストの情報のみ取得します。完全ポーリングでは、各クライアントデバイスに対して、オペレーティングシステムの名前、IP アドレス、DNS 名、NetBIOS 名などより詳細な情報が要求されます。既定では、簡易ポーリングと完全ポーリングの両方がオンです。Windows ネットワークのポーリングでは、一部の状況（例：UDP 137、UDP 138、TCP 139 ポートがルーターまたはファイアウォールで閉じている）ではデバイスの検出に失敗する場合があります。
- ［**ドメインコントローラーのポーリング**］。管理サーバーまたはディストリビューションポイントは、ドメイン構造と、ドメインに含まれるデバイスの DNS 名に関する情報を取得します。既定では、この種別のポーリングはオンです。すべてのネットワークデバイスがドメインのメンバーである場合は、ドメインコ

ントローラーのポーリングを使用することを推奨します。ネットワークに接続されたデバイスの一部がドメインに含まれていない場合、これらのデバイスはドメインコントローラーのポーリングでは検出できません。

- **IP アドレス範囲のポーリング**：管理サーバーが ICMP パケットまたは NBNS プロトコルを使用して指定の IP アドレス範囲をポーリングし、IP アドレス範囲内にあるデバイスの完全なデータを作成します。既定では、この種別のポーリングはオフです。Windows ネットワークのポーリングや Active Directory のポーリングを使用する場合は、この種別のポーリングの使用は推奨されません。

- **Zeroconf ポーリング**：ゼロコンフィギュレーションネットワーキング（zero-configuration networking）（「*Zeroconf*」とも表記）を使用して IPv6 ネットワークを検索するディストリビューションポイント。既定では、この種別のポーリングはオフです。ディストリビューションポイントが Linux を実行している場合は Zeroconf ポーリングを使用できます。

デバイス移動ルールを設定しオンにしている場合、新たに検出されたデバイスは自動的に**管理対象デバイス**グループに含まれます。移動ルールがオンでない場合、新たに検出されたデバイスは自動的に**未割り当てデバイス**グループに含まれます。

デバイスの検索の各種別に対して設定を編集できます。たとえば、ポーリングのスケジュールや、ポーリングの対象をドメインフォレストとするか特定のドメインのみにするかなどの設定が可能です。

ネットワークポーリングを開始する前に、SMB プロトコルが有効になっていることを確認してください。有効でない場合、Kaspersky Security Center はポーリングされたネットワークでデバイスを検出できません。SMB プロトコルを有効にするには、オペレーティングシステムの指示に従ってください。

Windows ネットワークのポーリング

Windows ネットワークのポーリングの概要

簡易ポーリングでは管理サーバーが、すべてのネットワークドメインとワークグループ内のデバイスの NetBIOS 名リストの情報のみ取得します。完全ポーリングでは、各クライアントデバイスに対して次の情報が要求されます：

- オペレーティングシステムの名前
- IP アドレス
- DNS 名
- NetBIOS 名

簡易ポーリングと完全ポーリングの両方で次の要件を満たす必要があります：

- UDP 137/138、TCP 139、UDP 445、TCP 445 ポートをネットワーク内で利用できる必要があります。
- SMB プロトコルが有効になっています。
- Microsoft のコンピューターブラウザーサービスを使用し、管理サーバー上でプライマリブラウザーコンピューターが有効である必要があります。
- Microsoft のコンピューターブラウザーサービスを必ず使用し、クライアントデバイス上でプライマリブラウザーコンピューターが有効であり、かつ次の条件を満たす必要があります：

- ネットワークデバイスが 32 台以内の場合、1 台以上のデバイスで実行する
- ネットワークデバイス 32 台につき、1 台以上のデバイスで

完全ポーリングは簡易ポーリングを 1 回以上実行している場合にのみ実行できます。

Windows ネットワークのポーリング設定の表示と変更

Windows ネットワークのポーリングのプロパティを変更するには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**Windows ドメイン**］の順に移動します。
2. ［**プロパティ**］をクリックします。
   Windows ドメインのプロパティウィンドウが開きます。
3. ［**Windows ネットワークのポーリングを有効にする**］を使用して、Windows ネットワークのポーリングをオンまたはオフにします。
4. ポーリングスケジュールを設定します。既定では、簡易ポーリングが 15 分ごとに、完全ポーリングが 60 分ごとに実行されます。
   ポーリングスケジュールのオプション：

   - **N 日ごと**

     指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。
     既定では、現在のシステム日時から、1 日ごとにポーリングが実行されます。

   - **N 分ごと**

     指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。

   - **曜日ごと**

     指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。

   - **毎月、選択した週の指定日**

     毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。

   - **未実行のタスクを実行する**

     ポーリングの実行がスケジュールされていた時刻に管理サーバーがオフまたは接続できなかった場合は、管理サーバーがオンになった時に即座にポーリングを実行させるか、ポーリングの次回のスケジュールまで待機するかを選択できます。
     このオプションをオンにすると、管理サーバーがオンになるとすぐにポーリングを開始します。
     このオプションをオフにすると、管理サーバーはポーリングの次回のスケジュールまでポーリングの実行を待機します。
     既定では、このオプションはオフです。

5. Windows ネットワークポーリングのプロパティを保存します。

プロパティが保存され、検出されたすべての Windows ドメインおよびワークグループに適用されます。

手動でのポーリングの実行

手動でポーリングを実行するには：

［**簡易ポーリングの開始**］または［**完全ポーリングの開始**］をクリックします。

ポーリングの完了後、［**Windows ドメイン**］ページでドメイン名に隣接するチェックボックスをオンにして［**デバイス**］をクリックすると、検出されたデバイスのリストを表示できます。

IP アドレス範囲のポーリング

Kaspersky Security Center は最初、ポーリングを行う IP アドレスを、Kaspersky Security Center がインストールされているデバイスのネットワーク設定から取得します。デバイスアドレスが 192.168.0.1 でサブネットマスクが 255.255.255.0 の場合、Kaspersky Security Center は 192.168.0.0/24 ネットワークをポーリング対象のアドレスのリストに自動的に含めます。Kaspersky Security Center は 192.168.0.1 から 192.168.0.254 までのすべてのアドレスのポーリングを実行します。

Windows ネットワークのポーリングや Active Directory のポーリングを使用する場合は、IP アドレス範囲のポーリングの使用は推奨されません。

Kaspersky Security Center は DNS のリバースルックアップまたは NBNS プロトコルを使用して IP 範囲を検索できます：

- **DNS のリバースルックアップ**

  Kaspersky Security Center は、指定された範囲のすべての IP アドレスに対して、標準的な DNS リクエストを使用して DNS 名への逆解決を実行します。この処理が成功すると、取得した名前に対してサーバーは「`ICMP ECHO REQUEST`（Ping コマンドと同一）」を送信します。これに対してデバイスが応答した場合、デバイスの情報が Kaspersky Security Center のデータベースに追加されます。逆引きの名前解決は、IP アドレスを付与されているがコンピューターではないネットワークデバイス（ネットワークプリンターやルーターなど）を除外するために必要です。

  このポーリング方法は、ローカル DNS サービスが適切に構成されているかどうかに依存します。ローカル DNS サービスで、逆引きの検索ゾーンが設定されている必要があります。Active Directory を使用しているネットワークでは、こうした検索ゾーンが自動的に維持されます。ただし、Active Directory を使用しているネットワークでは、IP アドレス範囲のポーリングを使用しても Active Directory のポーリングで得られる以上の情報は取得できません。また、ネットワーク規模が小さい場合、その他のネットワークサービスでは逆引きの検索ゾーンが必要ないことが多いため、管理者が逆引きの検索ゾーンを設定していない場合も多いです。こうした理由から、IP アドレス範囲のポーリングは既定ではオフになっています。

- **NBNS プロトコル**

  何らかの理由によりネットワークでリバースルックアップでの名前解決ができない場合は、Kaspersky Security Center は NBNS プロトコルを使用して IP アドレス範囲をポーリングします。IP アドレスの要求に対して NetBIOS 名が返された場合、このデバイスに関する情報は Kaspersky Security Center のデータベースに追加されます。

ネットワークポーリングを開始する前に、SMB プロトコルが有効になっていることを確認してください。有効でない場合、Kaspersky Security Center はポーリングされたネットワークでデバイスを検出できません。SMB プロトコルを有効にするには、オペレーティングシステムの指示に従ってください。

IP アドレス範囲のポーリング設定の表示と変更

IP アドレス範囲のポーリング設定の表示と変更を行うには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**IP アドレス範囲**］の順に移動します。
2. ［**プロパティ**］をクリックします。
   IP ポーリングのプロパティウィンドウが開きます。
3. ［**ポーリングを許可**］を使用して、IP ポーリングをオンまたはオフにします。
4. ポーリングスケジュールを設定します。既定では、IP ポーリングは 420 分（7 時間）ごとに実行されます。
   ポーリング間隔の指定時には、指定する値が［IP アドレスの有効期間］の値を超えないように注意してください。IP アドレスの有効期間の間にポーリングによって IP アドレスが確認されなかった場合、この IP アドレスはポーリングの結果から自動的に削除されます。既定では、（DHCP プロトコルを使用して割り当てられる）動的 IP アドレスは 24 時間ごとに変更されるので、ポーリング結果の有効期間は 24 時間です。
   ポーリングスケジュールのオプション：

   - **N 日ごと**

     指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。
     既定では、現在のシステム日時から、1 日ごとにポーリングが実行されます。

   - **N 分ごと**

     指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。

   - **曜日ごと**

     指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。

   - **毎月、選択した週の指定日**

     毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。

   - **未実行のタスクを実行する**

ポーリングの実行がスケジュールされていた時刻に管理サーバーがオフまたは接続できなかった場合は、管理サーバーがオンになった時に即座にポーリングを実行させるか、ポーリングの次回のスケジュールまで待機するかを選択できます。

このオプションをオンにすると、管理サーバーがオンになるとすぐにポーリングを開始します。

このオプションをオフにすると、管理サーバーはポーリングの次回のスケジュールまでポーリングの実行を待機します。

既定では、このオプションはオフです。

5. ［**保存**］をクリックします。

プロパティが保存され、すべての IP アドレス範囲に適用されます。

手動でのポーリングの実行

手動でポーリングを実行するには：

［**ポーリングを開始する**］をクリックします。

IP アドレス範囲の追加と変更

Kaspersky Security Center は最初、ポーリングを行う IP アドレスを、Kaspersky Security Center がインストールされているデバイスのネットワーク設定から取得します。デバイスアドレスが 192.168.0.1 でサブネットマスクが 255.255.255.0 の場合、Kaspersky Security Center は 192.168.0.0/24 ネットワークをポーリング対象のアドレスのリストに自動的に含めます。Kaspersky Security Center は 192.168.0.1 から 192.168.0.254 までのすべてのアドレスのポーリングを実行します。自動的に定義された IP アドレス範囲を編集したり、カスタム IP アドレス範囲を追加できます。

IPv4 アドレスに対してのみ範囲を作成できます。Zeroconf ポーリングを有効にしている場合は、Kaspersky Security Center はネットワーク全体をポーリングします。

新しい IP アドレス範囲を追加するには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**IP アドレス範囲**］の順に移動します。
2. 新しい IP アドレス範囲を追加するには、［**追加**］をクリックします。
3. 表示されたウィンドウで、次の設定を行います：

- **IP アドレス範囲の名前**

  IP アドレス範囲の名前。「192.168.0.0/24」のように、指定した IP アドレス範囲自体を名前として使用することもできます。

- **IP 区間またはサブネットアドレスとマスク**

開始 IP アドレスと終了 IP アドレスを指定するか、サブネットアドレスとサブネットマスクを指定して、IP アドレス範囲を設定します。［**参照**］をクリックして、既存の IP アドレス範囲を選択することもできます。

- **IP アドレスの有効期間（時間）**

  このパラメータの指定時には、値がポーリングのスケジュールで指定したポーリング間隔を超えるように指定してください。IP アドレスの有効期間の間にポーリングによって IP アドレスが確認されなかった場合、この IP アドレスはポーリングの結果から自動的に削除されます。既定では、（DHCP プロトコルを使用して割り当てられる）動的 IP アドレスは 24 時間ごとに変更されるので、ポーリング結果の有効期間は 24 時間です。

4. 追加したサブネットまたは IP アドレスの区間をポーリングするには、［**IP アドレス範囲のポーリングを有効にする**］をオンにします。そうでない場合、追加したサブネットまたは IP 区間を対象としたポーリングは実行されません。

5. ［**保存**］をクリックします。

IP アドレス範囲のリストに新しい IP アドレス範囲が追加されます。

［**ポーリングを開始する**］を使用して、IP アドレス範囲ごとに個別にポーリングを実行できます。ポーリングの完了後、［**デバイス**］を使用して、検出されたデバイスのリストを表示できます。既定では、ポーリング結果の有効期間は 24 時間で、これは IP アドレスの有効期間と同じ長さです。

既存の IP アドレス範囲にサブネットを追加するには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**IP アドレス範囲**］の順に移動します。

2. サブネットを追加する IP アドレス範囲の名前をクリックします。

3. ウィンドウが表示されたら、［**追加**］をクリックします。

4. サブネットアドレスとサブネットマスクを指定するか、開始 IP アドレスと終了 IP アドレスを指定して、IP アドレス範囲を指定します。または、［**参照**］をクリックして既存のサブネットを追加することもできます。

5. ［**保存**］をクリックします。

   IP アドレス範囲に新しいサブネットが追加されます。

6. ［**保存**］をクリックします。

IP アドレス範囲の新しい設定が保存されます。

サブネットは、個数の制限なく必要な数だけ追加できます。名前のある IP アドレス範囲同士での範囲の重複は許可されていませんが、1 つの IP アドレス範囲内の名前のないサブネット（IP 区間同士）にはそうした制限はありません。IP アドレス範囲ごとのポーリングを個別にオンまたはオフに切り替えることができます。

Zeroconf ポーリング

この検索方法は Linux ベースのディストリビューションポイントでのみサポートされます。

ディストリビューションポイントは IPv6 アドレスのデバイスを持つネットワークを検索できます。この場合、IP 範囲は指定されず、ディストリビューションポイントはネットワーク全体をゼロコンフィギュレーションネットワーキング（「*Zeroconf*」とも表記）を使用して検索します。Zeroconf の使用を開始するには、ディストリビューションポイントで avahi-browse ユーティリティをインストールする必要があります。

IPv6 ネットワークポーリングを有効にするには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**IP アドレス範囲**］の順に移動します。
2. ［**プロパティ**］をクリックします。
3. ウィンドウが表示されたら、［**Zeroconf を使用して IPv6 ネットワークのポーリングを実行する**］をオンにします。

その後、ディストリビューションポイントはネットワークの検索を開始します。この場合、指定された IP 範囲は無視されます。

ドメインコントローラーのポーリング

Kaspersky Security Center は、Microsoft Active Directory ドメインコントローラーと Samba ドメインコントローラーのポーリングをサポートしています。

Kaspersky Security Center は、Linux ディストリビューションポイントを使用してのみ Samba ドメインコントローラーをポーリングできます。Samba ドメインコントローラーの場合、Samba 4 が Active Directory ドメインコントローラーとして使用されます。

ドメインコントローラーをポーリングすると、管理サーバーまたはディストリビューションポイントは、ドメイン構造、ユーザーアカウント、セキュリティ グループ、およびドメインに含まれるデバイスの DNS 名に関する情報を取得します。

すべてのネットワークに接続されたデバイスがドメインのメンバーである場合は、ドメインコントローラーのポーリングを使用することを推奨します。ネットワークに接続されたデバイスの一部がドメインに含まれていない場合、これらのデバイスはドメインコントローラーのポーリングでは検出できません。

必須条件

ドメインコントローラーをポーリングする前に、ファイアウォールまたはプロキシサーバー経由でドメインコントローラーへの接続を許可していることを確認してください。また、ドメインコントローラーで次のプロトコルが有効になっていることを確認してください。

- ライトウェイトディレクトリアクセスプロトコル（LDAP）
- 簡易認証およびセキュリティ層（SASL）

  このプロトコルは、SASL 認証を使用してドメインコントローラーへの接続が確立される場合に使用されます。管理サーバーおよびディストリビューションポイントは、DIGEST-MD5 メカニズムのみをサポートします。
- セキュアソケットレイヤー経由の軽量ディレクトリアクセスプロトコル（LDAPS）

このプロトコルは、暗号化された接続を介してドメインコントローラーに接続する必要がある場合に使用されます。

ドメインコントローラーデバイスで次のポートが使用可能であることを確認してください：

- LDAP プロトコルおよび簡易認証（SASL を含む）の場合は 389
- LDAPS プロトコルの場合は 636

管理サーバーを使用したドメインコントローラーのポーリング

管理サーバーを使用して、Microsoft Active Directory ドメインコントローラーのみをポーリングできます。

管理サーバーを使用してドメインコントローラーをポーリングするには、次の手順を実行します：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**ドメインコントローラー**］の順に移動します。
2. ［**ポーリングの設定**］をクリックします。
   ［**ドメインコントローラーのポーリング設定**］ウィンドウが開きます。
3. ［**ドメインコントローラーのポーリングを有効にする**］をオンにします。
4. ［**詳細設定**］セクションで、ポーリング範囲を指定します：
   - **現在のドメインのポーリング**
     Kaspersky Security Center が属するドメインをポーリングするには、このオプションを選択します。
   - **ドメインフォレスト全体のポーリング**
     Kaspersky Security Center が属するドメインフォレストをポーリングするには、このオプションを選択します。
   - **指定したドメインのポーリング**
     指定されたアドレスとユーザー資格情報を使用してドメインをポーリングするには、このオプションを選択します。
5. 必要に応じて、ポーリングスケジュールを指定します。既定では、時間は 1 時間です。次のポーリングで受信したデータは、古いデータと完全に置き換わります。
   ポーリングスケジュールには次のオプションがあります：
   - **N 日ごと**
     指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。
     既定では、現在のシステム日時から、1 日ごとにポーリングが実行されます。
   - **N 分ごと**
     指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。
   - **曜日ごと**

指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。

- **未実行のタスクを実行する**

  ポーリングの実行がスケジュールされていた時刻に管理サーバーがオフまたは接続できなかった場合は、管理サーバーがオンになった時に即座にポーリングを実行させるか、ポーリングの次回のスケジュールまで待機するかを選択できます。

  このオプションをオンにすると、管理サーバーがオンになるとすぐにポーリングを開始します。

  このオプションをオフにすると、管理サーバーはポーリングの次回のスケジュールまでポーリングの実行を待機します。

  既定では、このオプションはオフです。

ドメインのセキュリティグループ内のユーザーアカウントを変更した場合、ドメインコントローラーをポーリングしてから1時間後に、これらの変更がKaspersky Security Centerに表示されます。

6. ［**保存**］をクリックして変更を適用します。
7. すぐにポーリングを実行するには、［**ポーリングを開始する**］をクリックします。

ディストリビューションポイントを使用したドメインコントローラーのポーリング

ディストリビューションポイントを使用して、Microsoft Active Directoryドメインコントローラーと Sambaドメインコントローラーをポーリングすることもできます。WindowsまたはLinuxベースの管理対象デバイスは、ディストリビューションポイントとして機能できます。

Linuxディストリビューションポイントの場合、Microsoft Active Directoryドメインコントローラーと Sambaドメインコントローラーのポーリングがサポートされています。
Windowsディストリビューションポイントの場合、Microsoft Active Directoryドメインコントローラーのポーリングのみがサポートされます。
Macディストリビューションポイントを使用したポーリングはサポートされていません。

ディストリビューションポイントを使用してドメインコントローラーのポーリングを設定するには：

1. ディストリビューションポイントのプロパティを開きます。
2. ［**ドメインコントローラーのポーリング**］セクションを選択します。
3. ［**ドメインコントローラーのポーリングを有効にする**］をオンにします。
4. ポーリングするドメインコントローラーを選択します。

   Linuxディストリビューションポイントを使用する場合は、［**指定したドメインのポーリング**］セクションで、［**追加**］をクリックし、ドメインコントローラーのアドレスとユーザー資格情報を指定します。

Windows ディストリビューションポイントを使用する場合は、次のオプションのいずれかをオンにできます：

- **現在のドメインのポーリング**
- **ドメインフォレスト全体のポーリング**
- **指定したドメインのポーリング**

5. 必要に応じて、［**ポーリングのスケジュールを設定する**］をクリックして、ポーリングスケジュールオプションを指定します。

   ポーリングは、指定されたスケジュールに従ってのみ開始されます。ポーリングを手動で開始することはできません。

ポーリングが完了すると、ドメイン構造が［**ドメインコントローラー**］セクションに表示されます。

デバイス移動ルールを設定しオンにしている場合、新たに検出されたデバイスは自動的に**管理対象デバイス**グループに含まれます。移動ルールがオンでない場合、新たに検出されたデバイスは自動的に**未割り当てデバイス**グループに含まれます。

検出されたユーザーアカウントは、Kaspersky Security Center Web コンソールでのドメイン認証に使用できます。

認証とドメインコントローラーへの接続

ドメインをポーリングする際の認証とドメインコントローラーへの接続

Linux ディストリビューションポイントを使用してドメインコントローラーをポーリングする時、ディストリビューションポイントは、ドメインコントローラーへの初期接続を確立するための接続プロトコルを識別します。このプロトコルは、ドメインコントローラーへの今後のすべての接続に使用されます。ドメインコントローラーへの初期接続を確立する時に、ネットワークエージェントフラグ（`KLNAG_LDAP_TLS_REQCERT` および `KLNAG_LDAP_SSL_CACERT`）を使用して接続オプションを変更できます。この記事で説明されているように、klscflag を使用してネットワークエージェントフラグを構成できます。

ドメインコントローラーへの最初の接続は次のように行われます：

1. Linux ディストリビューションポイントが、LDAPS 経由でドメインコントローラーに接続しようとします。

   既定では、証明書の検証は必要ありません。証明書の検証を実施するには、`KLNAG_LDAP_TLS_REQCERT` フラグを 1 に設定します。

   `KLNAG_LDAP_TLS_REQCERT` フラグに指定できる値：

   - `0` - 証明書が要求されますが、証明書が提供されない場合や証明書の検証が失敗した場合でも、TLS 接続は正常に作成されたと判断されます（既定値）。
   - `1` - LDAP サーバー証明書の厳密な検証が必要です。

   既定では、`KLNAG_LDAP_SSL_CACERT` フラグが指定されていない場合、OS 依存の認証局（CA）へのパスが証明書チェーンへのアクセスに使用されます。`KLNAG_LDAP_SSL_CACERT` フラグを使用してカスタムパスを指定します。

2. LDAPS 接続が失敗した場合、Linux ディストリビューションポイントは、SASL（DIGEST-MD5）を使用して暗号化されていない TCP 接続経由でドメインコントローラーへの接続をしようとします。

フラグの設定

klscflag ユーティリティを使用してフラグを設定できます。

Linux ディストリビューションポイントでは、コマンドラインを実行し、カレントディレクトリを klscflag ユーティリティのあるディレクトリに変更します。既定では、Linux ディストリビューションポイントの klscflag ユーティリティは /opt/kaspersky/ksc64/sbin にあります。

たとえば、次のコマンドは証明書の検証を強制します：

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Samba ドメインコントローラーの設定

Kaspersky Security Center は、Samba 4 上でのみ実行される Linux ドメインコントローラーをサポートします。

Samba ドメインコントローラーは、Microsoft Active Directory ドメインコントローラーと同じスキーマ拡張をサポートします。Samba 4 スキーマ拡張機能を使用すると、Samba ドメインコントローラーと Microsoft Active Directory ドメインコントローラーとの完全な互換性を有効にすることができます。これはオプションのアクションです。

Samba ドメインコントローラーと Microsoft Active Directory ドメインコントローラーの完全な互換性を有効にすることを推奨します。これにより、Kaspersky Security Center と Samba ドメインコントローラー間の適切な対話が保証されます。

Samba ドメインコントローラーと Microsoft Active Directory ドメインコントローラーの完全な互換性を有効にするには、次の手順を実行します：

1. RFC2307 スキーマ拡張を使用するには、次のコマンドを実行します：

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Samba ドメインコントローラーでスキーマのアップデートを有効にします。これを行うには、ファイル `/etc/samba/smb.conf` に以下の行を追加します。

   ```
   dsdb:schema update allowed = true
   ```

   スキーマのアップデートがエラーで完了した場合は、スキーママスターとして機能するドメインコントローラーの完全な復元を実行する必要があります。

Samba ドメインコントローラーを正しくポーリングするには、ファイル `/etc/samba/smb.conf` で `netbios name` と `workgroup` パラメータを指定する必要があります。

未割り当てデバイスの保持ルールの設定

Windows のネットワークポーリングの完了後、検出されたデバイスは［未割り当てデバイス］管理グループのサブグループに配置されます。［**検出と製品の導入**］ - ［**検出**］ - ［**Windows ドメイン**］の順に移動すると、この管理グループが見つかります。［**Windows ドメイン**］フォルダーが親グループです。この親グループ内に、ポーリングで検出された対応ドメインとワークグループに基づいて命名された子グループが含まれています。親グループにはモバイルデバイスの管理グループが含まれる場合もあります。親グループとそれぞれの子グループで、未割り当てデバイスの保持ルールを設定できます。保持ルールはデバイスの検出の設定には依存せず、デバイスの検出が無効な場合でも機能します。

デバイスの保持ルールは、ディスク全体の暗号化で暗号化された1つ以上のドライブを備えたデバイスには影響しません。このようなデバイスは自動的に削除されず、手動でのみ削除できます。暗号化されたドライブを含むデバイスを削除する必要がある場合は、まずドライブを復号化してから、デバイスを削除してください。

未割り当てデバイスの保持ルールを設定するには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**Windows ドメイン**］の順に選択します。
2. 次のいずれかの手順を実行します：
   - 親グループの設定を編集するには、［**プロパティ**］をクリックします。
     Windows ドメインのプロパティウィンドウが開きます。
   - 子グループの設定を編集するには、目的の子グループの名前をクリックします。
     子グループのプロパティウィンドウが開きます。
3. 次の設定を定義します：
   - **次の期間デバイスが不可視の場合グループから削除（日）**

     このオプションをオンにすると、デバイスをグループから自動的に削除するまでの期間を指定できます。既定では、この設定が子グループにも反映されます。既定の期間は 7 日です。

     既定では、このオプションはオンです。
   - **親グループから継承する**

     このオプションをオンにすると、デバイスの保持期間が設定が親グループから現在のグループに継承され、変更することはできません。

     このオプションは子グループでのみ利用できます。

     既定では、このオプションはオンです。
   - **子グループへ強制的に継承する**

     設定値が子グループに配信され、子グループのプロパティではそれらの設定がロックされます。

     既定では、このオプションはオフです。
4. ［**同意**］をクリックします。

変更内容が保存され、適用されます。

カスペルスキー製品：ライセンスとアクティベーション

このセクションでは、管理対象のカスペルスキー製品のライセンスを Kaspersky Security Center で操作する方法について説明します。

Kaspersky Security Center では、クライアントデバイスにカスペルスキー製品のライセンスを一元的に配信し、使用状況の監視およびライセンスの更新を実行できます。

Kaspersky Security Center でライセンスを追加すると、ライセンスの設定が管理サーバーで保存されます。アプリケーションでは、この情報に基づいて、ライセンス使用レポートを生成し、ライセンスの有効期限と、ライセンスのプロパティで設定されるライセンスの制限事項の違反について管理者に通知します。ライセンス使用の通知の設定は管理サーバーで設定できます。

管理対象アプリケーションのライセンスの管理

管理対象デバイスにインストールされているカスペルスキー製品には、各製品のライセンス情報ファイルまたはアクティベーションコードを適用してライセンスを付与する必要があります。ライセンス情報ファイルとアクティベーションコードは次の方法で展開できます：

- 自動配信
- 管理対象アプリケーションのインストールパッケージ
- 管理対象アプリケーションへの *ライセンスの追加*タスク
- 管理対象アプリケーションの手動アクティベーション

上記のいずれかの方法で、新しい現在のライセンスまたは予備のライセンスを追加できます。カスペルスキー製品は、現時点で現在のライセンスを使用し、現在のライセンスの有効期限が切れた後に適用する予備のライセンスを保存します。ライセンスを追加するアプリケーションは、ライセンスが現在のライセンスか予備のライセンスかを定義します。ライセンスの定義は、新しいライセンスの追加方法には依存しません。

自動配信

異なる複数の管理対象アプリケーションを使用し、特定のライセンス情報ファイルまたはアクティベーションコードをデバイスに配信する必要がある場合は、他の配信方法を選択してください。

Kaspersky Security Center を使用して、使用可能なライセンスをデバイスに配信できます。ここでは、3 個のライセンスが管理サーバーのリポジトリに保管されている場合を例にします。［**管理対象デバイスにライセンスを自動的に配信する**］を 3 個のライセンスすべてに対してオンにしていると仮定します。カスペルスキーのセキュリティ製品（例：Kaspersky Endpoint Security for Windows）が、組織内のデバイスにインストールされているとします。ライセンスを配信する必要がある新しいデバイスが検出されます。リポジトリ内に保管されている、名前がそれぞれ「*Key_1*」「*Key_2*」である 2 個のライセンス情報ファイルが、そのデバイスに配信可能であると本製品が判断します。そのうち 1 個のライセンス情報ファイルが、デバイスに配信されます。この場合、どのライセンス情報ファイルがデバイスに適用されるかは予測ができません。自動配信されるライセンスに対して、管理者が設定可能な項目がないからです。

ライセンスが配信されると、そのライセンスを適用中のデバイスの台数が再度計上されます。ライセンスが適用可能な台数を超えないように、適用中のデバイスの台数を確認しておく必要があります。ライセンスを適用可能な台数の上限を超えると、ライセンスが適用されていないデバイスのステータスが「*緊急*」になります。

配信前に、管理サーバーのリポジトリにライセンス情報ファイルまたはアクティベーションコードを追加する必要があります。

実行手順の説明：

- 管理コンソール：
  - ライセンスの管理サーバーリポジトリへの追加
  - ライセンスの自動配信

  または
- Kaspersky Security Center Web コンソール：
  - ライセンスの管理サーバーリポジトリへの追加
  - ライセンスの自動配信

次の場合、自動的に配布されたライセンスが仮想管理サーバーのリポジトリに表示されない場合があることに注意してください：

- ライセンスがアプリケーションに対して有効ではありません。
- 仮想管理サーバーには管理対象デバイスがありません。
- ライセンスは別の仮想管理サーバーによって管理されているデバイスに既に使用されており、デバイス数の制限に達しています。

ライセンス情報ファイルまたはアクティベーションコードを管理対象アプリケーションのインストールパッケージに追加

セキュリティ上の理由から、このオプションの使用は推奨されません。インストールパッケージに追加したライセンス情報ファイルまたはアクティベーションコードは、漏洩などの危険にさらされる可能性があります。

インストールパッケージを使用して管理対象アプリケーションをインストールする場合、パッケージ内またはアプリケーションのポリシー内に含まれるアクティベーションコードまたはライセンス情報ファイルを指定できます。ライセンスが管理対象デバイスに配信されるのは、デバイスと管理サーバーの次回の同期時です。

実行手順の説明：

- 管理コンソール：
  - インストールパッケージの作成
  - クライアントデバイスへのアプリケーションのインストール

  または

- Kaspersky Security Center Web コンソール：インストールパッケージへのライセンスの追加

管理対象アプリケーションへのライセンスの追加タスクを使用して配信

管理対象アプリケーションへの*ライセンスの追加*タスクを使用する場合、配信する必要があるライセンスを選択後、対象デバイスを都合のよい方法で選択できます。たとえば、管理グループを選択したり、デバイスの抽出を使用したりすることが可能です。

配信前に、管理サーバーのリポジトリにライセンス情報ファイルまたはアクティベーションコードを追加する必要があります。

実行手順の説明：

- 管理コンソール：
  - ライセンスの管理サーバーリポジトリへの追加
  - ライセンスのクライアントデバイスへの配信

  または
- Kaspersky Security Center Web コンソール：
  - ライセンスの管理サーバーリポジトリへの追加
  - ライセンスのクライアントデバイスへの配信

アクティベーションコードまたはライセンス情報ファイルを手動でデバイスに追加

インストール済みのカスペルスキー製品を、製品インターフェイス内のツールを使用してローカルでアクティベーションできます。詳しくは、インストールされているアプリケーションのヘルプを参照してください。

ライセンスの管理サーバーリポジトリへの追加

ライセンスを管理サーバーリポジトリに追加するには：

1. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。
2. ［**追加**］をクリックします。
3. 目的の対象を追加します：
   - **ライセンス情報ファイルの追加**
     ［**ライセンス情報ファイルの選択**］をクリックし、追加するライセンス情報ファイルを指定します。
   - **アクティベーションコードの入力**
     テキストフィールドにアクティベーションコードを入力し、［**送信**］をクリックします。
4. ［**閉じる**］をクリックします。

管理サーバーのリポジトリにライセンスが追加されます。

管理サーバーのライセンスの追加

管理サーバーのライセンスを追加するには：

1. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
2. 開いた［管理サーバーのプロパティ］ウィンドウで、［**ライセンス**］セクションを選択します。
3. ［**現在のライセンス**］セクションで、［**編集**］ボタンをクリックします。
4. 開いたウィンドウで、［**追加**］ボタンをクリックしてライセンスを追加します。
   ライセンス追加ウィザードが起動します。

ウィザードが完了したら、対応するライセンスに従って機能が管理コンソールに表示されるかどうかを確認できます。

ライセンスのクライアントデバイスへの配信

Kaspersky Security Center Web コンソールでは、ライセンスをクライアントデバイスに自動的に、または［**アプリケーションのアクティベーション**］タスクを通じて配信することができます。このタスクを使用して、特定のデバイスグループにライセンスを配信できます。タスク経由でライセンスが配信される際、デバイス数へのライセンスの制限が適用されません。自動ライセンス配信を使用すると、ライセンス制限に達した時にライセンスの配信を自動的に停止できます。

ライセンスの自動配信を有効にする場合は、そのライセンスをクライアントデバイスに配信するための［**アプリケーションのアクティベーション**］タスクを作成しないでください。そうしないと、頻繁な同期により管理サーバーの負荷が増加します。

配信前に、ライセンスを管理サーバーリポジトリに追加します。

*［**アプリケーションのアクティベーション**］タスクを使用してクライアントデバイスにライセンスを配信するには、次の手順を実行します：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. ［**アプリケーション**］ドロップダウンリストで、ライセンスを追加する製品を選択します。
4. ［**タスク種別**］リストから、［**アプリケーションのアクティベーション**］タスクを選択します。
5. ［**タスク名**］フィールドに、新しいタスクの名前を指定します。
6. ［タスクを割り当てるデバイス］を選択します。
7. ウィザードの［**ライセンス情報ファイルの選択**］手順で、［**ライセンスの追加**］リンクをクリックしてライセンスを追加します。

8. ［ライセンスの追加］ペインで、次のいずれかのオプションを使用してライセンスを追加します：

ライセンスを追加する必要があるのは、［**アプリケーションのアクティベーション**］タスクを作成する前にライセンスを管理サーバーのリポジトリに追加しなかった場合のみです。

- ［**アクティベーションコードの入力**］オプションを選択してアクティベーションコードを入力し、次の手順を実行します：

  a. アクティベーションコードを指定して［**送信**］ボタンをクリックしてください。
  ライセンスに関する情報が［ライセンスの追加］ペインに表示されます。

  b. ［**保存**］をクリックします。

  ライセンスを管理対象デバイスに自動的に配信する場合は、［**管理対象デバイスにライセンスを自動配信する**］オプションを有効にします。

  ［ライセンスの追加］ペインが閉じます。

- ［**ライセンス情報ファイルの追加**］オプションを選択してライセンスファイルを追加し、次の操作を実行します：

  a. ［**ライセンス情報ファイルの選択**］ボタンをクリックします。

  b. ［ライセンス情報ファイルの選択］ウィンドウが開いたら、ライセンス情報ファイルを選択し、［**開く**］をクリックします。
  ライセンスに関する情報が［ライセンスの追加］ペインに表示されます。

  c. ［**保存**］をクリックします。

  管理対象デバイスにライセンスを自動的に配信する場合は、［**管理対象デバイスにライセンスを自動配信する**］オプションを有効にします。

  ［ライセンスの追加］ペインが閉じます。

9. ライセンスのテーブルで［ライセンス］を選択します。

10. ウィザードの［**ライセンス情報**］手順で、現在のライセンスを置き換える場合は、既定の［**予備のライセンスとして使用する**］をオフにします。
  たとえば、組織が変更され、デバイスで別の組織のライセンスが必要な場合や、ライセンスが再発行され、新しいライセンスの有効期限が現在のライセンスよりも早く切れる場合に、これが必要になります。エラーを回避するには、［**予備のライセンスとして使用する**］をオフにする必要があります。
  Kaspersky Security Center にライセンスを追加する際に発生する可能性のある問題とその解決方法の詳細については、Kaspersky Security Center ナレッジベースを参照してください。

11. ウィザードの［**タスク作成の終了**］ステップで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。
  このオプションをオンにしない場合、タスクは既定の設定で作成されます。既定の設定からの変更は、後からいつでも実行できます。

12. ［**終了**］をクリックします。

ウィザードではタスクを作成します。［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスクのプロパティウィンドウが自動的に表示されます。このウィンドウでは、［一般的なタスク設定］を指定し、必要に応じてタスク作成時に指定した設定を変更できます。

タスクのリストで作成されたタスクの名前をクリックして、タスクのプロパティウィンドウを開くこともできます。

タスクが作成、設定され、タスクリストに表示されます。

13. タスクを実行するには、タスクリストで目的のタスクを選択し、［**開始**］をクリックします。
    タスクのプロパティウィンドウの［**スケジュール**］タブでタスクの開始スケジュールを設定することもできます。
    スケジュール開始設定の詳細については、「タスクの一般設定」を参照してください。

タスクが完了すると、選択したデバイスにライセンスが導入されます。

ライセンスの自動配信

Kaspersky Security Center では、管理サーバーのライセンスリポジトリにあるライセンスを管理対象デバイスに自動配信できます。

管理対象デバイスにライセンスを自動配信するには：

1. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。
2. デバイスに自動配信するライセンスをクリックします。
3. 表示されるライセンスのプロパティウィンドウで［**管理対象デバイスにライセンスを自動的に配信する**］をオンにします。
4. ［**保存**］をクリックします。

ライセンスは、互換性のあるすべてのデバイスに自動的に配信されます。

ライセンスはネットワークエージェント経由で配信されます。アプリケーションに対するライセンスの配信タスクは作成されません。

ライセンスが自動配信される際、デバイス数へのライセンスの制限が適用されます。ライセンスの制限は、ライセンスのプロパティで設定済みです。ライセンス数の上限に達した場合は、デバイスへの配信は自動的に停止します。

次の場合、自動的に配布されたライセンスが仮想管理サーバーのリポジトリに表示されない場合があることに注意してください：

- ライセンスがアプリケーションに対して有効ではありません。
- 仮想管理サーバーには管理対象デバイスがありません。
- ライセンスは別の仮想管理サーバーによって管理されているデバイスに既に使用されており、デバイス数の制限に達しています。

仮想管理サーバーは、そのリポジトリと管理サーバーのリポジトリからライセンスを自動的に配布します。以下を推奨します。

- *ライセンスの追加*タスクを使用して、デバイスに導入する必要があるライセンスを選択します。
- 仮想管理サーバーの設定で、［**この仮想管理サーバーからデバイスへのライセンスの自動配信を許可する**］をオフにしないでください。オフにした場合、仮想管理サーバーは、管理サーバーリポジトリからのライセンスを含め、ライセンスをデバイスに配布しません。

ライセンスのプロパティウィンドウで［**管理対象デバイスにライセンスを自動的に配信する**］がオンになっている場合、ライセンスキーはネットワークにすぐに配布されます。このオプションを選択しない場合は、後でタスクを使用してライセンスを配信することができます。

プライマリ管理サーバー上で構成されたライセンスの自動配信は、非仮想セカンダリ管理サーバーによって管理されるデバイスには適用されません。

使用中のライセンスに関する情報の表示

管理サーバーのリポジトリに追加されているライセンスのリストを表示するには：

メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。

管理サーバーのリポジトリに追加されているライセンス情報ファイルとアクティベーションコードのリストが表示されます。

ライセンスの詳細情報を表示するには：

1. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。
2. 目的のライセンスの名前をクリックします。

ライセンスのプロパティウィンドウが表示され、次の情報を確認できます：

- ［**全般**］タブ：ライセンスに関する主要な情報
- ［**デバイス**］タブ：このライセンスが、インストールされているカスペルスキー製品のアクティベーションに使用されたクライアントデバイスのリスト

特定のクライアントデバイスにどのライセンスが追加されたかを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
2. 目的のデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**アプリケーション**］タブをクリックします。
4. ライセンスの情報を確認するアプリケーションの名前をクリックします。
5. 表示されるアプリケーションのプロパティウィンドウで、［**全般**］タブを選択し、［**ライセンス**］セクションを表示します。

現在のライセンスと予備のライセンスに関する主要な情報が表示されます。

仮想管理サーバーのライセンスの最新の設定を定義するため、管理サーバーはカスペルスキーのアクティベーションサーバーに少なくとも毎日1度はリクエストを送信します。システムDNSを使用したサーバーへのアクセスが不可能な場合は、パブリックDNSサーバーが使用されます。

リポジトリからのライセンスの削除

管理サーバーの基本機能には含まれない追加機能（例：脆弱性とパッチ管理およびモバイルデバイス管理）の現在のライセンスを削除すると、該当する機能は使用できなくなります。予備のライセンスが追加されている場合、予備のライセンスは、前の現在のライセンスが削除された後、自動的に現在のライセンスになります。

管理対象デバイスに追加済みの現在のライセンスを管理サーバーのリポジトリから削除した場合、管理対象デバイスにインストールされている製品は動作を継続します。

管理サーバーのリポジトリからライセンス情報ファイルまたはアクティベーションコードを削除するには：

1. 削除するライセンス情報ファイルまたはアクティベーションコードが管理サーバーで使用されていないことを確認します。管理サーバーで使用されている場合、ライセンスを削除することはできません。チェックを実行するには：

   a. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

   b. ［**全般**］タブで、［**ライセンス**］セクションを選択します。

   c. 開いたセクションに必要なライセンス情報ファイルまたはアクティベーションコードが表示されている場合は、［**現在のライセンスの削除**］をクリックし、処理内容を確定します。その後、削除されたライセンスが管理サーバーで使用されることはありませんが、ライセンスは管理サーバーのリポジトリに残ります。必要なライセンス情報ファイルまたはアクティベーションコードが表示されない場合、管理サーバーはこのライセンスを使用していません。

2. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。

3. 必要なライセンス情報ファイルまたはアクティベーションコードを選択し、［**削除**］をクリックします。

選択したライセンス情報ファイルまたはアクティベーションコードが削除されます。

削除されたライセンスの再追加や、新しいライセンスの追加も可能です。

使用許諾契約書による同意の取り消し

一部のクライアントデバイスの保護を停止する場合、任意の管理対象カスペルスキー製品の使用許諾契約書（EULA）への同意を取り消すことができます。EULAへの同意を取り消す前に、選択したアプリケーションをアンインストールする必要があります。

仮想管理サーバー上でのEULAへの同意は、仮想管理サーバーまたはプライマリ管理サーバーで取り消すことができます。プライマリ管理サーバー上でのEULAへの同意は、プライマリ管理サーバー上でしか取り消すことはできません。

管理対象のカスペルスキー製品のEULAを取り消すには：

1. 管理サーバーのプロパティウィンドウを開き、［**全般**］タブの［**使用許諾契約書**］セクションに移動します。

   インストールパッケージの作成時、アップデートのシームレスインストール時、または Kaspersky Security for Mobile の導入時に同意した EULA のリストが表示されます。

2. リストから、同意を取り消す EULA を選択します。

   EULA の以下のプロパティを確認できます：

   - EULA に同意した日付
   - EULA に同意したユーザーの名前

3. EULA に同意した日付のうち任意のものをクリックし、次のデータが表示されるプロパティウィンドウを開きます：

   - EULA に同意したユーザーの名前
   - EULA に同意した日付
   - EULA の一意な識別子（UID）
   - EULA のテキスト
   - EULA に関連するオブジェクト、および各オブジェクトの名前と種別のリスト（インストールパッケージ、シームレスアップデート、モバイルアプリ）

4. EULA のプロパティウィンドウの下部で、［**使用許諾契約書への同意を取り消す**］をクリックします。

   > EULA への同意の取り消しを妨げるオブジェクト（インストールパッケージ、およびそのパッケージを使用するタスク）が存在する場合、そのオブジェクトに関する通知が表示されます。これらのオブジェクトを削除するまで、取り消しの動作を続行できません。

   表示されたウィンドウで、この EULA に対応するカスペルスキー製品を最初にアンインストールすることが必要であることが示されます。

5. ボタンをクリックして取り消しを確定します。

これで EULA が取り消されました。［**使用許諾契約書** ］セクションの使用許諾契約書のリストに表示されなくなります。EULA のプロパティウィンドウが閉じ、製品がインストールされなくなります。

カスペルスキー製品のライセンスの更新

有効期間の終了した、または有効期間がまもなく終了する（残り 30 日以内）のカスペルスキー製品のライセンスを更新できます。

有効期間が終了した、もしくは有効期間がまもなく終了するライセンスを更新するには：

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。

- ［**監視とレポート**］→［**ダッシュボード**］の順に移動し、通知に隣接する［**有効期間がまもなく終了するライセンスを表示**］をクリックします。

［**カスペルスキーのライセンス**］ウィンドウが表示され、ライセンスを表示および更新できます。

2. 目的のライセンスに隣接する［**ライセンスの更新**］をクリックします。

ライセンスの更新リンクをクリックすることで、お客様はカスペルスキーに次の情報を送信することに同意したものとします：バージョン、使用中の言語版、本ソフトウェアのライセンス識別子（更新しているライセンスの識別子）、および本製品を販売代理店経由でライセンスを購入したかどうかの情報。

3. 表示されるライセンス更新サービスのウィンドウで、ライセンスを更新する手順に従ってください。

ライセンスが更新されました。

Kaspersky Security Center Web コンソールでは、ライセンスの有効期間の終了間近になると次のスケジュールで通知が表示されます：

- 有効期限の 30 日前
- 有効期限の 7 日前
- 有効期限の 3 日前
- 有効期限の 24 時間前
- ライセンスの有効期間が終了した時

マーケットプレイスを使用してカスペルスキーの法人向けソリューションを選択する

［**マーケットプレイス**］はカスペルスキーのビジネスソリューションを全体的に表示できるメインメニューのセクションです。必要なものを選択してカスペルスキーの Web サイトに移動して購入プロセスに進むことができます。フィルターを使用してお客様の組織や情報セキュリティシステムの要件に一致するソリューションのみを表示することが可能です。ソリューションを選択すると、Kaspersky Security Center はそのソリューションの詳細について関連する Web ページにリダイレクトします。各 Web ページで、製品の購入に進んだり、購入に関する手順を確認したりできます。

［**マーケットプレイス**］セクションでは、次の条件を使用してカスペルスキー製品をフィルターすることができます：

- 保護対象のデバイスの数（エンドポイント、サーバー、その他の種別の資産）：
  - 50～250
  - 250～1000
  - 1000 以上
- 組織の情報セキュリティチームの成熟度：
  - **基本のセキュリティ**

このレベルはIT チームを1つのみ持つ企業に典型的なレベルです。脅威は、自動的に可能な最大数ブロックされます。

- **最適なセキュリティ**

  このレベルはIT チーム内にIT セキュリティ機能を持つ特定のIT チームを持つ企業に典型的なレベルです。このレベルでは、企業はコモディティ型の脅威や既存の防御メカニズムを回避する脅威などに対応するソリューションを必要とします。

- **高度なセキュリティ**

  このレベルは複雑で分散化されたIT 環境を持つ機能に典型的なレベルです。IT セキュリティチームの熟練度が高い、または企業がSOC（セキュリティオペレーションセンター）チームを持っているなどのレベルです。必要とされるソリューションは、複雑な脅威および標的型攻撃に対応するものです。

- 保護対象の資産の種別：

  - **エンドポイント**：物理および仮想マシン、埋め込みシステムなどの社員のワークステーション
  - **サーバー**：物理および仮想サーバー
  - **クラウド**：パブリック、プライベート、またはハイブリッドのクラウド環境およびクラウドサービス
  - **ネットワーク**：ローカルエリアネットワーク、IT インフラストラクチャ
  - **サービス**：カスペルスキーによって提供されるセキュリティ関連のサービス

カスペルスキーのビジネスソリューションを検索および購入するには：

1. メインメニューで、［**マーケットプレイス**］に移動します。

   既定では、セクションにはすべての使用可能なカスペルスキーのビジネスソリューションが表示されています。

2. 企業に合ったソリューションのみを表示するには、フィルターで必要な値を選択します。

3. 購入する、もしくは詳細を確認したいソリューションをクリックします。

   ソリューションのWeb ページにリダイレクトされます。画面上の説明に従って、購入プロセスを進められます。

ネットワーク保護の設定

このセクションには、ポリシーとタスクの手動設定、ユーザーロール、管理グループの構造とタスクの階層構造の構築に関する情報を記載しています。

シナリオ：ネットワーク保護の設定

クイックスタートウィザードにより、既定の設定でポリシーとタスクが作成されます。これらの設定は、組織のルールなどに照らして最適でない、または許容できない内容を含む可能性があります。したがって、ネットワークの必要性に応じて、これらのポリシーとタスクを調整し、他のポリシーとタスクを作成してください。

必須条件

導入を開始する前に、次が完了していることを確認してください：

- Kaspersky Security Center 管理サーバーをインストール済み
- Kaspersky Security Center Web コンソールをインストール済み（任意）
- Kaspersky Security Center の主要なインストールシナリオを完了済み
- クイックスタートウィザードを完了済みまたは［**管理対象デバイス**］管理グループで以下のポリシーとタスクを手動で作成済み：
  - Kaspersky Endpoint Security のポリシー
  - Kaspersky Endpoint Security をアップデートするグループタスク
  - ネットワークエージェントのポリシー
  - *脆弱性とアプリケーションのアップデートの検索*タスク

ネットワーク保護の設定は、次の手順で進みます：

1. **カスペルスキー製品のポリシーとポリシーのプロファイルの設定と各デバイスへの反映**

   管理対象デバイスにインストールされているカスペルスキー製品のポリシーとポリシーのプロファイルを設定しデバイスに反映するには、デバイスベースとユーザーベースの 2 種類のセキュリティ管理方法を使用できます。これらの 2 つの管理方法を組み合わせることもできます。デバイスベースのセキュリティ管理を実施するには、MMC ベースの管理コンソールまたは Kaspersky Security Center Web コンソールで提供されているツールを使用できます。ユーザーベースのセキュリティ管理は、Kaspersky Security Center Web コンソールでのみ実施できます。

2. **カスペルスキー製品のリモート管理用のタスクの設定**

   必要に応じて、クイックスタートウィザードを使用して作成したタスクを確認、調整します。

   実行手順の説明：

   - 管理コンソール：
     - Kaspersky Endpoint Security をアップデートするグループタスクの設定
     - 脆弱性とアプリケーションのアップデートの検索タスクのスケジュール設定
   - Kaspersky Security Center Web コンソール：
     - Kaspersky Endpoint Security をアップデートするグループタスクの設定
     - 脆弱性とアプリケーションのアップデートの検索タスクの設定

   必要に応じて、クライアントデバイスにインストールされているカスペルスキー製品を管理するためのタスクを追加で作成します。

3. **データベースでのイベント情報による負荷の評価と制限**

   管理対象アプリケーションの動作中のイベントに関する情報は、クライアントデバイスから送信され、管理サーバーデータベースに記録されます。管理サーバーの負荷を軽減するには、データベースに保管される可能性のあるイベント数の最大値を評価し、上限を設定します。

   実行手順の説明：

- 管理コンソール：イベント数の上限の設定
- Kaspersky Security Center Web コンソール：イベント数の上限の設定

結果

この手順を完了すると、カスペルスキー製品、タスク、管理サーバーで取得されるイベントの設定によってネットワークの保護が機能するようになります。

- ポリシーとポリシーのプロファイルに従ってカスペルスキー製品が設定されます。
- 製品が一連のタスクによって管理されるようになります。
- データベースに保存されるイベント数の上限が設定されます。

ネットワーク保護の設定が完了すると、定義データベースとカスペルスキー製品の定期アップデートの設定ステップに進むことができます。

Kaspersky Sandbox により検知された脅威への自動応答を設定する方法の詳細は、Kaspersky Sandbox 2.0 のオンラインヘルプを参照してください。

デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理の概要

セキュリティ設定を、デバイスの仕様の観点やユーザーロールの観点から管理できます。1つ目のアプローチは*デバイスベースのセキュリティ管理*、2つ目のアプローチは*ユーザーベースのセキュリティ管理*と呼ばれます。異なるデバイスに異なる設定を適用するには、いずれかの管理方法あるいは両者を組み合わせた管理方法を使用できます。デバイスベースのセキュリティ管理を実施するには、MMC ベースの管理コンソールまたは Kaspersky Security Center Web コンソールで提供されているツールを使用できます。ユーザーベースのセキュリティ管理は、Kaspersky Security Center Web コンソールでのみ実施できます。

デバイスベースのセキュリティ管理では、デバイスごとの状況などに合わせて、セキュリティ製品について複数の異なる設定を管理対象デバイスに適用できます。たとえば、異なる管理グループに属するデバイスに、異なる設定を適用できます。あるいは、Active Directory でデバイスに割り当てられている用途や、ハードウェアの仕様などに応じて、デバイスを区分することもできます。

ユーザーベースのセキュリティ管理を使用すると、ユーザーロールに応じて、異なるセキュリティ設定を適用できます。複数のユーザーロールを作成し、ユーザーごとに適切なユーザーロールを割り当てた上で、デバイスの所有者のユーザーロールに応じて、異なるセキュリティ設定をデバイスに適用できます。たとえば、経理部門の従業員と人事部門の従業員それぞれのデバイスに異なるアプリケーション設定を適用する場合などがありえます。これにより、ユーザーベースのセキュリティ管理を実施すると、経理部門の従業員と人事部門の従業員のカスペルスキー製品に対して、それぞれ独自の設定が適用されます。詳細設定により、製品設定のどの部分をユーザー側で設定でき、どの部分は管理者による設定が強制的に適用されるかを指定できます。

ユーザーベースのセキュリティ管理を使用すると、特定の1人のユーザーに特定の製品設定を適用できます。該当する従業員が社内で固有のロールを担っていたり、特定のユーザーのデバイスに関連したセキュリティ問題を監視したい場合などに、こうした処理が必要になることがあります。社内でのこの従業員のロールに基づいて、ユーザーが製品設定を変更できる権限を拡張したり制限できます。たとえば、ローカルオフィスのクライアントデバイスを管理しているシステム管理者の権限を拡張する場合などです。

デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理を組み合わせることもできます。たとえば、管理グループごとに製品ポリシーを設定した上で、企業内の1つ以上のユーザーロールを対象としたポリシープロファイルを作成するなどの方法を使用できます。この場合、ポリシーとポリシープロファイルは次の順序で適用されます。

1. デバイスベースのセキュリティ管理用に作成されたポリシーが適用されます。
2. ポリシーは、ポリシープロファイルの優先度に応じてポリシープロファイルで変更されます。
3. ポリシーは、ユーザーロールと関連付けられたポリシープロファイルで変更されます。

ポリシーの設定と継承先への反映：デバイスベースの管理

この手順を完了すると、すべての管理対象デバイスにインストールされている製品が、定義した製品ポリシーとポリシープロファイルに従って設定されます。

必須条件

手順を開始する前に、Kaspersky Security Center 管理サーバーと Kaspersky Security Center Web コンソール（任意）のインストールが完了していることを確認してください。Kaspersky Security Center Web コンソールをインストールしている場合、デバイスベースの管理方法の代替案もしくは追加で組み合わせて使用する管理方法としてユーザーベースのセキュリティ管理も検討すると有益な場合があります。

実行するステップ

カスペルスキー製品のデバイスベースの管理シナリオは、次の 2 つの手順からなります。

1 製品ポリシーの設定

管理対象デバイスにインストールされているカスペルスキー製品ごとにポリシーを作成して、製品の設定を指定します。これらのポリシーはクライアントデバイスに反映されます。

クイックスタートウィザードを使用してネットワークの保護を設定する場合、Kaspersky Security Center は次のアプリケーションの既定のポリシーを作成します：

- Kaspersky Endpoint Security for Windows - Windows ベースのクライアントデバイス用
- Kaspersky Endpoint Security for Linux - Linux ベースのクライアントデバイス用

このウィザードを使用して設定プロセスを完了した場合、この製品の新しいポリシーを作成する必要はありません。Kaspersky Endpoint Security ポリシーの手動セットアップに進みます。

複数の管理サーバーと管理グループからなる階層構造が存在する場合、既定では、セカンダリ管理サーバーと子管理グループはプライマリ管理サーバーのポリシーを継承します。子グループとセカンダリ管理サーバーでの継承を強制的に適用して、上位のポリシーで指定された設定の変更を禁止することもできます。一部の設定のみを強制的に継承させたい場合は、上位のポリシーで該当する設定項目をロックできます。残りのロックされていない設定は下位のポリシーで変更できます。ポリシーの階層を作成することで、管理グループ内の管理対象デバイスを効果的に管理できます。

実行手順の説明：

- 管理コンソール： ポリシーの作成
- Kaspersky Security Center Web コンソール：ポリシーの作成

2. **ポリシーのプロファイルの作成（任意）**

   同じ管理グループ内にあるデバイスを異なるポリシー設定に従って動作させる場合には、ポリシーのプロファイルを作成します。ポリシーのプロファイルには、ポリシー設定のサブセットが指定されています。このサブセットはポリシーとともに対象デバイスに配信され、*プロファイルの有効化条件*と呼ばれる特定の条件下でポリシーを補完する機能を果たします。プロファイルに含まれるのは、管理対象デバイスでアクティブな「基本」ポリシーとは異なる設定（差分）のみです。

   プロファイルの有効化条件を使用することで、たとえば、Active Directory の特定の組織単位やセキュリティグループに属するデバイス、特定のハードウェア設定のデバイス、特定のタグが付与されているデバイスなどの条件に応じて異なるポリシープロファイルを適用できます。タグを使用すると特定の基準を満たすデバイスをフィルタリングできます。たとえば、「*Windows*」というタグを作成し、Windows オペレーティングシステムを実行しているデバイスすべてにこのタグを付与し、ポリシープロファイルの有効化条件としてこのタグを指定します。これにより、Windows を実行しているすべてのデバイスにインストールされているカスペルスキー製品は該当するポリシープロファイルで管理されます。

   実行手順の説明：

   - 管理コンソール：
     - ポリシーのプロファイルの作成
     - ポリシーのプロファイルの有効化ルールの作成
   - Kaspersky Security Center Web コンソール：
     - ポリシーのプロファイルの作成
     - ポリシーのプロファイルの有効化ルールの作成

3. **ポリシーとポリシープロファイルの管理対象デバイスへの反映**

   既定では、管理サーバーは 15 分ごとに管理対象デバイスと自動的に同期します。自動同期を回避して、［強制同期］コマンドを使用して手動で同期を実行できます。また、ポリシーまたはポリシープロファイルを作成または変更すると、同期が強制的に行われます。同期中に、新しいまたは変更されたポリシーとポリシープロファイルが管理対象デバイスに反映されます。

   Kaspersky Security Center Web コンソールを使用する場合、ポリシーとポリシーのプロファイルがデバイスに配信されたかを確認できます。Kaspersky Security Center では、デバイスのプロパティで該当する配信日時が表示されます。

   実行手順の説明：

   - 管理コンソール：強制同期
   - Kaspersky Security Center Web コンソール：強制同期

実行結果

デバイスベースの管理の導入手順が完了すると、ポリシーの階層を通して指定または反映された設定がカスペルスキー製品に適用されます。

管理グループに新しく追加されたデバイスには、設定された製品ポリシーとポリシープロファイルが自動的に適用されます。

ポリシーの設定と継承先への反映：ユーザーベースの管理

このセクションでは、管理対象デバイスにインストールされているカスペルスキー製品の設定をユーザーベースで一元的に行う手順について説明します。この手順を完了すると、すべての管理対象デバイスにインストールされている製品が、定義した製品ポリシーとポリシープロファイルに従って設定されます。

このシナリオは Kaspersky Security Center Web コンソールのバージョン 13 以降で実装可能です。

必須条件

手順を開始する前に、Kaspersky Security Center 管理サーバーのインストールと Kaspersky Security Center Web コンソールのインストールが正常に完了しており、さらに主要な導入シナリオが完了していることを確認してください。また、ユーザーベースの管理方法の代替案もしくは追加で組み合わせて使用する管理方法としてデバイスベースのセキュリティ管理も検討すると有益な場合があります。2 種類の管理方法について詳しくは、こちらのページを参照してください。

プロセス

カスペルスキー製品のユーザーベースの管理シナリオは、次の 2 つの手順からなります。

1. **製品ポリシーの設定**

   管理対象デバイスにインストールされているカスペルスキー製品ごとにポリシーを作成して、製品の設定を指定します。これらのポリシーはクライアントデバイスに反映されます。

   クイックスタートウィザードを使用してネットワークの保護を設定する場合、Kaspersky Security Center は Kaspersky Endpoint Security の既定のポリシーを作成します。このウィザードを使用して設定プロセスを完了した場合、この製品の新しいポリシーを作成する必要はありません。Kaspersky Endpoint Security ポリシーの手動セットアップに進みます。

   複数の管理サーバーと管理グループからなる階層構造が存在する場合、既定では、セカンダリ管理サーバーと子管理グループはプライマリ管理サーバーのポリシーを継承します。子グループとセカンダリ管理サーバーでの継承を強制的に適用して、上位のポリシーで指定された設定の変更を禁止することもできます。一部の設定のみを強制的に継承させたい場合は、上位のポリシーで該当する設定項目をロックできます。残りのロックされていない設定は下位のポリシーで変更できます。ポリシーの階層を作成することで、管理グループ内の管理対象デバイスを効果的に管理できます。

   実行手順の説明：ポリシーの作成

2. **デバイスの所有者の指定**

   管理対象デバイスを対応するユーザーに割り当てます。

   実行手順の説明：デバイスの所有者ユーザーの指定

3. **組織内の主なユーザーロールの定義**

   組織内の従業員が行う様々な業務の主要なものを検討します。すべての従業員がロールに従って振り分けられるようにする必要があります。たとえば、所属部門、職務内容、役職などで振り分けを行うことができます。この検討が完了したら、各グループに対応するユーザーロールを作成する必要があります。各ユーザーロールには、そのロールに固有の製品設定を含む独自のポリシープロファイルが割り当てられることを念頭において作業してください。

4. **ユーザーロールの作成**

   前の手順で定義した従業員のグループごとにユーザーロールの作成と設定を行うか、あるいは事前定義されたユーザーロールを使用します。ユーザーロールには製品の各機能に対するアクセス権限が組み合わされたかたちで付与されます。

   実行手順の説明：ユーザーロールの作成

5. **各ユーザーロールの対象範囲の指定**

   作成したユーザーロールごとに、ロールを割り当てるユーザーやセキュリティグループ、管理グループを指定します。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

   実行手順の説明：各ユーザーロールの対象範囲の編集

6. **ポリシーのプロファイルの作成**

   組織内のユーザーロールごとに、ポリシープロファイルを作成します。ポリシープロファイルによって、ユーザーのデバイスにインストールされている製品にユーザーロールに応じてどの設定が適用されるかが定義されます。

   実行手順の説明：ポリシープロファイルの作成

7. **ポリシープロファイルとユーザーロールの関連付け**

   作成したポリシープロファイルをユーザーロールに関連付けます。完了すると、指定されたロールを割り当てられたユーザーに対してポリシープロファイルが有効になります。ユーザーのデバイスにインストールされているカスペルスキー製品に、ポリシープロファイルで指定した設定が適用されます。

   実行手順の説明：ポリシーのプロファイルとロールの関連付け

8. **ポリシーとポリシープロファイルの管理対象デバイスへの反映**

   既定では、管理サーバーは 15 分ごとに管理対象デバイスと自動的に同期します。同期中に、新しいまたは変更されたポリシーとポリシープロファイルが管理対象デバイスに反映されます。自動同期を回避して、［強制同期］コマンドを使用して手動で同期を実行できます。同期が完了すると、ポリシーとポリシープロファイルが配信され、インストールされているカスペルスキー製品に適用されます。

   ポリシーとポリシーのプロファイルがデバイスに配信されたかを確認できます。Kaspersky Security Center では、デバイスのプロパティで該当する配信日時が表示されます。

   実行手順の説明：強制同期

結果

ユーザーベースの管理の導入手順が完了すると、ポリシーの階層を通して指定または反映された設定がカスペルスキー製品に適用されます。

新規ユーザーに対しては、新しいアカウントを作成して作成済みのユーザーロールのいずれかを割り当て、デバイスをユーザーに割り当てる必要があります。このユーザーのデバイスには、設定された製品ポリシーとポリシープロファイルが自動的に適用されます。

ネットワークエージェントのポリシー設定

ネットワークエージェントのポリシーを設定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. ネットワークエージェントポリシーの名前をクリックします。
   ネットワークエージェントポリシーのプロパティウィンドウが表示されます。

Windows、macOS、および Linux ベースのデバイスでは、様々な設定が使用可能であることを考慮してください。

全般

このタブでは、ポリシーステータスを変更したり、継承ポリシーを設定したりすることができます：

- ［**ポリシーのステータス**］で、ポリシーのステータスを選択します：
  - **アクティブ**

    このオプションをオンにすると、ポリシーがアクティブになります。

    既定では、このオプションがオンです。

  - **非アクティブ**

    このオプションをオンにすると、ポリシーは非アクティブになりますが［**ポリシー**］フォルダーに保持されます。必要に応じて、ポリシーをアクティブにすることができます。

- ［**設定の継承**］セクションでは、ポリシーの継承を設定できます。
  - **親ポリシーから設定を継承する**

    このオプションをオンにすると、ポリシーの設定値は上位レベルグループのポリシーから継承されるため、ロックされます。

    既定では、このオプションはオンです。

  - **設定を子ポリシーへ強制的に継承させる**

    このオプションをオンにすると、ポリシーの変更を適用した後に次の処理が実行されます：
    - 管理サブグループのポリシー（子ポリシー）に、ポリシーの設定値が継承されます。
    - 各子ポリシーのプロパティウィンドウの［**全般**］セクションにある［**設定の継承**］ブロックで、［**親ポリシーから設定を継承する**］が自動的にオンになります。

    このオプションをオンにすると、子ポリシーの設定はロックされます。

    既定では、このオプションはオフです。

イベントの設定

このタブでは、イベントの記録と通知を設定できます。イベントは、［**イベントの設定**］タブの次のセクションの重要度に応じて配信されます：

- **機能エラー**
- **警告**
- **情報**

それぞれのセクションのイベント種別リストには、イベントの種別と、管理サーバーでイベントが保存される既定の日数が表示されます。イベント種別をクリックすると、リストで選択したイベントについてのイベントログとイベント通知を設定できます。既定では、すべてのイベントで、管理サーバー全体を対象に指定された共通の通知設定が使用されます。しかしながら、目的のイベント種別の特定の設定を変更できます。

たとえば、［**警告**］セクションでは、［**セキュリティ問題が発生しました**］イベント種別の設定を編集できます。このようなイベントは、たとえばディストリビューションポイントのディスク空き容量が 2 GB 未満の場合などに発生します（アプリケーションのインストール、アップデートのダウンロードをリモートで実行するには、少なくとも 4 GB が必要となります）。［**セキュリティ問題が発生しました**］イベントをクリックし、発生したイベントを保存する場所とその通知方法を指定します。

ネットワークエージェントがセキュリティ問題を検知した場合は、管理対象デバイスの設定を使用してこの問題を管理できます。

アプリケーション設定

設定

［**設定**］セクションでは、ネットワークエージェントのポリシーを設定できます。

- **ディストリビューションポイント経由でのみファイルを配信する**

  このオプションをオンにすると、管理対象デバイスのネットワークエージェントはディストリビューションポイントからのみアップデートを取得します。

  このオプションをオフにすると、管理対象デバイス上のネットワークエージェント ディストリビューションポイントまたは管理サーバーからアップデートを取得します。

  管理対象デバイスのセキュリティ製品は、各セキュリティ製品のアップデートタスクで設定されたアップデート元からアップデートを取得することに注意してください。［**ディストリビューションポイント経由でのみファイルを配信する**］を有効にする場合、Kaspersky Security Center がアップデートタスクのアップデート元に設定されていることを確認してください。

  既定では、このオプションはオフです。

- **イベントキュー最大サイズを MB で指定**

  このフィールドでは、イベントキューが使用できるドライブの最大サイズを指定できます。

  既定値は 2 メガバイト（MB）です。

- **アプリケーションがポリシーの拡張データをデバイスから取得可能である**

管理対象デバイスにインストールされたネットワークエージェントは、適用されたセキュリティ製品のポリシーに関する情報をセキュリティ製品（たとえば、Kaspersky Endpoint Security for Windows）に転送します。転送された情報は、セキュリティ製品のインターフェイスで表示できます。

ネットワークエージェントは次の情報を転送します：

- 管理対象デバイスへのポリシー導入の時間
- 管理対象デバイスへポリシー導入の時点でのアクティブポリシーまたはモバイルユーザーポリシーの名前
- 管理対象デバイスへポリシー導入の時点で管理対象デバイスが含まれていた管理グループの名前とフルパス
- アクティブポリシーのプロファイルのリスト

  情報を使用して、デバイスに正しいポリシーが適用されていることを確認し、トラブルシューティングを行うことができます。既定では、このオプションはオフです。

- **ネットワークエージェントを不正な削除・停止から保護し、設定の変更を防止する**

  このオプションをオンにすると、管理対象デバイスにネットワークエージェントのインストールされた後、必要な権限がない場合はコンポーネントの削除や再設定が行えなくなります。また、ネットワークエージェントサービスを停止できなくなります。このオプションはドメインコントローラーに影響しません。

  ローカル管理者権限で操作されているワークステーション上のネットワークエージェントを保護するには、このオプションをオンにします。

  既定では、このオプションはオフです。

- **アンインストール用パスワードを使用する**

  このオプションをオンにすると、［**変更**］をクリックして、klmover ユーティリティおよびネットワークエージェントのリモートアンインストール時に使用するパスワードを指定できます。

  既定では、このオプションはオフです。

リポジトリ

［**リポジトリ**］セクションでは、情報ネットワークエージェントから管理サーバーに詳細が送信されるオブジェクトの種別を選択できます。このセクションの設定の一部を変更することがネットワークエージェントのポリシーで禁止されている場合、それらの設定を変更することはできません。

- **インストール済みアプリケーションの詳細**

  このオプションをオンにすると、クライアントデバイスにインストールされたアプリケーションに関する情報が管理サーバーに送信されます。

  既定では、このオプションはオンです。

- **パッチの情報を含める**

クライアントデバイスにインストールされたアプリケーションのパッチに関する情報が管理サーバーに送信されます。このオプションをオンにすると、データベースに保存されるデータの容量が増えるとともに管理サーバーと DBMS での負荷が増大します。

既定では、このオプションはオンです。Windows でのみ使用できます。

- **Windows Update 更新プログラムの詳細**

  このオプションをオンにすると、クライアントデバイスにインストールする必要のある Microsoft Windows 更新プログラムに関する情報が管理サーバーに送信されます。

  このオプションをオフにしても、［**適用なアップデート**］セクションのデバイスのプロパティに更新プログラムが表示されることがあります。たとえば、組織のデバイスにこれらの更新プログラムによって修正できる脆弱性がある場合などに、こうしたことが起こる可能性があります。

  既定では、このオプションはオンです。Windows でのみ使用できます。

- **ソフトウェアの脆弱性と対応するアップデートの詳細**

  このオプションをオンにすると、管理対象デバイスで検出されたサードパーティソフトウェア（Microsoft ソフトウェアを含む）の脆弱性に関する情報、およびサードパーティの脆弱性（Microsoft ソフトウェアを含まない）を修正するソフトウェアアップデートに関する情報が、管理サーバーに送信されます。

  このオプション（**ソフトウェアの脆弱性と対応するアップデートの詳細**）を選択すると、ネットワーク負荷、管理サーバーのディスク負荷、およびネットワークエージェントのリソース消費が増加します。

  既定では、このオプションはオンです。Windows でのみ使用できます。

  Microsoft ソフトウェアのソフトウェアアップデートを管理するには、［**Windows Update 更新プログラムの詳細**］を使用します。

- **ハードウェアレジストリの詳細**

  デバイスにインストールされたネットワークエージェントから、そのデバイスのハードウェアに関する情報が管理サーバーに送信されます。ハードウェアの詳細は、デバイスのプロパティで確認できます。

  ハードウェアの詳細を取得する Linux デバイスに lshw ユーティリティがインストールされていることを確認してください。使用されているハイパーバイザーによっては、仮想マシンから取得されたハードウェアの詳細が不完全である場合があります。

ソフトウェアのアップデートと脆弱性

この［**ソフトウェアのアップデートと脆弱性**］セクションでは、Windows アップデートの検索と配信を設定し、実行ファイルの脆弱性のスキャンを有効化できます。［**ソフトウェアのアップデートと脆弱性**］セクションの設定は、Windows を実行しているデバイスでのみ使用できます：

- **管理サーバーを WSUS サーバーとして使用する**

このオプションをオンにすると、Windows 更新プログラムが管理サーバーにダウンロードされます。管理サーバーは、ダウンロードしたアップデートを、ネットワークエージェントを利用してクライアントデバイスの Windows Update に一括配信します。

このオプションをオフにすると、Windows 更新プログラムのダウンロードに管理サーバーを使用しません。この場合、それぞれのクライアントデバイスが Windows アップデートを受信します。

既定では、このオプションはオフです。

- ユーザーが Windows Update サービスを使用してデバイスに手動でインストールできるアップデートを制限できます。

  Windows 10 を実行しているデバイスで、デバイスに適用可能な更新プログラムが Windows Update 内で既に検出されている場合、［**Kaspersky Security Center 11 がインストールされた管理サーバーデバイスが WSUS サーバーとして使用されている場合に、バージョン 11 以降のネットワークエージェントがインストールされたデバイス上で、Windows Update 更新プログラムのインストールをユーザーが管理することを許可する**］は、検出された更新プログラムがインストールされた後に適用されます。

  ドロップダウンリストからオプションを選択します：

  - **Windows Update のすべての適用可能な更新プログラムのインストールをユーザーに許可する**

    ユーザーは、デバイスに適用可能な Microsoft Windows Update のすべての更新プログラムをインストールできます。

    アップデートのインストールをブロックしない場合は、このオプションを選択します。

    ユーザーが Microsoft Windows Update の更新プログラムを手動でインストールする時、更新プログラムを管理サーバーからではなく Microsoft サーバーからダウンロードする場合があります。これは、管理サーバーが対象の更新プログラムをまだダウンロードしていない場合に起こります。Microsoft サーバーから更新プログラムをダウンロードすると、トラフィック量が増加します。

  - **Windows Update の承認された更新プログラムのみのインストールをユーザーに許可する**

    ユーザーは、デバイスに適用可能で管理者に承認された Microsoft Windows Update のすべての更新プログラムをインストールできます。

    たとえば、最初にテスト環境にアップデートをインストールしてデバイスのオペレーティングシステムとの互換性の問題が生じないかを確認してから、クライアントデバイスへの承認されたアップデートのインストールを許可することができます。

    ユーザーが Microsoft Windows Update の更新プログラムを手動でインストールする時、更新プログラムを管理サーバーからではなく Microsoft サーバーからダウンロードする場合があります。これは、管理サーバーが対象の更新プログラムをまだダウンロードしていない場合に起こります。Microsoft サーバーから更新プログラムをダウンロードすると、トラフィック量が増加します。

  - **Windows Update 更新プログラムのインストールをユーザーに許可しない**

ユーザーは、デバイスに Microsoft Windows Update の更新プログラムを手動でインストールできません。すべての適用可能な更新プログラムは、管理者の設定に従ってインストールされます。

アップデートのインストールを一元的に管理する場合は、このオプションをオンにします。

たとえば、ネットワークの過負荷を避けるために、アップデートのスケジュールを最適化したい場合などです。ユーザーの業務に支障をきたさないように、業務時間外にアップデートをスケジュールすることができます。

- ［**Windows Update 検索モード**］で、更新プログラムの検索モードを選択できます：
  - **アクティブ**

    このオプションをオンにすると、管理サーバーがネットワークエージェントのサポートにより、クライアントデバイス上の Windows Update エージェントからアップデート元である Windows Update Server または WSUS への要求を開始します。次に、ネットワークエージェントが、Windows Update エージェントから受け取った情報を管理サーバーに渡します。

    このオプションは、*脆弱性とアプリケーションのアップデートの検索*タスクで［**アップデートサーバーに接続してアップデートを取得**］が選択されている場合にのみ有効になります。

    既定では、このオプションがオンです。

  - **パッシブ**

    このオプションをオンにすると、ネットワークエージェントは、Windows Update エージェントとアップデート元との前回の同期で取得した更新プログラムの情報を定期的に管理サーバーに渡します。Windows Update エージェントとアップデート元が同期されない場合、管理サーバー上のアップデートの情報が最新ではなくなります。

    アップデート元のメモリキャッシュからアップデートを取得する場合は、このオプションを選択します。

  - **無効**

    このオプションをオンにすると、管理サーバーは更新プログラムに関する情報を要求しません。

    このオプションは、たとえば手元のローカルデバイスで最初にアップデートをテストしたい場合などに選択します。

- **実行ファイルの実行中に脆弱性をスキャンする**

  このオプションをオンにすると、実行ファイルが実行時にスキャンされ、脆弱性がないかチェックされます。

  既定では、このオプションはオンです。

再起動の設定

［**再起動の設定**］セクションでは、アプリケーションの正しい使用、インストール、またはアンインストールのために管理対象デバイスのオペレーティングシステムの再起動が必要な場合に行う動作を指定できます。
［**再起動の設定**］セクションの設定は、Windows を実行しているデバイスでのみ使用できます：

- **OS を再起動しない**

操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **必要に応じて自動的に OS を再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

  - **通知の繰り返し間隔（分）**

    このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

    既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

    このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

  - **次の時間経過後に強制的に再起動する（分）**

    ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

    既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

  - **セッションがブロックされたアプリケーションを強制終了する**

    アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

    このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

    このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

    既定では、このオプションはオフです。

Windows デスクトップ共有

［**Windows デスクトップ共有**］セクションでは、デスクトップアクセスの共有時にリモートデバイスで実行される管理者の処理の監査を有効にしたり、設定したりできます。［**Windows デスクトップ共有**］セクションの設定は、Windows を実行しているデバイスでのみ使用できます：

- **監査を有効にする**

  このオプションをオンにすると、リモートデバイスにおける管理者の処理の監査が有効になります。リモートデバイスにおける管理者の処理の記録は次に保存されます：
  - リモートデバイスのイベントログ
  - リモートデバイス上のネットワークエージェントのインストールフォルダーにある、拡張子が syslog のファイル
  - Kaspersky Security Center のイベントデータベース

  管理者の処理の監査が使用可能である条件は次の通りです：
  - 脆弱性とパッチ管理のライセンスが使用されている
  - 管理者がリモートデバイスのデスクトップに対する共有アクセスを開始する権限を持っている

  このオプションをオフにすると、リモートデバイスにおける管理者の処理の監査が無効になります。

  既定では、このオプションはオフです。

- **読み取り時に監視する必要のあるファイルのマスク**

  リストにはファイルマスクが含まれます。監査が有効になると、マスクと一致する管理者の読み取りファイルが監視され、ファイルの読み取りに関する情報が保存されます。リストは、［**監査を有効にする**］がオンの場合に使用できます。ファイルマスクを編集し、新しいマスクをリストに追加できます。新しいファイルマスクは、新しい行のリストに指定する必要があります。

  既定では、*.txt、*.rtf、*.doc、*.xls、*.docx、*.xlsx、*.odt、*.pdf のファイルマスクが指定されます。

- **変更時に監視する必要のあるファイルのマスク**

  リストには、リモートデバイス上のファイルのマスクが含まれます。監査が有効になると、マスクと一致するファイルで管理者によって行われた変更が監視され、その変更に関する情報が保存されます。リストは、［**監査を有効にする**］がオンの場合に使用できます。ファイルマスクを編集し、新しいマスクをリストに追加できます。新しいファイルマスクは、新しい行のリストに指定する必要があります。

  既定では、*.txt、*.rtf、*.doc、*.xls、*.docx、*.xlsx、*.odt、*.pdf のファイルマスクが指定されます。

パッチとアップデートの管理

［**パッチとアップデートの管理**］セクションでは、アップデートのダウンロードを設定できます。また、管理対象デバイスへのパッチの配信とインストールについても設定できます：

- **コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**

このオプションをオンにすると、*承認*ステータスが「*未定義*」のカスペルスキー製品のパッチが、アップデートサーバーにダウンロードされるとすぐに、管理対象デバイスに自動インストールされます。

このオプションをオフにすると、ダウンロードされたパッチのうちステータスが「*未定義*」のものは、管理者がステータスを「*承認*」に変更しない限りインストールされません。

既定では、このオプションはオンです。

- **アップデートと定義データベースをあらかじめ管理サーバーからダウンロードする（推奨）**

  このオプションをオンにすると、オフライン方式でのアップデートのダウンロードが使用されます。管理サーバーは、アップデートの受信時に、管理対象アプリケーションに必要なアップデートを、該当するアプリケーションがインストールされたデバイス上のネットワークエージェントに通知します。ネットワークエージェントは、アップデートに関する情報を受け取ると、適切なファイルを管理サーバーからあらかじめダウンロードします。具体的には、管理サーバーは、ネットワークエージェントが次に接続された時にアップデートのダウンロードを開始します。ネットワークエージェントによってすべてのアップデートがクライアントデバイスにダウンロードされると、そのデバイスのアプリケーションでこれらのアップデートが利用可能になります。

  クライアントデバイス上の管理対象アプリケーションがアップデートのためにネットワークエージェントにアクセスしようとすると、ネットワークエージェントは必要なアップデートがあるかどうか確認します。管理対象アプリケーションから要求された時点で、管理サーバーからアップデートを受信してから経過した時間が 25 時間以内の場合、ネットワークエージェントは管理サーバーと接続せずに、ローカルキャッシュからアップデートを管理対象アプリケーションに渡します。ネットワークエージェントからクライアントデバイス上のアプリケーションへアップデートを配信する際には、アップデートのために管理サーバーへの接続を確立する必要はありません。

  このオプションをオフにすると、オフライン方式でのアップデートのダウンロードは使用されません。アップデートは、アップデートダウンロードタスクのスケジュールに従って配信されます。

  既定では、このオプションはオンです。

接続

［**接続**］セクションには 3 つのサブセクションが含まれます：

- **ネットワーク**
- **接続プロファイル**
- **接続スケジュール**

［**ネットワーク**］サブセクションでは、管理サーバーからクライアントコンピューターへの接続を設定したり、UDP ポートの使用を有効化したり、UDP ポート番号を定義したりできます。

- ［**管理サーバーに接続**］セクションでは、管理サーバーへの接続を設定し、クライアントデバイスと管理サーバーを同期する間隔を指定できます：

  - **同期間隔（分）**

    ネットワークエージェントによって管理対象デバイスと管理サーバーが同期します。同期間隔（「ハートビート」とも表記）を管理対象 10,000 台につき 15 分に設定することを推奨します。

    同期間隔が 15 分以下に設定された場合、同期は 15 分ごとに実行されます。同期間隔が 15 分以上に設定されている場合は、指定された間隔で同期が実行されます。

- **ネットワークトラフィックを圧縮する**

  このオプションをオンにすると、送信される情報量が減ることでネットワークエージェントによるデータ送信速度が向上し、これにより管理サーバーの負荷が軽減されます。

  クライアントコンピューターの CPU の負荷は増加する可能性があります。

  既定では、このチェックボックスはオンです。

- **Microsoft Windows ファイアウォールでネットワークエージェントのポートを開く**

  このオプションをオンにすると、ネットワークエージェントと管理サーバーの動作に必要なポートが、Microsoft Windows ファイアウォールの除外リストに追加されます。

  既定では、このオプションはオンです。

- **SSL 接続を使用する**

  このオプションをオンにすると、SSL を使用してセキュアなポート経由で管理サーバーへの接続が確立されます。

  既定では、このオプションはオンです。

- **既定の接続設定でディストリビューションポイントの接続ゲートウェイを使用する（使用可能な場合）**

  このオプションをオンにすると、ディストリビューションポイントの接続ゲートウェイが、管理グループのプロパティで指定された設定で使用されます。

  既定では、このオプションはオンです。

- **UDP ポートを使用する**

  ネットワークエージェントが UDP ポートを経由して管理サーバーを接続する場合は、［**UDP ポートを使用**］をオンにして、［**UDP ポート番号**］を指定します。既定では、このオプションはオンです。管理サーバーに接続するための既定の UDP ポートは 15000 です。

- **UDP ポート番号**

  このフィールドに、UDP ポート番号を入力できます。既定のポート番号は 15000 です。

  レコードには 10 進法が使用されます。

  Windows XP Service Pack 2 で稼働するクライアントデバイスでは、UDP ポート 15000 が OS のファイアウォールによりブロックされます。このポートを手動で開く必要があります。

- **ディストリビューションポイントを使用して管理サーバーへ強制的に接続する**

  ［**ディストリビューションポイントをプッシュサーバーとして使用する**］をディストリビューションポイントの設定ウィンドウでオンにする場合、このオプションをオンにします。オンにしないと、ディストリビューションポイントはプッシュサーバーとして動作しません。

［**接続プロファイル**］サブセクションで、ネットワークロケーションを設定したり、管理サーバーが使用できない際のモバイルユーザーモードを有効にしたりできます。［**接続プロファイル**］セクションの設定は、Windows または macOS を実行しているデバイスでのみ使用できます：

- **ネットワークロケーションの設定**

  ネットワークロケーションの設定では、クライアントデバイスが接続するネットワークの特性を定義し、ネットワークの特性が変更された時にネットワークエージェントが管理サーバーの接続プロファイルを切り替えるためのルールを指定します。

- **管理サーバー接続プロファイル**

  このセクションでは、ネットワークエージェントから管理サーバーへの接続のプロファイルを表示して追加することができます。次のイベントの発生時、ネットワークエージェントから別の管理サーバーに切り替えるルールを作成することもできます：

  - クライアントデバイスが別のローカルネットワークに接続した場合
  - デバイスから組織のローカルネットワークへの接続が切断した場合
  - 接続ゲートウェイアドレスまたは DNS サーバーアドレスが変更された場合

  接続プロファイルは、Windows および macOS を実行しているデバイスでのみサポートされます。

- **管理サーバーが使用できない時にモバイルユーザーモードを有効にする**

  このオプションを有効にすると、このプロファイルで接続しているクライアントデバイスにインストールされているアプリケーションは、モバイルユーザーモードおよびモバイルユーザーポリシーを使用します。モバイルユーザーポリシーがアプリケーションに対して定義されていない場合は、アクティブポリシーが使用されます。

  このオプションを無効にすると、アプリケーションはアクティブポリシーを使用します。

  既定では、このオプションはオフです。

［**接続スケジュール**］サブセクションでは、ネットワークエージェントから管理サーバーにデータを送信する時間間隔を指定できます。

- **要求時に接続**

  このオプションをオンにすると、ネットワークエージェントが管理サーバーへのデータ送信を要求された時に、接続が確立されます。

  既定では、このオプションがオンです。

- **指定の時間間隔で接続**

  このオプションをオンにすると、ネットワークエージェントは指定した時間に管理サーバーへ接続します。複数の接続時間帯を追加できます。

ディストリビューションポイント別のネットワークポーリング

［**ディストリビューションポイント別のネットワークポーリング**］セクションでは、ネットワークの自動ポーリングを設定できます。ポーリングの設定は、Windows を実行しているデバイスでのみ使用できます。次のオプションを使用してポーリングを有効にしたり、頻度を設定できます：

- **Windows ネットワーク**

  このオプションをオンにすると、［**簡易ポーリングのスケジュールを設定する**］と［**完全ポーリングのスケジュールを設定する**］をクリックして設定したスケジュールに従って、管理サーバーによってネットワークが自動的にポーリングされます。

  このオプションをオフにすると、管理サーバーは［**ネットワークポーリングの間隔（分）**］フィールドで指定された間隔でネットワークをポーリングします。

  ネットワークエージェントのバージョンが 10.2 より前の場合、デバイスの検索間隔は、［**Windows ドメインをポーリングする間隔（分）**］（簡易の Windows ネットワークポーリング）と［**ネットワークポーリングの間隔（分）**］（簡易の Windows ネットワークポーリング）で設定できます。

  既定では、このオプションはオフです。

- **Zeroconf**

  このオプションをオンにすると、ディストリビューションポイントは自動的にゼロコンフィギュレーションネットワーキング（「*Zeroconf*」とも表記）を使用して IPv6 ネットワークを検索します。この場合、ディストリビューションポイントはネットワーク全体を検索するため、有効な IP 範囲の検索は無視されます。

  Zeroconf の使用を開始するには、次の条件が満たされている必要があります：

  - ディストリビューションポイントが Linux を実行している必要があります。
  - ディストリビューションポイントで avahi-browse ユーティリティをインストールする必要があります。

  このオプションをオフにすると、ディストリビューションポイントは IPv6 デバイスを持つネットワークを検索しません。

  既定では、このオプションはオフです。

- **IP アドレス範囲**

  このオプションをオンにすると、［**ポーリングのスケジュールを設定する**］をクリックして設定したスケジュールに従って、ディストリビューションポイントによって IP アドレス範囲が自動的にポーリングされます。

  このオプションをオフにすると、ディストリビューションポイントは IP アドレス範囲をポーリングしません。

  ネットワークエージェントのバージョンが 10.2 より前の場合、IP アドレス範囲のポーリング頻度は、［**ポーリング間隔（分）**］で設定できます。このフィールドは、オプションをオンにすると使用可能になります。

  既定では、このオプションはオフです。

- **ドメインコントローラー**

このオプションをオンにすると、［**ポーリングのスケジュールを設定する**］をクリックして設定したスケジュールに従って、ディストリビューションポイントによって Active Directory が自動的にポーリングされます。

このオプションをオフにすると、管理サーバーは Active Directory をポーリングしません。

ネットワークエージェントのバージョンが 10.2 より前の場合、Active Directory のポーリング頻度は、［**ポーリング間隔（分）**］で設定できます。このフィールドは、このオプションをオンにすると使用可能になります。

既定では、このオプションはオフです。

このオプションをオンにすると、［**ポーリングのスケジュールを設定する**］をクリックして設定したスケジュールに従って、ディストリビューションポイントによって Active Directory が自動的にポーリングされます。

このオプションをオフにすると、ディストリビューションポイントはドメインコントローラーをポーリングしません。

10.2 より前のバージョンのネットワークエージェントドメインコントローラーのポーリング頻度は、［**ポーリング間隔（分）**］で設定できます。このフィールドは、このオプションをオンにすると使用可能になります。

既定では、このオプションはオフです。

ディストリビューションポイントのネットワーク設定

［**ディストリビューションポイントのネットワーク設定**］セクションで、インターネットアクセス設定を指定できます：

- **プロキシサーバーを使用する**
- **アドレス**
- **ポート番号**
- **ローカルアドレスにプロキシサーバーを使用しない**

  このオプションをオンにすると、ローカルネットワークのデバイスへの接続にプロキシサーバーが使用されません。

  既定では、このオプションはオフです。

- **プロキシサーバー認証**

  このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。

  既定では、このチェックボックスはオフです。

- **ユーザー名**
- **パスワード**

KSN プロキシ（ディストリビューションポイント）

［**KSN プロキシ（ディストリビューションポイント）**］セクションでは、ディストリビューションポイントを使用して管理対象デバイスからの Kaspersky Security Network（KSN）リクエストを転送するようにアプリケーションを設定できます：

- **ディストリビューションポイントで KSN プロキシを有効にする**

  ディストリビューションポイントとして使用しているデバイス上で KSN プロキシサービスが実行されます。この機能を使用することで、ネットワーク上でトラフィックを分配しなおし、最適化できます。

  ディストリビューションポイントは、Kaspersky Security Network に関する声明に記載されている KSN の統計情報をカスペルスキーに送信します。既定では、KSN 声明は「%ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula」にあります。

  既定では、このオプションはオフです。管理サーバーのプロパティウィンドウで、［**管理サーバーをプロキシサーバーとして使用する**］と［**Kaspersky Security Network への参加に同意する**］がオンになっている場合にのみ使用できます。

  アクティブ / パッシブモードのクラスターのノードをディストリビューションポイントに割り当て、ノード上で KSN プロキシサーバーを有効にできます。

- **KSN リクエストを管理サーバーに転送する**

  ディストリビューションポイントは管理対象デバイスからの KSN リクエストを管理サーバーに転送します。

  既定では、このオプションはオンです。

- **インターネット経由で直接 KSN クラウド / KPSN にアクセスする**

  ディストリビューションポイントは管理対象デバイスからの KSN リクエストを KSN クラウドまたは KPSN に転送します。ディストリビューションポイント自体で生成された KSN リクエストも、KSN クラウドまたは KPSN に直接送信されます。

  バージョン 11 以前のネットワークエージェントをインストールしているディストリビューションポイントでは、KPSN に直接アクセスできません。これらのディストリビューションポイントで KPSN リクエストを KPSN に送信するように設定を編集するには、各ディストリビューションポイントで［**KSN リクエストを管理サーバーに転送する**］をオンにします。

  バージョン 12 以降のネットワークエージェントをインストールしているディストリビューションポイントでは、KPSN に直接アクセスできません。

- **ポート**

  管理対象デバイスが KSN プロキシサーバーへの接続に使用する TCP ポートの番号。既定のポート番号は 13111 です。

- **UDP ポート**

  ネットワークエージェントが UDP ポートを経由して管理サーバーを接続する場合は、［**UDP ポートを使用**］をオンにして、［**UDP ポート番号**］を指定します。既定では、このオプションはオンです。管理サーバーに接続するための既定の UDP ポートは 15000 です。

アップデート（ディストリビューションポイント）

［**アップデート（ディストリビューションポイント）**］セクションでは、差分ファイルのダウンロード機能を有効にすることができます。そのため、ディストリビューションポイントはカスペルスキーのアップデートサーバーから差分ファイルの形式でアップデートを取得します。

ローカルアカウントの管理（Linux のみ）

［**ローカルアカウントの管理（Linux のみ）**］セクションには、次の 3 つのサブセクションが含まれます。

- **ユーザー証明書の管理**
- **適用可能なローカル管理者グループの追加または変更**
- **ユーザーのデバイス上で sudo ファイルを変更から保護する参照ファイルをアップロードしてください**

［**ユーザー証明書の管理**］サブセクションでは、インストールするルート証明書を指定できます。これらの証明書は、たとえば、Web サイトまたは Web サーバーの信頼性を検証するために使用できます。

- **ルート証明書のインストール**

  このオプションをオンにすると、テーブルに追加された証明書が指定されたデバイスにインストールされます。
  このオプションをオフにすると、指定されたデバイスに証明書はインストールされません。
  既定では、このオプションはオフです。

- **追加**

  このボタンをクリックすると、証明書を追加できるウィンドウが開きます。
  証明書は 10 MB 未満である必要があります。
  Kaspersky Security Center は、CER、CRT、CERT、PEM、および KEY 拡張子を持つ証明書をサポートしています。

［**適用可能なローカル管理者グループの追加または変更**］サブセクションでは、ローカル管理グループを管理できます。これらのグループは、たとえば、ローカル管理者権限を取り消す時に使用されます。**特権付きのデバイスのユーザーに関するレポート（Linux のみ）**を使用して、特権ユーザーアカウントのリストを確認することもできます。

- **追加**

  このボタンをクリックするとウィンドウが開き、ローカル管理グループを追加できます。

- **編集**

  このボタンをクリックするとウィンドウが開き、ローカル管理グループを編集できます。
  このボタンは、ローカル管理グループの横にあるチェックボックスがオンの場合に使用できます。

- **削除**

このボタンをクリックすると、選択したローカル管理グループがテーブルから削除されます。
このボタンは、ローカル管理グループの横にあるチェックボックスがオンの場合に使用できます。

［**ユーザーのデバイス上で sudo ファイルを変更から保護する参照ファイルをアップロードしてください**］サブセクションでは、ファイル sudoers の制御を設定できます。特権グループとデバイスユーザーは、デバイス上のファイル sudoers によって定義されます。ファイル sudoers は `/etc/sudoers` にあります。参照 sudoers ファイルをアップロードして、ファイル sudoers が変更されないように保護できます。これにより、ファイル sudoers への不要な変更が防止されます。

無効な参照 sudoers ファイルにより、ユーザーのデバイスが誤動作する可能性があります。

- **コントロール sudo ファイル**

  このオプションをオンにすると、ファイル sudoers は現在の参照 sudoers ファイルに置き換えられます。

  このオプションをオフにすると、ファイル sudoers は変更されません。

  既定では、このオプションはオフです。

- **参照 sudo ファイル**

  このフィールドには、アップロードされた参照 sudoers ファイルの名前が表示されます。

- **アップロード**

  このボタンをクリックするとウィンドウが開き、参照 sudoers ファイルをアップロードできます。

- **現在の参照 sudo ファイル**

  このボタンをクリックすると、現在の sudoers ファイルの内容が表示されます。

変更履歴

このタブでは、必要に応じて、ポリシーのリビジョンのリストを表示したり、ポリシーで行われた変更をロールバックすることができます。

ネットワークエージェントのポリシー設定のオペレーティングシステム別の比較

次の表は、特定のオペレーティングシステムでネットワークエージェントの設定に使用できるネットワークエージェントのポリシー設定を示しています。

ネットワークエージェントのポリシー設定：オペレーティングシステムによる比較

［ポリシー］セクション	Windows	macOS	Linux

全般	✓	✓	✓
イベントの設定	✓	✓	✓
設定	✓	✓	✓ 次のオプションを使用できます： • **ディストリビューションポイント経由でのみファイルを配信する** • **イベントキューの最大サイズ（MB）** • **アプリケーションがポリシーの拡張データをデバイスから取得可能である**
リポジトリ	✓	✓ ［**ハードウェアレジストリの詳細**］が使用可能です。	✓ 次のオプションを使用できます： • **インストール済みアプリケーションの詳細** • **ハードウェアレジストリの詳細**
ソフトウェアのアップデートと脆弱性	✓	—	—
再起動の設定	✓	—	—
Windows デスクトップ共有	✓	—	—
パッチとアップデートの管理	✓	—	—
［**接続**］→［**ネットワーク**］	✓	✓	✓ ［**Microsoft Windows ファイアウォールでネットワークエージェントのポートを開く**］以外。
［**接続**］→［**接続プロファイル**］	✓	✓	—
［**接続**］→［**接続スケジュール**］	✓	✓	✓
ディストリビューションポイント別のネットワークポーリング	✓ ［**Windows ネットワーク**］、［**IP アドレス範囲**］、および［**ドメインコントローラー**］のみ使用可能です。	—	✓ 次のオプションを使用できます： • **Zeroconf** • **IP アドレス範囲** • **ドメインコントローラー**
ディストリビューションポイントのネットワーク設定	✓	✓	✓
KSN プロキシ（ディストリビューションポイント）	✓	—	✓
アップデート（ディストリビューションポイント）	✓	—	✓
変更履歴	✓	✓	✓

ネットワークエージェントの低リソース消費モードの有効化と無効化

低リソース消費モードでは、クライアントデバイスにインストールされているネットワークエージェントの RAM 使用量を制限できます。既定では、低リソース消費モードは無効になっています。

低リソース消費モードでは、次の機能は実行されません：

- ネットワークエージェントを（手動または自動で）ディストリビューションポイントとして割り当てることはできません。
- ネットワークエージェントは、ネットワークエージェントのステータスに関する情報を別のテキストファイルに記録しません。
- ネットワークエージェントは、アップデートダウンロードのオフラインモデルをサポートしていません。
- 次のコンポーネントとプロセスは無効になっています：
  - サードパーティのアップデートと脆弱性に関する情報の取得
  - ディストリビューションポイント側での KSN プロキシの実行
  - アップデートのディストリビューションポイントリポジトリへのアップロード
  - DNS サーバーブロックのバイパス
  - 空きディスク容量に関する情報を取得しています

低リソース消費モードを無効にすると、コンポーネントとプロセスは動作を再開します。

低リソース消費モードを有効にするには：

1. クライアントデバイスのコマンドラインで次のコマンドを実行します：

   ```
   C:\Program files (x86)\ カスペルスキー Lab\NetworkAgent>klscflag -fset -pv klnagent -n KLNAG_FLAG_TEST_VM_PERF -td -v 1
   ```

2. ネットワークエージェントを再起動します。
3. 低リソース消費モードが有効になっているかどうかを確認するには、Windows で**イベントビューアー**を開き、［**アプリケーションとサービスログ**］→［**Kaspersky イベントログ**］を選択します。

   ログに、**Kaspersky Security Center ネットワークエージェントが低リソース消費モードで動作している**などのイベントが含まれていることを確認します。

低リソース消費モードが有効になりました。

低リソース消費モードを無効にするには：

1. クライアントデバイスのコマンドラインで次のコマンドを実行します：

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. ネットワークエージェントを再起動します。
3. 低リソース消費モードが無効になっていることを確認するには、Windows で**イベントビューアー**を開き、［**アプリケーションとサービスログ**］→［**Kaspersky イベントログ**］を選択します。

   最後の klnagent イベントに、「**Kaspersky Security Center ネットワークエージェントは低リソース消費モードで動作しています**」というメッセージが含まれていないことを確認します。

低リソース消費モードが無効になりました。

*スクリプトをリモートで実行タスク*を使用して、低リソース消費モードをリモートで有効にすることもできます。

Kaspersky Endpoint Security ポリシーの手動セットアップ

このセクションでは、 Kaspersky Endpoint Security ポリシーの設定方法に関する推奨事項について説明します。ポリシーのプロパティウィンドウで設定を実行できます。設定を編集する際には、関連する設定グループの右側にあるロックアイコンをクリックして、指定した値をワークステーションに適用します。

Kaspersky Security Network の設定

Kaspersky Security Network（KSN）は、ファイル、Web リソース、およびソフトウェアのレピュテーションに関する情報が含まれるクラウドサービスのインフラストラクチャです。Kaspersky Security Network を使用することで、 Kaspersky Endpoint Security for Windows はより迅速に様々な種類の脅威に対応し、保護コンポーネントのパフォーマンスを向上させ、誤検知の可能性を減らすことができます。Kaspersky Security Network の詳細は、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

KSN について推奨される設定を指定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。
   選択したポリシーのプロパティウィンドウが表示されます。
3. ポリシーのプロパティで、［**アプリケーション設定**］→［**先進の脅威対策**］→［**Kaspersky Security Network**］の順に選択します。
4. ［**KSN プロキシを使用する**］をオンにすることを推奨します。このオプションを使用することで、ネットワーク上でトラフィックを再分配し、最適化できます。

   > Managed Detection and Response を使用する場合、ディストリビューションポイントの［**KSN プロキシ**］をオンにし、拡張 KSN モードを有効にする必要があります。

5. KSN プロキシサービスが使用できない場合は、KSN サーバーの使用を有効にします。KSN サーバーは、カスペルスキー側に配置されている場合（KSN の使用時）とサードパーティ側に配置されている場合（KPSN の使用時）があります。
6. ［**OK**］をクリックします。

KSN について推奨される設定が指定されます。

ファイアウォールで保護されているネットワークのリストの確認

Kaspersky Endpoint Security for Windows ファイアウォールがすべてのネットワークを保護していることを確認してください。既定では、ファイアウォールは次の種別の接続でネットワークを保護します：

- **パブリックネットワーク**：セキュリティ製品、ファイアウォール、またはフィルターは、このようなネットワーク内のデバイスを保護しません。
- **ローカルネットワーク**：このネットワーク内のデバイスは、ファイルとプリンターへのアクセスが制限されます。
- **信頼できるネットワーク**：このようなネットワーク内のデバイスは、ファイルやデータへの攻撃や不正アクセスから保護されます。

カスタムネットワークを設定している場合は、ファイアウォールがネットワークを保護していることを確認してください。このために、 Kaspersky Endpoint Security for Windows ポリシーのプロパティでネットワークのリストを確認します。このリストには、すべてのネットワークが含まれているとは限りません。

ファイアウォールの詳細は、 Kaspersky Endpoint Security for Windows のヘルプを参照してください。

ネットワークのリストを確認するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。
   選択したポリシーのプロパティウィンドウが表示されます。
3. ポリシーのプロパティで、［**アプリケーション設定**］→［**脅威対策**］→［**ファイアウォール**］の順に選択します。
4. ［**使用可能なネットワーク**］で、［**ネットワーク設定**］をクリックします。
   ［**ネットワーク接続**］ウィンドウが表示されます。このウィンドウにはネットワークのリストが表示されます。
5. リストに欠落しているネットワークがある場合は、追加します。

ネットワークデバイスのスキャンの無効化

Kaspersky Endpoint Security for Windows がネットワークドライブをスキャンすると、ネットワークドライブに大きな負荷がかかる可能性があります。ファイルサーバーで間接スキャンを実行するのが有効です。

Kaspersky Endpoint Security for Windows ポリシーのプロパティで、ネットワークドライブのスキャンを無効にすることができます。ポリシーのプロパティの説明は、 Kaspersky Endpoint Security for Windows のヘルプを参照してください。

ネットワークドライブのスキャンを無効にするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。
   選択したポリシーのプロパティウィンドウが表示されます。
3. ポリシーのプロパティで、［**アプリケーション設定**］-［**脅威対策**］-［**ファイル脅威対策**］の順に選択します。

4. ［**保護範囲**］セクションで、［**すべてのネットワークドライブ**］を無効にします。

5. ［**OK**］をクリックします。

ネットワークドライブのスキャンが無効になります。

管理サーバーのメモリからのソフトウェアの詳細情報の除外

ネットワークデバイスで起動されたソフトウェアモジュールに関する情報を管理サーバーに保存しないことを推奨します。その結果、管理サーバーのメモリがオーバーランすることはありません。

Kaspersky Endpoint Security for Windows ポリシーのプロパティで、この情報の保存を無効にすることができます。

インストール済みのソフトウェアモジュールに関する情報の保存を無効にするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。
選択したポリシーのプロパティウィンドウが表示されます。

3. ポリシーのプロパティで、［**アプリケーション設定**］→［**全般設定**］→［**レポートと保管領域**］の順に選択します。

4. ［**管理サーバーへのデータ転送**］セクションで、［**起動されたアプリケーションの情報**］が上位のポリシーでオンになっている場合、これをオフにします。
このチェックボックスをオンにすると、管理サーバーデータベースに、ネットワーク接続されたデバイス上にあるすべてのバージョンのソフトウェアモジュールに関する情報が保存されます。この情報は、Kaspersky Security Center データベース内に大量のディスク容量を必要とする場合があります（数十ギガバイト）。

インストール済みのソフトウェアモジュールに関する情報が保存されなくなります。

ワークステーションの Kaspersky Endpoint Security for Windows インターフェイスへのアクセスの設定

組織のネットワーク上の脅威対策による保護を Kaspersky Security Center を介して集中モードで管理する必要がある場合は、以下の説明に従って、Kaspersky Endpoint Security for Windows ポリシーのプロパティでインターフェイス設定を指定します。その結果、ワークステーション上の Kaspersky Endpoint Security for Windows への不正アクセスと Kaspersky Endpoint Security for Windows 設定の変更を防ぐことができます。

ポリシーのプロパティの説明は、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

インターフェイスの推奨設定を指定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。
選択したポリシーのプロパティウィンドウが表示されます。

3. ポリシーのプロパティで、［**アプリケーション設定**］-［**全般設定**］-［**インターフェイス**］の順に選択します。

4. ［**ユーザーインターフェイス**］セクションで、［**表示しない**］を選択します。これにより、ワークステーションで Kaspersky Endpoint Security for Windows のユーザーインターフェイスが表示されなくなり、ユーザーは Kaspersky Endpoint Security for Windows の設定を変更できなくなります。

5. ［**パスワードによる保護**］のスイッチをオンにします。これにより、ワークステーションで Kaspersky Endpoint Security for Windows の設定が不正に変更されたり、ユーザーが意図せずに変更してしまったりする危険性を低減できます。

以上の手順で、Kaspersky Endpoint Security for Windows のインターフェイスの推奨設定の指定が完了します。

重要なポリシーイベントを管理サーバーデータベースに保存する

管理サーバーデータベースのオーバーフローを回避するために、データベースには重要なイベントのみを保存することを推奨します。

管理サーバーのデータベースへの重要なイベントの記録を設定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。
選択したポリシーのプロパティウィンドウが表示されます。

3. ポリシーのプロパティで、［**イベントの設定**］タブを開きます。

4. ［**緊急**］セクションで、［**イベントの追加**］をクリックし、次のイベントのチェックボックスのみをオンにします：

- *使用許諾契約書の条項に違反しています*
- *コンピューター起動時の自動起動が無効です*
- *アクティベーションエラー*
- *アクティブな脅威が検知されました。高度な駆除を開始する必要があります*
- *駆除不可*
- *以前開いた危険なリンクを検知しました*
- *プロセスが終了しました*
- *ネットワーク動作がブロックされました*
- *ネットワーク攻撃が検知されました*
- *アプリケーションの起動が禁止されました*
- *アクセスが拒否されました（ローカルデータベース）*

- *アクセスが拒否されました（KSN）*
- *ローカルのアップデートエラー*
- *2 つのタスクを同時に開始できません*
- *Kaspersky Security Center との対話中にエラーが発生しました*
- *アップデートされていないコンポーネントがあります*
- *ファイル暗号化 / 復号化ルールの適用中にエラーが発生しました*
- *ポータブルモードの有効化中にエラーが発生しました*
- *ポータブルモードの無効化中にエラーが発生しました*
- *暗号化モジュールを読み込めません*
- *ポリシーを適用できません*
- *アプリケーション機能の変更中にエラーが発生しました*

5. ［**OK**］をクリックします。

6. ［**機能エラー**］セクションで、［**イベントの追加**］をクリックし、イベント「*無効なタスク設定です。設定は適用されません。*

7. ［**OK**］をクリックします。

8. ［**警告**］セクションで、［**イベントの追加**］をクリックし、次のイベントのチェックボックスのみをオンにします：

- *セルフディフェンスが無効です*
- *保護コンポーネントが無効です*
- *予備のライセンスが正しくありません*
- *侵入者がコンピューターまたは個人データに損害を与える可能性がある正規のソフトウェアが検知されました（ローカルデータベース）*
- *侵入者がコンピューターまたは個人データに損害を与える可能性がある正規のソフトウェアが検知されました（KSN）*
- *オブジェクトが削除されました*
- *オブジェクトが駆除されました*
- *ユーザーが暗号化ポリシーを拒否しました*
- *ファイルは管理者によって Kaspersky Anti Targeted Attack Platform サーバー上の隔離から復元されました*
- *ファイルは管理者によって Kaspersky Anti Targeted Attack Platform サーバー上で隔離されました*
- *アプリケーションの起動ブロックに関するメッセージが管理者に送信されました*

- *デバイスへのアクセスブロックに関するメッセージが管理者に送信されました*
- *Web ページへのアクセスブロックに関するメッセージが管理者に送信されました*

9. ［**OK**］をクリックします。
10. ［**情報**］セクションで、［**イベントの追加**］をクリックし、次のイベントのチェックボックスのみをオンにします：
    - *オブジェクトのバックアップコピーが作成されました*
    - *アプリケーションの起動がテストモードでブロックされています*
11. ［**OK**］をクリックします。

管理サーバーデータベースへの重要なイベントの記録が設定されます。

Kaspersky Endpoint Security のグループアップデートタスクの手動セットアップ

［**タスクの開始を自動的かつランダムに遅延させる**］がオンの場合、Kaspersky Endpoint Security での最適かつ推奨されるスケジュールオプションは［**新しいアップデートがリポジトリにダウンロードされ次第**］です。

デバイスコントロールでブロックされた外部デバイスへのオフラインモードでのアクセス権の付与

Kaspersky Endpoint Security for Windows のポリシーでのデバイスコントロール機能の設定により、クライアントデバイスに接続された外部デバイス（ハードディスク、カメラ、Wi-Fi モジュール）へのユーザーアクセスをコントロールできます。これにより、外部デバイスの接続によるクライアントデバイスへのマルウェアなどの感染を防止し、データの損失や流出などの被害を防ぐことができます。

デバイスコントロールでブロックされている外部デバイスへの一時的なアクセス権を付与する必要があるが、デバイスを信頼デバイスのリストに追加することは避けたい場合、外部デバイスへのオフラインモードでのアクセス権を付与することができます。オフラインモードでのアクセス権とは、クライアントデバイスがネットワークに接続されていない状態でのアクセス権です。

デバイスコントロールでブロックされている外部デバイスへのオフラインモードでのアクセス権を付与できるのは、Kaspersky Endpoint Security for Windows ポリシーの設定の［**アプリケーション設定**］→［**セキュリティコントロール**］→［**デバイスコントロール**］セクションで［**一時アクセスの要求を許可する**］がオンになっている場合のみです。

デバイスコントロールでブロックされた外部デバイスへのオフラインモードでのアクセス権の付与は、以下の手順で進みます：

1. クライアントデバイス上の Kaspersky Endpoint Security for Windows のウィンドウで、ブロックされている外部デバイスへのアクセス権を必要としているユーザーがアクセス要求ファイルを生成し、Kaspersky Security Center の管理者に送信します。

2. この要求を受け取った Kaspersky Security Center の管理者は、アクセスキーファイルを作成し、クライアントデバイスを使用しているユーザーに送信します。

3. クライアントデバイス上の Kaspersky Endpoint Security for Windows のウィンドウで、デバイスのユーザーはアクセスキーファイルを有効化し、外部デバイスへの一時的なアクセスを取得します。

デバイスコントロールでブロックされた外部デバイスへの一時的なアクセス権を付与するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

   管理対象デバイスのリストが表示されます。

2. このリストで、デバイスコントロールでブロックされている外部デバイスへのアクセス権を付与するクライアントデバイスを選択します。

   選択できるデバイスは1台のみです。

3. 管理対象デバイスのリストの上で省略記号（**...**）をクリックして、［**オフラインモードでのデバイスへのアクセスを許可**］をクリックします。

4. 表示される［**アプリケーション設定**］ウィンドウの［**デバイスコントロール**］セクションで、［**参照**］をクリックします。

5. ユーザーから受け取ったアクセス要求ファイルを選択し、［**開く**］をクリックします。ファイルは AKEY 形式である必要があります。

   現在ブロックされていて、ユーザーがアクセスを要求した外部デバイスの詳細情報が表示されます。

6. ［**アクセス期間**］の値を指定します。

   この設定では、ユーザーがブロックされたデバイスへのアクセスを許可される時間の長さを定義します。既定値は、アクセス要求ファイルの作成時にユーザーが希望して指定した値です。

7. ［**アクティベーション期間**］の値を指定します。

   この設定では、ブロックされているデバイスへのアクセスを、ユーザーが受け取ったアクセスキーを使用して有効化できる期間を指定します。

8. ［**保存**］をクリックします。

   ［**アクセスキーの保存**］ウィンドウが表示されます。

9. ブロックされているデバイスへのアクセスキーを含んだファイルを保存する保存先フォルダーを選択します。

10. ［**保存**］をクリックします。

    保存したアクセスキーをユーザーに送信し、ユーザーが Kaspersky Endpoint Security for Windows のウィンドウでこれを有効化すると、指定した期間、ブロックされているデバイスへのアクセス権がユーザーに付与されます。

アプリケーションまたはソフトウェアのアップデートのリモートでの削除

選択したデバイスからリモートでアプリケーションまたはソフトウェアのアップデートを削除するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。

2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**アプリケーションのリモートアンインストール**］タスク種別を選択します。

4. 作成中のタスク名を入力します。

   タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

5. タスクを割り当てるデバイスを選択します。

6. 削除するソフトウェアの種類を選択してから、削除する特定のアプリケーション、アップデート、またはパッチを選択します。

   - **管理対象アプリケーションをアンインストールする**

     カスペルスキー製品のリストが表示されます。削除するアプリケーションを選択します。

   - **競合アプリケーションをアンインストールする**

     カスペルスキーのセキュリティ製品または Kaspersky Security Center と互換性のないアプリケーションのリストが表示されます。削除するアプリケーションの隣にあるチェックボックスをオンにします。

   - **アプリケーションレジストリからアプリケーションを削除する**

既定では、ネットワークエージェントは管理対象デバイスにインストールされているアプリケーションに関する情報を管理サーバーに送信します。インストールされているアプリケーションのリストは、アプリケーションレジストリに保存されます。

アプリケーションレジストリからアプリケーションを選択するには：

a. ［**アンインストールするアプリケーション**］をクリックし、削除するアプリケーションを選択します。

Kaspersky Security Center ネットワークエージェントを選択した場合、タスクを実行すると、削除プロセスが開始されたことを表「*正常に完了*」ステータスが表示されます。Kaspersky Security Center ネットワークエージェントが削除されても、ステータスは変わりません。タスクが失敗すると、ステータスは「*失敗*」に変わります。

b. アンインストールオプションを指定します：

- **アンインストールモード**

アプリケーションを削除する方法を選択します：

- **アンインストールコマンドを自動的に定義する**

  アプリケーションの製造元によって定義されたアンインストールコマンドがアプリケーションにある場合、Kaspersky Security Center はこのコマンドを使用します。このオプションをオンにすることを推奨します。

- **アンインストールコマンドを指定する**

  アプリケーションのアンインストール用のコマンドを指定する場合は、このオプションをオンにします。

  まず、［**アンインストールコマンドを自動的に定義する**］をオンにしてアプリケーションを削除してみてください。自動的に定義されたコマンドによるアンインストールが失敗した場合は、独自のコマンドを使用してください。

  フィールドにインストールコマンドを入力し、次のオプションをオンにします。

  既定コマンドが自動検知されない場合、このアンインストール用コマンドを使用

  Kaspersky Security Center は、選択されたアプリケーションに、アプリケーションの製造元が定義したアンインストールコマンドがあるかどうかを確認します。コマンドが見つかった場合、Kaspersky Security Center は、［**アプリケーションのアンインストール用コマンド**］で指定されたコマンドの代わりにそのコマンドを使用します。

  このオプションをオンにすることを推奨します。

- **アプリケーションのアンインストール後に再起動する**

アンインストールが正常に完了した後で、アプリケーションが管理対象デバイスでオペレーティングシステムを再起動する必要がある場合、オペレーティングシステムは自動的に再起動されます。

- **指定したソフトウェアアップデート、パッチ、サードパーティ製品をアンインストールする**

  アップデート、パッチ、サードパーティ製品のリストが表示されます。削除する項目を選択します。

  表示されるリストは、アプリケーションとアップデートの一般的なリストであり、管理対象デバイスにインストールされているアプリケーションとアップデートには対応していません。項目を選択する前に、タスク範囲で定義されたデバイスにアプリケーションまたはアップデートがインストールされていることの確認を推奨します。アプリケーションまたはアップデートがインストールされているデバイスのリストを、プロパティウィンドウで表示できます。

  デバイスのリストを表示するには：

  a. アプリケーションまたはアップデートの名前をクリックします。

  プロパティウィンドウが表示されます。

  b. ［**デバイス**］セクションを開きます。

  インストールされているアプリケーションとアップデートのリストをデバイスのプロパティウィンドウで表示することもできます。

7. クライアントデバイスがアンインストールユーティリティをダウンロードする方法を指定します：

- **ネットワークエージェントを使用する**

  ファイルは、クライアントデバイスにインストールされているネットワークエージェントによってクライアントデバイスに配布されます。

  このオプションがオフになっている場合、ファイルは Microsoft Windows ツールを使用して配信されます。

  ネットワークエージェントがインストールされたデバイスにタスクが割り当てられている場合は、このチェックボックスをオンにすることを推奨します。

- **管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**

  ファイルは、管理サーバーのオペレーティングシステムツールを使用してクライアントデバイスに送信されます。このオプションは、クライアントデバイスにネットワークエージェントがインストールされていないものの、クライアントデバイスが管理サーバーと同じネットワークに存在する場合にオンにできます。

- **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**

  ファイルは、オペレーティングシステムのツールを使用してディストリビューションポイント経由でクライアントデバイスに送信されます。このオプションをオンにできるのは、ネットワークに少なくとも1つのディストリビューションポイントがある場合です。

  ［**ネットワークエージェントを使用する**］をオンにすると、ネットワークエージェントのツールが使用できない場合に限り、ファイルがオペレーティングシステムのツールを使用して配布されます。

- **同時ダウンロード数の上限**

  管理サーバーが同時にファイルを送信できるクライアントデバイスの最大許容数。この数が大きいほど、アプリケーションのアンインストールは高速になりますが、管理サーバーの負荷が増大します。

- **アンインストール試行回数の上限**

  *アプリケーションのリモートアンインストール*タスクの実行時に、パラメータで指定されたインストーラーの実行回数の範囲内で、管理対象デバイスから対象製品をアンインストールすることに失敗した場合、Kaspersky Security Center はこの管理対象デバイスへのインストールユーティリティの配布を中止し、そのデバイス上でインストーラーを起動しなくなります。

  ［**アンインストール試行回数の上限**］パラメータを使用することで、管理対象デバイス上でのリソースの消費量とネットワークのトラフィック量を軽減できます（アンインストールの実行や MSI ファイルの実行によるリソース消費、エラーメッセージのトラフィック）。

  タスクの開始が繰り返し試行されることは、デバイス上でインストールを阻害する問題が発生していることを示している可能性があります。管理者は、指定されたアンインストールの試行回数内で問題を解決してから、タスクを（手動でまたはスケジュールによって）再起動する必要があります。

  指定された試行回数以内にアンインストールを実行できなかった場合、問題は解決不可能なものとして認識され、それ以上タスクの開始を試行することは不必要にリソースとトラフィックを消費してしまうものと判断されます。

  タスクが作成されると、試行回数のカウンターは「`0`」にセットされます。デバイス上でインストーラーを実行してエラーが返されるたびに、カウンターの値が 1 ずつ増加します。

  パラメータで指定した回数のインストールの試行が既に実行された後に、デバイスでアンインストールの準備が完了した場合は、［**アンインストール試行回数の上限**］パラメータの値を増やすことでアプリケーションをアンインストールするタスクを開始できます。または、［*アプリケーションのリモートアンインストール*］タスクを新規に作成することもできます。

- **ダウンロード前に OS の種別を確認する**

  ファイルをクライアントデバイスに送信する前に、Kaspersky Security Center Linux はインストールユーティリティの設定がクライアントデバイスのオペレーティングシステムに適用可能であるかどうかを確認します。設定を適用できない場合、Kaspersky Security Center はファイルを送信せず、アプリケーションのインストールを試行しません。たとえば、様々なオペレーティングシステムを実行しているデバイスが存在する管理グループのデバイスにアプリケーションをインストールするには、インストールタスクを管理グループに割り当ててから、このオプションをオンにして、必要なオペレーティングシステム以外を実行しているデバイスをスキップできます。

- **アンインストール用パスワードを使用する**

  このパラメータは、前の手順で［**管理対象アプリケーションのアンインストール**］を選択し、［**アンインストールするアプリケーション**］フィールドに Kaspersky Security Center ネットワークエージェントを指定した時に表示されます。

  以前にネットワークエージェントポリシー設定でネットワークエージェントリモートアンインストールのパスワードを設定した場合は、［**アンインストールパスワードを使用する**］をオンにし、［**パスワード**］フィールドにアンインストールパスワードを入力します。ネットワークエージェントのリモートアンインストールのパスワードを設定していない場合は、チェックボックスをオンにしないでください。

8. OS の再起動設定を指定します。

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

- **通知の繰り返し間隔（分）**

  このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

  既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

  このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

- **再起動するまでの時間（分）**

  ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

  既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

9. 必要に応じて、リモートアンインストールタスクの開始に使用するアカウントを追加できます：

- **アカウントが不要（ネットワークエージェントインストール済み）**

このオプションをオンにすると、アプリケーションのインストーラーを実行するアカウントを指定する必要はありません。タスクは管理サーバーのサービスを実行しているアカウントで実行されます。

クライアントデバイスにネットワークエージェントがインストールされていない場合、このオプションは使用できません。

- **アカウントが必要（ネットワークエージェントの使用なし）**

  *アプリケーションのリモートアンインストール*タスクを割り当てるデバイスにネットワークエージェントがインストールされていない場合は、このオプションをオンにします。

  アプリケーションのインストーラーを実行するユーザーアカウントを指定します。［**追加**］をクリックし、［**アカウント**］を選択してから、ユーザーアカウントの資格情報を指定します。

  タスクを割り当てるすべてのデバイスで必要なすべての権限をどのアカウントも持たない場合などのために、複数のユーザーアカウントを追加できます。この場合、追加されたすべてのアカウントが上から下へ順番に使用され、タスクが実行されます。

10. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

11. ［**終了**］をクリックします。

    タスクが作成され、タスクリストに表示されます。

12. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

13. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。

14. ［**保存**］をクリックします。

15. 手動でタスクを実行するか、タスク設定で指定したスケジュールに基づいてタスクが起動するのを待ちます。

リモートアンインストールタスクが完了すると、選択したアプリケーションが選択したデバイスから削除されます。

タスク

このセクションでは、Kaspersky Security Center で使用できるタスクについて説明します。

タスクの概要

Kaspersky Security Center は、様々な*タスク*を作成して実行することにより、デバイス上にインストールされたカスペルスキー製品を管理します。アプリケーションのインストール、起動、停止、ファイルのスキャン、定義データベースやソフトウェアモジュールのアップデート、アプリケーションでのその他のタスクを実行するには、タスクが必要です。

Kaspersky Security Center Web コンソールを使用してアプリケーションのタスクを作成できるのは、そのアプリケーション用の管理プラグインが Kaspersky Security Center Web コンソールサーバーにインストールされている場合に限られます。

タスクは管理サーバー上とデバイス上で実行できます。

次の種別のタスクは管理サーバーで実行されます：

- レポートの自動配信
- リポジトリへのアップデートのダウンロード
- 管理サーバーデータのバックアップ
- データベースのメンテナンス

次の種別のタスクはデバイスで実行されます：

- *ローカルタスク* - 特定の1台のデバイスで実行されるタスク

  ローカルタスクを変更するには、管理者が管理コンソールツールを使用するか、またはリモートデバイスのユーザーが実行します（たとえば、セキュリティ製品のインターフェイスを使用）。管理対象デバイスの管理者とユーザーが同時にローカルタスクを変更する場合、管理者が行う変更内容の方が優先度が高いため有効になります。

- *グループタスク* - 特定のグループに属するすべてのデバイスで実行されるタスク

  タスクのプロパティで特別な設定を行わない限り、グループタスクは選択したグループのすべてのサブグループに影響します。さらに、グループタスクは該当するグループまたはそのサブグループのいずれかに導入されている、セカンダリおよび仮想管理サーバーに接続されているデバイスにも適用されます（オプション設定による）。

- *グローバルタスク* - 管理グループに含まれるかどうかに関係なく、特定のデバイスで実行されるタスク

アプリケーションごとに、任意の数のグループタスク、グローバルタスク、ローカルタスクを作成できます。

タスクの設定に変更を加え、タスクの進行状況を表示し、タスクをコピー、エクスポート、インポート、および削除できます。

タスクは、そのタスクを作成した対象のアプリケーションが実行中である場合のみ、デバイス上で開始されます。

タスクの実行結果は、各デバイスのオペレーティングシステムのイベントログと管理サーバーのオペレーティングシステムのイベントログ、および管理データベースに保存されます。

タスクの設定には個人データを使用しないでください。たとえば、ドメイン管理者パスワードを指定することは避けてください。

タスクの対象範囲

*タスク範囲*とは、タスクが実行されるデバイスの範囲です対象範囲には次の種別があります：

- *ローカルタスク*の対象範囲は、そのデバイス自体です。
- *管理サーバータスク*の対象範囲は、管理サーバーです。
- *グループタスク*の対象範囲は、グループに含まれているデバイスのリストです。

*グローバルタスク*の作成時に、次の方法を使用して対象範囲を指定できます：

- 特定のデバイスを手動で指定する

  デバイスのアドレスとして、IP アドレス（または IP アドレス範囲）、NetBIOS 名または DNS 名を使用できます。

- 追加するデバイスのアドレスが記載されている TXT ファイルからデバイスのリストをインポートする（各アドレスを独立した行に記載する必要があります）。

  デバイスのリストをファイルからインポートするかまたはリストを手動で作成し、デバイスが名前によって識別される場合、リストに含めることができるのはその情報が管理サーバーのデータベースに登録済みであるデバイスのみです。データベースへの情報の入力は、デバイスの接続時、またはデバイスの検索中に実行されます。

- デバイスの抽出を指定する。

  時間の経過とともに、抽出に含まれるデバイスセットの変更に応じてタスクの範囲が変化します。デバイスの抽出は、デバイスにインストールされているソフトウェアを含むデバイス属性、およびデバイスに割り当てられているタグに基づいて作成できます。デバイスの抽出は、タスクの範囲を定義するための最も柔軟性の高い方法です。

  デバイスの抽出を対象とするタスクは常に、管理サーバーのスケジュールに基づいて実行されます。このタスクは、管理サーバーと接続されていないデバイスでは実行できません。他の方法でタスク範囲が指定されたタスクはデバイス上で直接実行されるため、デバイスと管理サーバーとの接続の有無には左右されません。

デバイスの抽出を対象とするタスクは、デバイスのローカル時間ではなく管理サーバーのローカル時間に基づいて実行されます。他の方法でタスク範囲が指定されたタスクはデバイスのローカル時間に基づいて実行されます。

タスクの作成

タスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。表示される指示に従ってください。
3. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
4. ［**終了**］をクリックします。

タスクが作成され、タスクリストに表示されます。

選択したデバイスに割り当てる新しいタスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

   管理対象デバイスのリストが表示されます。

2. 管理対象デバイスのリストで、デバイスの横にあるチェックボックスをオンにして、そのデバイスに対してタスクを実行します。対象のデバイスを見つけるには、検索機能とフィルター機能を使用できます。

3. ［**タスクの実行**］ボタンをクリックし、［**新規タスクの追加**］を選択します。

   新規タスクウィザードが起動します。

   ウィザードの最初の手順で、タスク範囲に含めるように選択したデバイスを削除できます。ウィザードの指示に従ってください。

4. ［**終了**］をクリックします。

選択したデバイスに対してタスクが作成されます。

タスクの手動での開始

タスクは、各タスクのプロパティで指定されたスケジュール設定に従って、開始されます。タスクはタスクリストからいつでも手動で起動できます。あるいは、［**管理対象デバイス**］リストでデバイスを選択し、それらのデバイスに対する既存のタスクを開始することもできます。

タスクを手動で開始するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。

2. リスト内で、削除するタスクに隣接するチェックボックスをオンにします。

3. ［**開始**］をクリックします。

タスクが開始します。タスクのステータスは、［**ステータス**］列で、または［**結果**］をクリックして確認できます。

タスクリストの表示

Kaspersky Security Center で作成されたタスクのリストを表示できます。

タスクのリストを表示するには：

メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。

タスクのリストが表示されます。タスクは、関連するアプリケーションの名前でグループ化されます。たとえば、［*アプリケーションのリモートアンインストール*］タスクは管理サーバーに関連しており、［*脆弱性とアプリケーションのアップデートの検索*］タスクはネットワークエージェントを参照します。

タスクのプロパティを表示するには：

タスクの名前をクリックします。

タスクのプロパティウィンドウにいくつかの名前付きタブが表示されます。たとえば、［**タスク種別**］は［**全般**］タブに、タスクスケジュールは［**スケジュール**］タブに表示されます。

タスクの全般的な設定

このセクションでは、ほとんどのタスクで表示および構成できる設定について説明します。使用可能な設定のリストは、構成しているタスクによって異なります。

タスク作成時に指定する設定

タスク作成時に次の設定を指定できます。これらの設定の一部は、作成したタスクのプロパティから変更することもできます。

- OS の再起動設定：
  - **デバイスを再起動しない**

    操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

  - **デバイスを再起動する**

    インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

  - **ユーザーに処理を確認する**

    手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

    既定では、このオプションがオンです。

  - **通知の繰り返し間隔（分）**

    このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

    既定では、このオプションはオンです。既定の間隔は 5 分です。1分から1,440 分までの値を指定できます。

    このオプションをオフにすると、確認メッセージは1回だけ表示されます。

  - **再起動するまでの時間（分）**

ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

- タスクスケジュールの設定：

  スケジュールの種類はタスクによって異なる場合があります。

  - **タスク開始設定：**

    - **N 時間ごと**

      指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

      既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

    - **N 日ごと**

      日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

      既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

    - **N 分ごと**

      タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

      既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

    - **曜日ごと**

      指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

      既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。
  指定した日付が存在しない月には、月の最終日にタスクを実行します。
  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。
  規定では、日付は選択されていません。規定の開始時間は 18:00 です。

- **新しいアップデートがリポジトリにダウンロードされ次第**

  アップデートのリポジトリへのダウンロードが完了すると、タスクが実行されます。たとえば、脆弱性とアプリケーションのアップデートの検索タスクのスケジュールを設定する時に、このオプションを使用すると便利です。

- **ウイルスアウトブレイク検知次第**

  [*ウイルスアウトブレイク*] イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

  - ワークステーションとファイルサーバー向けアンチウイルス製品
  - 境界防御向けアンチウイルス製品
  - メールサーバー向けアンチウイルス製品

  既定では、すべてのアプリケーション種別がオンです。
  ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

- タスク名で検索するには、検索フィールドにタスク名を入力します。
- 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。
  既定では、タスクはアルファベットの昇順で並べ替えられます。
- フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

  このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

  このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

  このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

  既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内で自動的かつランダムに遅延させる（分）**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

既定では、このオプションはオフです。既定の時間は1分です。

- タスクを割り当てるデバイス：
  - **ネットワークの管理サーバーによって検出されたデバイスを選択する**

    タスクを特定のデバイスに割り当てます。特定のデバイスには、管理グループに属するデバイスと管理グループが割り当てられていないデバイスの両方を含めることができます。

    たとえば、未割り当てデバイスでネットワークエージェントのインストールタスクを実行する時に、このオプションを使用すると便利です。

  - **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

    タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

    特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

  - **デバイスの抽出にタスクを割り当てる**

    デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

    たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

  - **管理グループにタスクを割り当てる**

    任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

    たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

    タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

- アカウントの設定：
  - **既定のアカウント**

    タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。

    既定では、このオプションがオンです。

  - **アカウントの指定**

［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

- **アカウント**

  タスクを実行するアカウント。

- **パスワード**

  タスクが実行されるアカウントのパスワード。

タスク作成後に指定する設定

次の設定は、タスク作成後にのみ指定できます。

- グループタスクの設定：

  - **サブグループへ導入**

    このオプションはグループタスクの設定内でのみ使用可能です。

    このオプションをオンにすると、タスク範囲には次のものが含まれます：

    - タスクの作成中に選択した管理グループ。
    - 選択された管理グループに属する管理グループのすべてのレベルはグループ階層の下にあります。

    このオプションをオフにすると、タスク範囲にはタスクの作成中に選択された管理グループのみが含まれます。

    既定では、このオプションはオンです。

  - **セカンダリまたは仮想管理サーバーに配信**

    このオプションをオンにすると、プライマリ管理サーバーに対して有効なタスクがセカンダリ管理サーバーに対しても適用されます（仮想管理サーバーも含まれます）。同じ種別のタスクがセカンダリ管理サーバーに既に存在する場合は、既存のタスクとプライマリ管理サーバーから継承した両方のタスクがセカンダリ管理サーバーに適用されます。

    このオプションは［**サブグループへ導入**］がオンになっている場合にのみ使用可能です。

    既定では、このオプションはオフです。

- スケジュールの詳細設定

  - **Wake on LAN の機能を使用してタスク開始前にデバイスを起動する**

タスク開始よりも指定した時間だけ前に、デバイス上のオペレーティングシステムが起動します。既定では、時間は 5 分です。

タスクの開始予定時刻が近づいても電源がオフだったデバイスも含めて、タスク範囲に含まれるすべてのクライアントデバイスでタスクを実行するには、このオプションをオンにします。

タスクの完了後にデバイスの電源を自動的にオフにする場合は、［**タスク完了後にデバイスをシャットダウンする**］を有効にします。このオプションは同じウィンドウ内にあります。

既定では、このオプションはオフです。

- **タスク完了後にデバイスをシャットダウンする**

  たとえば、毎週金曜日の業務時間終了後にクライアントデバイスへのアップデートのインストールを行い、その後デバイスの電源を切りたい時に、アップデートインストールタスクでこのオプションを使用できます。

  既定では、このオプションはオフです。

- **次の時間を超える場合はタスクを停止する**

  指定した時間が経過すると、タスクが完了したかどうかに関係なくタスクが自動的に停止します。
  実行に時間がかかり過ぎているタスクを中断したい時に、このオプションを使用します。
  既定では、このオプションはオフです。既定のタスク実行時間は 120 分です。

- 通知の設定：
  - ［**タスク履歴の保存**］セクション：
    - **管理サーバーのデータベースに保存（日）**

      タスク範囲に含まれるすべてのクライアントデバイスでのタスク実行に関するアプリケーションイベントが、指定した日数の間、管理サーバーに保存されます。この期間が過ぎると、情報が管理サーバーから削除されます。

      既定では、このオプションはオンです。

    - **デバイスの OS イベントログに保存**

      タスク実行に関するアプリケーションイベントが、各クライアントデバイスの Windows イベントログにローカルで保存されます。

      既定では、このオプションはオフです。

    - **管理サーバーの OS イベントログに保存**

      タスク範囲に含まれるすべてのクライアントデバイスでのタスク実行に関するアプリケーションイベントが、管理サーバーのオペレーティングシステムの Windows イベントログに一元的に保存されます。

      既定では、このオプションはオフです。

- **すべてのイベントを保存**

  このオプションをオンにすると、タスクに関するすべてのイベントがイベントログに保存されます。

- **タスクの進捗に関連したイベントを保存**

  このオプションをオンにすると、タスク実行に関するイベントのみがイベントログに保存されます。

- **タスク実行結果のみ保存**

  このオプションをオンにすると、タスクの実行結果に関するイベントのみがイベントログに保存されます。

- **管理者にタスク実行結果を通知**

  管理者がタスク実行結果の通知を受け取る方法を、メール、SMS、実行ファイルの実行から選択できます。通知を設定するには、［**設定**］をクリックします。

  既定では、すべての通知方法がオフです。

- **エラーのみ通知**

  このオプションをオンにすると、管理者はタスクでエラーが発生して終了した場合にのみ通知を受け取ります。

  このオプションをオフにすると、管理者はタスク終了時に常に通知を受け取ります。

  既定では、このオプションはオンです。

- セキュリティ設定

- タスク範囲の設定

  タスク範囲の指定方法に応じて、次の設定が表示されます：

  - **デバイス**

    タスク範囲が管理グループを使用して指定されている場合、該当するグループを表示できます。ここでは、設定を変更することはできません。ただし、［**タスク範囲からの除外**］を設定できます。

    タスク範囲がデバイスのリストを使用して指定されている場合、デバイスを追加したり削除してこのリストを変更できます。

  - **デバイスの抽出**

    タスクが適用されるデバイスの抽出を変更できます。

  - **タスク範囲からの除外**

タスクを適用しないデバイスのグループを指定できます。タスク範囲から除外できるのは、タスクが適用されない管理グループのサブグループのみです。

- **変更履歴**

タスクのエクスポート

Kaspersky Security Center を使用すると、タスクとその設定を KLT ファイルに保存できます。この KLT ファイルを使用して、Kaspersky Security Center Windows と Kaspersky Security Center Linux の両方に保存したタスクをインポートできます。

タスクをエクスポートするには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. エクスポートするタスクの横のチェックボックスをオンにします。

   複数のタスクを同時にエクスポートすることはできません。複数のタスクを選択すると、［**エクスポート**］が無効になります。管理サーバーのタスクもエクスポートできません。
3. ［**エクスポート**］をクリックします。
4. 表示される［**名前を付けて保存**］ウィンドウで、タスクファイルの名前とパスを指定します。［**保存**］をクリックします。

   ［**名前を付けて保存**］ウィンドウは、Google Chrome、Microsoft Edge、または Opera を使用している場合にのみ表示されます。別のブラウザーを使用する場合、タスクファイルは自動的に［**Downloads**］フォルダーに保存されます。

タスクのインポート

Kaspersky Security Center を使用すると、KLT ファイルからタスクをインポートできます。KLT ファイルには、エクスポートされたタスクとその設定が含まれています。

タスクをインポートするには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**インポート**］をクリックします。
3. ［**参照**］をクリックして、インポートするタスクファイルを選択します。
4. 開いたウィンドウで、KLT タスクファイルへのパスを指定して、［**開く**］をクリックします。選択できるタスクファイルは 1 つだけです。

   タスクの処理が始まります。
5. タスクが正常に処理されたら、タスクを割り当てるデバイスを選択します。これには、次のいずれかのオプションを選択します：

   - **管理グループにタスクを割り当てる**

任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

  タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

  特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

- **デバイスの抽出にタスクを割り当てる**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

6. タスク範囲を指定します。

7. ［**完了**］をクリックしてタスクのインポートを完了します。

インポート結果の通知が表示されます。タスクが正常にインポートされた場合は、［**詳細**］をクリックして、タスクのプロパティを表示できます。

インポートが成功すると、タスクがタスクリストに表示されます。タスクの設定とスケジュールもインポートされます。タスクはスケジュールに従って開始されます。

新しくインポートされたタスクと同じ名前のタスクが既に存在している場合、インポートされたタスクの名前に、たとえば **(1)**、**(2)** のようなインデックス「**(<次の連番>)**」が付きます。

タスクのパスワード変更ウィザードの起動

非ローカルタスクの場合、タスクを実行するアカウントを指定できます。アカウントは、タスクの作成時または既存のタスクのプロパティで指定できます。指定されたアカウントが組織のセキュリティ指示に従って使用されている場合、その指示によってアカウントパスワードの変更が必要になる場合があります。アカウントパスワードの有効期限が切れて新しいパスワードを設定すると、タスクプロパティで新しい有効なパスワードを指定するまで、タスクを開始しません。

タスクのパスワード変更ウィザードを使用すると、アカウントが指定されているすべてのタスクで、古いパスワードを新しいパスワードに自動的に置換できます。または、各タスクのプロパティで、このパスワードを手動で変更できます。

タスクのパスワード変更ウィザードを起動するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**タスク開始に使用するアカウントの資格情報の管理**］をクリックします。

ウィザードの指示に従ってください。

ステップ 1：資格情報の指定

お使いのシステム（Active Directory など）で現在有効な新しい資格情報を指定します。ウィザードの次のステップに進むと、指定されたアカウント名が、非ローカルタスクそれぞれのプロパティのアカウント名と一致するかどうか確認されます。アカウント名が一致すると、タスクのプロパティのパスワードは自動的に新しいものに置換されます。

新しいアカウントを指定するには、オプションを選択します：

- **現在のアカウントを使用**

  ウィザードは、Kaspersky Security Center Web コンソールに現在サインインしているアカウントの名前を使用します。次に、［**タスクで使用する現在のパスワード**］で、アカウントのパスワードを手動で指定します。

- **別のアカウントを指定**

  タスクを起動する必要があるアカウントの名前を指定します。次に、［**タスクで使用する現在のパスワード**］で、アカウントのパスワードを指定します。

［**以前のパスワード（任意。現在のパスワードに置換したい場合に使用）**］フィールドに手動で入力した場合、アカウント名と古いパスワードの両方が見つかったタスクの、パスワードのみが置換されます。置換は自動で実行されます。その他の場合はすべて、ウィザードの次の手順で、実行する処理を選択する必要があります。

ステップ 2：実行する処理の選択

ウィザードの最初の手順で古いパスワードを指定しなかった場合、または指定した古いパスワードがタスクのプロパティのパスワードと一致しない場合、見つかったタスクに対して実行する処理を選択する必要があります。

タスクに対する処理を選択するには：

1. 処理を選択するタスクに隣接するチェックボックスをオンにします。
2. 次のいずれかを実行します：
   - タスクのプロパティのパスワードを削除するには、［**資格情報の削除**］をクリックします。
     タスクは既定のアカウントで実行されるように切り替わります。
   - パスワードを新しいパスワードに置換するには、［**古いパスワードが正しくないか未入力の場合でもパスワードの変更を強制する**］をクリックします。
   - パスワードの変更をキャンセルするには、［**処理が選択されていません**］をクリックします。

ウィザードの次のステップに移動すると、選択した処理が適用されます。

ステップ 3：結果の表示

ウィザードの最後のステップで、見つかった各タスクの結果を表示します。ウィザードを終了するには、［**終了**］をクリックします。

スクリプトをリモートで実行タスクの作成

クライアントデバイス上でインストールパッケージを実行し、アプリケーションをリモートでインストールするための*スクリプトをリモートで実行*タスクを作成できます。

インストールパッケージには、クライアントデバイスで実行するためのスクリプトのセットとファイル manifest.json を含む ZIP アーカイブが含まれています。このタイプのインストールパッケージの作成の詳細については、この記事を参照してください。

このタスクは、Linux 用ネットワークエージェントがインストールされているデバイスでのみ開始する必要があります。

スクリプトをリモートで実行タスクを開始するには：

1. **新規タスクウィザード**に移動し、**スクリプトをリモートで実行**タスクタイプを選択します。
2. タスク名を入力し、タスクを割り当てるデバイスを選択します。［**次へ**］をクリックします。
3. リモート実行用のファイル manifest.json を含む ZIP アーカイブに基づくインストールパッケージを選択します。

   タスクが既に完了しているデバイスで、タスクを再実行しない場合は、［**タスクが完了済みのデバイスではこのタスクを開始しない**］をオンにします。
4. タスクを実行するアカウントを選択します。

   既定アカウントを選択した場合、タスクはネットワークエージェント（root アカウント）によって実行されます。

   *スクリプトをリモートで実行*タスクが開始されると、割り当てられているアカウントを変更することはできません。タスクが割り当てられているアカウントを変更するには、タスク設定でタスクを停止し、正しいアカウント詳細で再度作成します。
5. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後でいつでも実行できます。
6. ［**終了**］をクリックします。

   *スクリプトをリモートで実行*タスクが作成され、タスクリストに表示されます。

ネットワークエージェントは、*スクリプトをリモートで実行*タスクからデータを受信した後、管理者とタスク設定で指定されたユーザーを除くすべてのユーザーに対して、受信したデータへのアクセスを制限します。

スクリプトをリモートで実行タスクを使用して、デバイスにアプリケーションをリモートでインストールする

*スクリプトをリモートで実行*タスクを使用すると、カスタムインストールパッケージを作成して、クライアントデバイスにアプリケーションをリモートでインストールできます。

このタスク用のアーカイブを準備する方法については、この記事を参照してください。

クライアントデバイスにアプリケーションをリモートインストールするためのインストールパッケージを作成するには、このタスク用にアップロードするアーカイブに次のファイルが含まれている必要があります。

- <package_name>.deb
- install.sh

  ```
  sudo dpkg -I <package_name>.deb
  ```

- manifest.json

アプリケーションのリモートインストール用の JSON スキーマ

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "< 必要に応じて引数を入力 >",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

配列の説明

1. `version` - マニフェストファイルとタスクのバージョン。
   現在、許容される値は 1 のみです。
2. `actions` 配列の要素によって、タスクで実行されるスクリプトの構成と順序が決まります。
   スクリプトの実行順序は、配列内の要素のインデックス（場所）に対応します。
3. `actions` 配列の各要素に対して、次の要素が定義されます。
   a. `type` - スクリプトから実行可能なコマンドのタイプ。現時点では、値は常に `execute` です。
   b. `path` - アーカイブ内のスクリプトファイルへのパス。
   c. `args` - 実行可能コマンドの一部としてスクリプトに渡される引数。
   d. `results` - タスクの結果に応じてさらなるアクションを定義する配列。
      1. `code` - スクリプトを返す値。
      2. `next` - 次に完了するアクション。`continue` アクションは次のスクリプト（`actions` 配列内の要素）の実行に進み、`break` アクションはタスクを停止します。
   e. `default_next` - スクリプトが `results` に含まれていない値を返した場合のアクション。

*スクリプトをリモートで実行*タスクが開始されると、ネットワークエージェントはアプリケーションを含むインストールパッケージをクライアントデバイスにアップロードします。クライアントデバイスがインストールパッケージを受信すると、このデバイス上のネットワークエージェントはファイル manifest.json を解析し、結果に応じてスクリプトとアクションの実行順序を定義して実行を開始します。

*スクリプトをリモートで実行*タスクが完了すると、アプリケーションがクライアントデバイスにインストールされます。

スクリプトをリモートで実行するタスクの通知と監視を設定する

*スクリプトをリモートで実行*タスクの監視、イベント保存動作、および通知を設定できます。

スクリプトをリモートで実行のステータスを表示するには：

1. メインメニューで、［**デバイス**］→［**タスク**］の順に移動します。
   タスクのリストが表示されます。
2. タスクを選択し、［**デバイスの履歴**］をクリックします。
   タスクの進行状況が表示されます。

イベント保存動作を設定するには：

1. タスクのリストで、タスクをクリックして［**設定**］タブに移動します。
2. ［**通知**］セクションで、［**設定**］をクリックします。
3. タスクが完了した後のアプリケーションの動作については、次のいずれかのオプションを選択します。
   - **すべてのイベントを保存**する。
   - **タスクの進捗に関連したイベントを保存**：
   - **タスク実行結果のみ保存**：
     イベントは**デバイスの履歴**と**イベントリポジトリ**に保存されます。
     既定では、タスクの実行結果のみが保存されます。

     ［**すべてのイベントを保存**］を選択した場合は、タスクの実行結果のみが保存されます。
4. イベントを管理サーバーの定義データベース、管理サーバー上のイベントログ、またはデバイス上に保存する場合は、対応するオプションをオンにします。

通知の設定の詳細については、この記事を参照してください。

スクリプトをリモートで実行タスク用のアーカイブを準備する

ファイル manifest.json に基づく*スクリプトをリモートで実行*タスクのアーカイブは、次の要件を満たす必要があります。

- アーカイブ形式：ZIP。
- 合計サイズ：1 GB 以下。
- アーカイブ内のファイルとフォルダーの数に制限はありません。
- アーカイブのマニフェストファイルは以下のスキーマと一致し、manifest.json という名前にする必要があります。スキーマは、デバイス上でタスクが実行されるときにのみ検証されます。

マニフェストファイルの JSON スキーマと配列の説明

JSON スキーマ

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
```

```
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

マニフェストファイルの例

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- アーカイブは次のように構造化する必要があります：

  `manifest.json`

<file1>

<file2>

<folder1>/<file3>

<folder2>/<folder3>/<file4>

...

<fileX>

manifest.json はタスクのマニフェストファイルです。

<file1>, ..., <fileX> は、実行されるスクリプトを含むファイルのセットです。

マニフェストファイルに基づいてインストールパッケージを作成する

マニフェストファイルに基づいてインストールパッケージを作成するには：

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動します。
   - メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

   管理サーバーで利用可能なインストールパッケージのリストが表示されます。

2. ［**追加**］をクリックします。

   新規パッケージウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. **ファイル manifest.json を含む ZIP アーカイブを基に［スクリプトを自動で実行］タスクのインストールパッケージを作成する**］を選択します。

4. パッケージ名を指定して、［**参照**］をクリックします。

   ブラウザーで Windows 標準の［**ファイルを開く**］ウィンドウが開き、インストールパッケージを作成するファイルを選択できます。

5. 事前に準備しておいた圧縮ファイルを選択します。このタスク用のアーカイブを準備する方法については、この記事を参照してください。

   ファイルが Kaspersky Security Center 管理サーバーにアップロードされ始めます。

   カスタムインストールパッケージを作成するプロセスが開始されます。

   プロセスが終了すると、ウィザードで通知されます。

   インストールパッケージが作成されなかった場合も、メッセージで通知されます。

6. ［**終了**］をクリックしてウィザードを終了します。

作成したインストールパッケージは、管理サーバーの共有フォルダーのパッケージ用のサブフォルダーにアップロードされます。アップロード後、インストールパッケージがインストールパッケージのリストに表示されます。

管理サーバーで利用できるインストールパッケージのリストで、カスタムインストールパッケージの名前をクリックすることで次の操作を実行できます：

- インストールパッケージのプロパティとして以下の情報を表示する：

- **名前：**カスタムインストールパッケージの名前。
- **ソース：**アプリケーションの開発元の名前。
- **バージョン：**アプリケーションのバージョン。
- **作成：**インストールパッケージの作成日時。
- **変更：**インストールパッケージの変更日時。
- **パス：**管理サーバー上のカスタムインストールパッケージへのパス。

- パッケージ名とコマンドラインのパラメータを変更する。この操作は、カスペルスキー製品に基づいて作成されていないインストールパッケージでのみ実行できます。

クライアントデバイスの管理

Kaspersky Security Center では、クライアントデバイスを管理することができます。

- クラスターやサーバーアレイなどの管理対象デバイスの設定とステータスを表示します。
- ディストリビューションポイントの設定。
- タスクの管理。

管理グループを使用すると、クライアントデバイスを1つのユニットとして管理できるセットにまとめることができます。クライアントデバイスは1つの管理グループにのみ含めることができます。［**ルールの条件**］に基づいてデバイスをグループに自動的に割り当てることができます。

- デバイス移動ルールの作成。
- デバイス移動ルールのコピー。
- デバイス移動ルールの条件。

デバイスの抽出を使用すると、条件に基づいてデバイスをフィルタリングできます。抽出を作成したり、デバイスを検索したり、管理グループ間でデバイスを配置したりするために、デバイスにタグを付けることもできます。

管理対象デバイスの設定

管理対象デバイスの設定を表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、目的のデバイス名のリンクをクリックします。

選択したデバイスのプロパティウィンドウが表示されます。

次のタブは、設定の主なグループを表すプロパティ ウィンドウの上部に表示されます。

- **全般**

このタブは次のセクションで構成されています。

- ［**全般**］セクションには、クライアントデバイスに関する全般的な情報が表示されます。情報は、クライアントデバイスと管理サーバーとの前回の同期中に受信されたデータに基づいて提供されます：

  - **名前**

    このフィールドでは、管理グループ内のクライアントデバイスの名前を表示したり変更したりできます。

  - **説明**

    このフィールドでは、クライアントデバイスの補足的な説明を入力できます。

  - **デバイスのステータス**

    管理者によって定義された基準に基づいて、デバイス上のアンチウイルスによる保護のステータスとデバイスのネットワーク動作に対して割り当てられたクライアントデバイスのステータス。

  - **グループの完全名**

    クライアントデバイスが属する管理グループ。

  - **前回の定義データベースのアップデート**

    定義データベースまたはアプリケーションをデバイス上で前回アップデートした日付。

  - **管理サーバーへの接続**

    クライアントデバイスにインストールされたネットワークエージェントが管理サーバーに最後に接続した日時。

  - **前回の可視**

    デバイスが前回ネットワークで検出された日時。

  - **ネットワークエージェントのバージョン**

    インストールされているネットワークエージェントのバージョン。

  - **作成**

    Kaspersky Security Center 内でデバイスが作成された日付。

  - **デバイスの所有者**

デバイス所有者の名前。［**デバイスの所有者の管理**］をクリックすることにより、ユーザーをデバイスの所有者として割り当てたり削除したりすることができます。

- **管理サーバーから切断しない**

  このオプションをオンにすると、管理対象デバイスと管理サーバー間の継続的な接続が維持されます。このオプションは、継続的な接続を提供するプッシュサーバーを使用していない場合に使用することがあります。

  このオプションがオフで、プッシュサーバーが使用されていない場合、管理対象デバイスは、データの同期または情報の送信のためにのみ管理サーバーに接続します。

  ［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

  このオプションは、管理対象デバイスでは既定でオフになっています。このオプションは、管理サーバーがインストールされているデバイスでは既定でオンになっており、オフにしようとしてもオンのままになります。

- ［**ネットワーク**］セクションには、クライアントデバイスのネットワークプロパティに関する次の情報が表示されます：

  - **IP アドレス**

    デバイスの IP アドレス。

  - **Windows ドメイン**

    このデバイスを含む Windows ドメインまたはワークグループ。

  - **DNS 名**

    クライアントデバイスの DNS ドメイン名。

  - **NetBIOS 名**

    クライアントデバイスの Windows ネットワークでの名前。

  - **IPv6 アドレス**

- ［**システム**］セクションには、クライアントデバイスにインストールされているオペレーティングシステムに関する情報が表示されます。

  - **オペレーティングシステム**
  - **CPU アーキテクチャ**
  - **デバイス名**
  - **仮想マシンの種別**

    仮想マシンの製造元。

- **動的仮想マシン (VDI の一部)**

  この行には、クライアントデバイスが VDI の一部である動的仮想マシンかどうかが表示されます。

- ［**プロテクション**］セクションには、次のようなクライアントデバイスにおけるアンチウイルスによる保護に関する現在のステータスが表示されます：

  - **可視**

    クライアントデバイスの可視性のステータス。

  - **デバイスのステータス**

    管理者によって定義された基準に基づいて、デバイス上のアンチウイルスによる保護のステータスとデバイスのネットワーク動作に対して割り当てられたクライアントデバイスのステータス。

  - **ステータスの説明**

    クライアントデバイスの保護と管理サーバーへの接続のステータス。

  - **保護ステータス**

    クライアントデバイスのリアルタイム保護に関する現在のステータスが表示されます。

    デバイスのステータスに変更があると、新しいステータスは、クライアントデバイスと管理サーバーが同期された後にのみデバイスのプロパティウィンドウに表示されます。

  - **前回の完全スキャン**

    クライアントデバイスで前回のマルウェアスキャンが実行された日時。

  - **ウイルスが検知されました**

    セキュリティ製品のインストール後（最初のスキャンの場合）またはウイルスカウンターを前回リセットした後に、クライアントデバイスで検知された脅威の合計数。

  - **駆除できていないオブジェクト**

    クライアントデバイスにおける未処理ファイルの数。

    このフィールドは、モバイルデバイス上の未処理ファイルの数をスキップします。

  - **ディスク暗号化ステータス**

    デバイスのローカルドライブでのファイル暗号化の現在のステータス。ステータスの説明は、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

- ［**製品が定義したデバイスのステータス**］セクションには、デバイスにインストールされている管理対象アプリケーションによって定義されたデバイスのステータスに関する情報が表示されます。このデバイスのステータスは、Kaspersky Security Center によって定義されたものとは異なる場合があります。

- **アプリケーション**

  このタブには、クライアントデバイスにインストールされているすべてのカスペルスキー製品が一覧表示されます。このタブには、選択したカスペルスキー製品（ネットワークエージェントを除く）を開始および停止できる［**開始**］と［**停止**］があります。管理対象デバイスで管理サーバーからの受信プッシュ通知用にポート 15000 UDP が使用可能な場合は、これらのボタンを使用できます。管理対象デバイスがプッシュ通知に使用できないが、管理サーバーへの継続的な接続モードが有効になっている場合（［**全般**］セクションの［**管理サーバーから切断しない**］がオンになっている場合）、［**開始**］と［**停止**］も使用できます。そうしないと、アプリケーションを起動または停止しようとすると、エラーメッセージが表示されます。また、アプリケーション名をクリックすると、アプリケーションに関する一般情報、デバイスで発生したイベントのリスト、およびアプリケーション設定が表示されます。

- **アクティブなポリシーとポリシーのプロファイル**

  このタブには、管理対象デバイスに現在割り当てられているポリシーとポリシープロファイルが一覧表示されます。

- **タスク**

  ［**タスク**］タブでは、既存タスクのリストの表示、新規タスクの作成、タスクの削除、タスクの開始と停止、タスク設定の変更、実行結果の表示など、クライアントデバイスのタスクを管理できます。タスクのリストは、管理サーバーとの前回のクライアント同期セッション中に受信されたデータに基づいて提供されます。管理サーバーは、タスクステータスに関する情報をクライアントデバイスに要求します。管理対象デバイスで管理サーバーからのプッシュ通知を受信するためにポート 15000 UDP が使用可能な場合は、タスクのステータスが表示され、タスクを管理するためのボタンが有効になります。管理対象デバイスがプッシュ通知に使用できないが、管理サーバーへの継続的な接続モードが有効になっている場合（［**全般**］セクションの［**管理サーバーから切断しない**］がオンになっている場合）、タスクによるアクションも利用できます。

  接続に失敗すると、ステータスは表示されず、ボタンは無効になります。

- **イベント**

  ［**イベント**］タブでは、選択したクライアントデバイスについて管理サーバーに記録されたイベントが表示されます。

- **セキュリティ問題**

［**セキュリティ問題**］タブでは、クライアントデバイスでのセキュリティ問題を表示、編集、作成できます。セキュリティ問題は、クライアントデバイスにインストールしたカスペルスキー製品によって自動で作成されるか、管理者が手動で作成します。たとえば、定期的にマルウェアを自分のリムーバブルドライブからデバイスに移しているユーザーがいた場合、管理者はこの件のセキュリティ問題を作成できます。管理者はセキュリティ問題のテキストに、概要説明と推奨される処分（ユーザーに下す懲戒処分など）を記載したり、ユーザーへのリンクを追加することもできます。

必要な処分がすべて行われたセキュリティ問題は、*処理済み*と呼ばれます。未処理のセキュリティ問題がある場合、デバイスのステータスを*緊急*または*警告*に変更する条件として選択できます。

このセクションには、デバイス用に作成したセキュリティ問題のリストがあります。セキュリティ問題は、重要度と種別で分類されます。セキュリティ問題のタイプは、セキュリティ問題を作成するカスペルスキー製品によって定義されます。［**処理済み**］列のチェックボックスをオンにすると、リストにある処理済みのセキュリティ問題を強調表示できます。

- **タグ**

［**タグ**］タブでは、クライアントデバイスの検索に使用されるキーワードのリストを管理できます。また、既存のタグのリストの表示、リストからのタグの割り当て、自動タグ付けルールの設定、新規タグの追加、既存のタグの名称変更、タグの削除なども可能です。

- **詳細**

このタブは次のセクションで構成されています。

- **アプリケーションレジストリ**。このセクションでは、クライアントデバイス上にインストールされたアプリケーションのレジストリとそのアップデートを表示し、アプリケーションレジストリの表示を設定することができます。

  インストール済みアプリケーションの情報は、クライアントデバイスにインストールされているネットワークエージェントから必要な情報が管理サーバーに送信されている場合に供給されます。管理サーバーへの情報の送信は、ネットワークエージェントまたはそのポリシーのプロパティウィンドウにある［**リポジトリ**］セクションで設定できます。

  アプリケーション名をクリックすると、アプリケーションの詳細とアプリケーションにインストールされているアップデートパッケージのリストを表示するウィンドウが開きます。

- **実行ファイル**。このセクションには、クライアントデバイスにある実行ファイルが表示されます。

- **ディストリビューションポイント**。このセクションでは、デバイスがインタラクトするディストリビューションポイントのリストについて説明します。

  - **ファイルへのエクスポート**

    ［**ファイルへのエクスポート**］をクリックすると、デバイスがインタラクトするディストリビューションポイントのリストがファイルに保存されます。既定では、デバイスのリストは CSV ファイルにエクスポートされます。

  - **プロパティ**

    ［**プロパティ**］をクリックすると、デバイスがインタラクトするディストリビューションポイントが表示および設定されます。

- **ハードウェアレジストリ**。このセクションでは、クライアントデバイスにインストールされているハードウェアに関する情報を表示できます。

- **適用可能なアップデート**。このセクションには、デバイスで検出されたがインストールされていないソフトウェアアップデートのリストが表示されます。

- **ソフトウェアの脆弱性**。このセクションには、クライアントデバイスにインストールされているサードパーティのソフトウェアの脆弱性に関する情報が表示されます。

  脆弱性をファイルに保存するには、保存する脆弱性に隣接するチェックボックスをオンにして、［**CSV へエクスポート**］または［**TXT へエクスポート**］をクリックします。

  このセクションには、次の設定項目があります：

  - **修正可能な脆弱性のみ表示**

    このオプションを有効にすると、パッチを使用して修正できる脆弱性が表示されます。

    このオプションをオフにすると、パッチを使用して修正できる脆弱性と、パッチがリリースされていない脆弱性の両方が表示されます。

    既定では、このオプションはオンです。

  - **脆弱性のプロパティ**

リストにあるソフトウェアの脆弱性の名前をクリックすると、選択したソフトウェアの脆弱性のプロパティが別のウィンドウに表示されます。ウィンドウで次の操作を実行できます：

- 対象の管理対象デバイスではこのソフトウェア脆弱性を無視するようにする（管理コンソールまたは Kaspersky Security Center Web コンソールで操作）。
- 脆弱性に対して推奨される修正のリストを表示する。
- 脆弱性を修正するソフトウェアアップデートを手動で指定する（管理コンソールまたは Kaspersky Security Center Web コンソール）。
- 脆弱性の該当数を表示する。
- 脆弱性を修正するための既存のタスクのリストを表示したり、脆弱性を修正するためのタスクを新規作成する。

- **リモート診断**。このセクションでは、クライアントデバイスのリモート診断を実行できます。

PostgreSQL、MariaDB、または MySQL DBMS を使用する場合、[**イベント**] タブには、選択したクライアントデバイスのイベントの不完全なリストが表示されることがあります。これは、DBMS が非常に大量のイベントを保存する場合に発生します。次のいずれかを実行すると、表示されるイベントの数を増やすことができます：

- 不要なイベントを削除します。
- 不要なイベントの保存期間を短縮します。

デバイスの管理サーバーに記録されたイベントの完全なリストを表示するには、レポートを使用します。

管理グループの作成

Kaspersky Security Center のインストール直後に、［**管理対象デバイス**］と呼ばれる管理グループが 1 つだけ管理グループの階層に含まれます。管理グループの階層の作成時に、仮想マシンを含むデバイスを［**管理対象デバイス**］グループに追加したり、ネストされたグループを追加したりできます。

管理グループ階層の表示

管理グループを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。

2. 管理グループの構成で、新しい管理グループを含める管理グループを選択します。

3. ［**追加**］をクリックします。

4. 表示される［**新しい管理グループの名前**］ウィンドウで、 グループの名前を入力して［**追加**］をクリックします。

   指定した名前の新しい管理グループが管理グループの階層に表示されます。

Active Directory またはドメインネットワークの構成に基づいて管理グループの階層を作成することが可能です。テキストファイルからグループの構成を作成することも可能です。

管理グループの構造を作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。

2. ［**インポート**］をクリックします。

   新規管理グループ構造作成ウィザードが開始します。ウィザードの指示に従ってください。

デバイスを管理グループへ手動で追加

デバイス移動ルールを作成してデバイスを管理グループに自動的に移動したり、選択した管理グループにデバイスを追加することで、デバイスを管理グループ間で手動で移動したりすることができます。このセクションでは、デバイスを管理グループに手動で追加する手順を説明します。

特定の管理グループに1台以上のデバイスを手動で追加するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

2. リストの上にある［**現在のパス：**<現在のパス>］をクリックします。

3. 表示されるウィンドウで、デバイスを追加する管理グループを選択します。

4. ［**デバイスの追加**］をクリックします。
   デバイス移動ウィザードが起動します。

5. 管理グループに追加するデバイスのリストを作成します。

   > デバイスへの接続時に、またはデバイスの検出後に、管理サーバーのデータベースに既に情報が追加されているデバイスのみを追加できます。

   デバイスをリストに追加する方法を選択します：

   - ［**デバイスの追加**］をクリックして、次のいずれかの方法でデバイスを指定します：
     - 管理サーバーによって検出されたデバイスのリストからデバイスを選択します。
     - デバイスの IP アドレスまたは IP アドレス範囲を指定します。
     - デバイスの NetBIOS 名または DNS 名を指定します。

デバイス名のフィールドには、空白文字および禁止されている文字（\/*;:`~!@#$^&()=+[]{}|,<>%）を含めることはできません。

- ［**デバイスをファイルからインポート**］をクリックして、テキストファイルからデバイスのリストをインポートします。各デバイスのアドレスまたは名前をそれぞれの行に指定する必要があります。

ファイルには、空白文字および禁止されている文字（\/*;:`~!@#$^&()=+[]{}|,<>%）を含めることはできません。

6. 管理グループに追加するデバイスのリストを表示します。デバイスを追加または削除することでリストを編集できます。

7. リストが正しいことを確認したら、［**次へ**］をクリックします。

ウィザードによってデバイスリストが処理され、結果が表示されます。正常に処理されたデバイスが管理グループに追加され、管理サーバーによって作成された名前でデバイスのリストに表示されます。

デバイスまたはクラスターを手動で管理グループに移動する

管理グループ間で、または未割り当てデバイスのグループから管理グループにデバイスを移動できます。

管理グループからクラスターまたはサーバーアレイを別の管理グループに移動することもできます。クラスターまたはサーバーアレイを別のグループに移動すると、そのすべてのノードも一緒に移動します。これは、クラスターとそのノードのいずれかが常に同じ管理グループに属しているためです。［**デバイス**］タブで単一のクラスターノードを選択すると、［**グループへ移動**］が使用できなくなります。

特定の管理グループに1台以上のデバイスまたはクラスターを移動するには：

1. デバイスの移動元の管理グループを開きます。開くには、次のいずれかの操作を行います：

   - 管理グループを開くには、メインメニューで［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動し、［**現在のパス**］フィールドのパスリンクをクリックして、開いた左側のペインで管理グループを選択します。

   - ［**未割り当てデバイス**］のグループを開くには、メインメニューで、［**検出と製品の導入**］→［**未割り当てデバイス**］の順に移動します。

2. 管理グループにクラスターまたはサーバーアレイが含まれている場合、［**管理対象デバイス**］セクションは、［**デバイス**］タブと［**クラスターとサーバーアレイ**］タブの2つのタブに分割されます。移動するオブジェクトのタブを開きます。

3. 別のグループに移動するデバイスまたはクラスターに隣接するチェックボックスをオンにします。

4. ［**グループへ移動**］をクリックします。

5. 管理グループの階層で、選択したデバイスまたはクラスターの移動先の管理グループに隣接するチェックボックスをオンにします。

6. ［**移動**］をクリックします。

選択したデバイスまたはクラスターが、選択した管理グループに移動します。

デバイス移動ルールの作成

デバイスを自動的に管理グループに割り当てるデバイス移動ルールを設定できます。

移動ルールを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**移動ルール**］の順に移動します。
2. ［**追加**］をクリックします。
3. 表示されたウィンドウの［**全般**］タブで、次の情報を指定します：

- **ルール名**

  新しいルールの名前を入力します。
  ルールのコピー時には、新しいルールでは、元のルールと同じ名前に「(1)」のようなインデックス「(数字)」が追加されます。

- **管理グループ**

  デバイスを自動的に移動する移動先の管理グループを選択します。

- **アクティブなルール**

  このオプションをオンにすると、ルールの保存後にルールが有効になり適用されます。
  このオプションをオフにすると、ルールは作成されますがオフの状態です。このオプションをオンにするまで、ルールは適用されません。

- **どの管理グループにも属していないデバイスのみ移動する**

  このオプションをオンにすると、未割り当てデバイスのみが選択したグループに移動します。
  このオプションをオフにすると、既に管理グループに割り当てられているデバイスと未割り当てデバイスの両方が選択したグループに移動します。

- **ルールの適用**

次の中からいずれかを選択できます：

- **各デバイスにつき1回**

  指定した条件に合致するデバイスで各デバイスにつき1回だけルールが適用されます。

- **各デバイスで1度実行、以降はネットワークエージェントの再インストールごとに実行**

  指定した条件に合致するデバイスで各デバイスにつき1回ルールが適用され、その後はデバイスにネットワークエージェントが再インストールされた場合にのみ適用されます。

- **ルールを永続的に適用**

  管理サーバーで自動的に設定されるスケジュールに従ってルールが適用されます（通常は数時間ごと）。

4. ［**ルールの条件**］タブで、デバイスを管理グループに移動する基準を少なくとも1つ指定します。
5. ［**保存**］をクリックします。

移動ルールが作成されます。新しいルールが移動ルールのリストに表示されます。

リストでの順位が高いほど、ルールの優先度が高くなります。移動ルールの優先度を上げたり下げたりするには、マウスを使用してルールをリスト内でそれぞれ上下に移動します。

［**ルールを永続的に適用**］をオンにした場合、優先度設定に関係なく移動ルールが適用されます。このようなルールは、管理サーバーが自動的に設定したスケジュールに従って適用されます。

デバイス属性が複数のルールの条件を満たしている場合、そのデバイスは優先度が最も高いルールの対象グループに移動されます（つまり、ルールのリスト内で最高ランク）。

デバイス移動ルールのコピー

異なる管理グループで同一のルールを使用する場合などに、移動ルールをコピーできます。

既存の移動ルールをコピーするには：

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**アセット（デバイス）**］→［**移動ルール**］の順に移動します。
   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**移動ルール**］の順に移動します。

   移動ルールのリストが表示されます。

2. コピーするルールに隣接するチェックボックスをオンにします。
3. ［**コピー**］をクリックします。
4. 表示されるウィンドウで、必要に応じて［**全般**］タブで次の情報を変更します。ただし、設定を変更せずにルールのコピーのみを行う場合は、設定を変更する必要はありません：

- **ルール名**

  新しいルールの名前を入力します。

  ルールのコピー時には、新しいルールでは、元のルールと同じ名前に「(1)」のようなインデックス「(数字)」が追加されます。

- **管理グループ**

  デバイスを自動的に移動する移動先の管理グループを選択します。

- **アクティブなルール**

  このオプションをオンにすると、ルールの保存後にルールが有効になり適用されます。

  このオプションをオフにすると、ルールは作成されますがオフの状態です。このオプションをオンにするまで、ルールは適用されません。

- **どの管理グループにも属していないデバイスのみ移動する**

  このオプションをオンにすると、未割り当てデバイスのみが選択したグループに移動します。

  このオプションをオフにすると、既に管理グループに割り当てられているデバイスと未割り当てデバイスの両方が選択したグループに移動します。

- **ルールの適用**

  次の中からいずれかを選択できます：

  - **各デバイスにつき1回**

    指定した条件に合致するデバイスで各デバイスにつき1回だけルールが適用されます。

  - **各デバイスで1度実行、以降はネットワークエージェントの再インストールごとに実行**

    指定した条件に合致するデバイスで各デバイスにつき1回ルールが適用され、その後はデバイスにネットワークエージェントが再インストールされた場合にのみ適用されます。

  - **ルールを永続的に適用**

    管理サーバーで自動的に設定されるスケジュールに従ってルールが適用されます（通常は数時間ごと）。

5. ［**ルールの条件**］タブで、自動的に移動するデバイスの基準を少なくとも1つ指定します。
6. ［**保存**］をクリックします。

新しい移動ルールが作成されます。新しいルールが移動ルールのリストに表示されます。

デバイス移動ルールの条件

クライアントデバイスを管理グループに移動するルールを作成またはコピーする場合、［**ルールの条件**］タブで、デバイスを移動するための条件を設定します。次の基準に従って、移動するデバイスを決定できます：

- クライアントデバイスに割り当てられたタグ。
- ネットワークパラメータ。たとえば、指定した範囲の IP アドレスを持つデバイスを移動することができます。
- ネットワークエージェントや管理サーバーなど、クライアントデバイスにインストールされた管理対象アプリケーション。
- クライアントデバイスである仮想マシン。
- クライアントデバイスを含む Active Directory 組織単位（OU）に関する情報。
- クライアントデバイスを含むクラウドセグメントに関する情報。

以下では、デバイス移動ルールにこの情報を指定する方法について説明します。

ルールに複数の条件を指定すると、AND 論理演算子が機能し、すべての条件が同時に適用されます。オプションを何も選択しない場合や、一部のフィールドを空白のままにした場合には、そのような条件は適用されません。

［タグ］タブ

このタブでは、クライアントデバイスの説明に追加済みのデバイスタグに基づいてデバイス移動ルールを設定できます。このためには、必要なタグを選択します。また、次のオプションをオンにすることもできます：

- **指定したタグのないデバイスに適用する**

  このオプションをオンにすると、指定したタグを持つすべてのデバイスがデバイス移動ルールから除外されます。このオプションをオフにすると、選択したすべてのタグを持つデバイスにデバイス移動ルールが適用されます。

  既定では、このオプションはオフです。

- **少なくとも 1 個のタグが一致する場合に適用する**

  このオプションをオンにすると、選択したタグを少なくとも 1 個持つクライアントデバイスにデバイス移動ルールが適用されます。このオプションをオフにすると、選択したすべてのタグを持つデバイスにデバイス移動ルールが適用されます。

  既定では、このオプションはオフです。

［ネットワーク］タブ

このタブでは、デバイス移動ルールで考慮するデバイスのネットワークデータを指定できます：

- **Windows ネットワーク上のデバイス名**

  デバイスの Windows ネットワーク名（NetBIOS 名）、あるいは IPv4 アドレスまたは IPv6 アドレス。

- **Windows ドメイン**

デバイス移動ルールは、指定された Windows ドメインに含まれるすべてのデバイスに適用されます。

- **デバイスの DNS 名**

  移動するクライアントデバイスの DNS ドメイン名。ネットワークに DNS サーバーが含まれている場合は、このフィールドに入力します。

  Kaspersky Security Center で使用するデータベースに大文字と小文字を区別する照合が設定されている場合は、デバイスの DNS 名の指定時に大文字と小文字を区別してください。そうしないと、デバイス移動ルールは機能しません。

- **DNS ドメイン**

  デバイス移動ルールは、指定されたメイン DNS サフィックスに含まれるすべてのデバイスに適用されます。ネットワークに DNS サーバーが含まれている場合は、このフィールドに入力します。

- **IP アドレス範囲**

  このオプションをオンにすると、検索されるデバイスが属する IP アドレス範囲の最初と最後の IP アドレスを入力できます。

  既定では、このオプションはオフです。

- **管理サーバー接続用 IP アドレス**

  このオプションを有効にすると、クライアントデバイスを管理サーバーに接続するための IP アドレスを設定できます。これを行うには、必要なすべての IP アドレスが含まれる IP 範囲を指定します。

  既定では、このオプションはオフです。

- **接続プロファイルが変更されました**

  次のいずれかの値を選択します：

  - **はい**デバイス移動ルールは、接続プロファイルが変更されたクライアントデバイスにのみ適用されます。
  - ［**いいえ**］。デバイス移動ルールは、接続プロファイルが変更されていないクライアントデバイスにのみ適用されます。
  - **値を選択しない**：条件は当てはまりません。

- **別の管理サーバーの管理対象**

次のいずれかの値を選択します：

- **はい**：デバイス移動ルールは、他の管理サーバーによって管理されているクライアントデバイスにのみ適用されます。これらのサーバーは、デバイス移動ルールを設定するサーバーとは異なります。
- ［**いいえ**］。デバイス移動ルールは、現在の管理サーバーによって管理されているクライアントデバイスにのみ適用されます。
- **値を選択しない**：条件は当てはまりません。

［アプリケーション］タブ

このタブでは、クライアントデバイスにインストールされている管理対象アプリケーションとオペレーティングシステムに基づいてデバイス移動ルールを設定できます：

- **ネットワークエージェントがインストール済み**

  次のいずれかの値を選択します：
  - **はい**デバイス移動ルールは、ネットワークエージェントがインストールされたクライアントデバイスにのみ適用されます。
  - ［**いいえ**］。デバイス移動ルールは、ネットワークエージェントがインストールされていないクライアントデバイスにのみ適用されます。
  - **値を選択しない**：条件は当てはまりません。

- **アプリケーション**

  クライアントデバイスにインストールされている必要がある管理対象アプリケーションを指定して、デバイス移動ルールがこれらのデバイスに適用されるようにします。たとえば、**Kaspersky Security Center 15.1 ネットワークエージェント** や **Kaspersky Security Center 15.1 管理サーバー** を選択できます。

  管理対象アプリケーションを選択しない場合、条件は適用されません。

- **OS のバージョン**

  オペレーティングシステムのバージョンに基づいてクライアントデバイスを選別できます。この目的のために、クライアントデバイスにインストールされている必要があるオペレーティングシステムを指定します。その結果、選択したオペレーティングシステムがインストールされたクライアントデバイスにデバイス移動ルールが適用されます。

  このオプションを有効にしない場合、条件は適用されません。既定では、このオプションはオフです。

- **OS のビット数**

オペレーティングシステムのビットサイズによってクライアントデバイスを選別できます。［**OS のビット数**］フィールドで、次のいずれかの値を選択できます：

- **不明**
- **x86**
- **AMD64**
- **IA64**

クライアントデバイスのオペレーティングシステムのビットサイズを確認するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］セクションの順に選択します。
2. 右側にある［**列の設定**］（）をクリックします。
3. ［**OS のビット数**］オプションを選択し、［**保存**］ボタンをクリックします。
   その後、管理対象デバイスごとにオペレーティングシステムのビットサイズが表示されます。

- **OS サービスパックのバージョン**

このフィールドでは、オペレーティングシステムのパッケージバージョンを「*X.Y*」形式で指定できます。これによって、デバイスに対する移動ルールの適用方法が決定されます。既定では、バージョンの値は指定されていません。

- **ユーザー証明書**

次のいずれかの値を選択します：

- **インストール**：デバイス移動ルールは、モバイル証明書を持つモバイルデバイスにのみ適用されます。
- **未インストール**：デバイス移動ルールは、モバイル証明書のないモバイルデバイスにのみ適用されます。
- **値を選択しない**：条件は当てはまりません。

- **OS のビルド**

この設定は Windows オペレーティングシステムにのみ適用できます。

選択したオペレーティングシステムのビルド番号が、入力したビルド番号と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したビルド番号を除くすべてのビルド番号に対してデバイス移動ルールを設定することもできます。

- **OS のリリース番号**

この設定は Windows オペレーティングシステムにのみ適用できます。

選択したオペレーティングシステムのリリース ID が、入力したリリース番号と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したリリース番号を除くすべてのリリース番号に対してデバイス移動ルールを設定することもできます。

［仮想マシン］タブ

このタブでは、クライアントデバイスが仮想マシンであるか仮想デスクトップインフラストラクチャ（VDI）の一部であるかに応じて、デバイス移動ルールを設定できます：

- **仮想マシン**

  このドロップダウンリストで、次のいずれかのオプションを選択できます：
  - **該当なし**：条件は当てはまりません。
  - ［**いいえ**］。仮想マシンでないデバイスを移動します。
  - **はい**仮想マシンであるデバイスを移動します。

- **仮想マシンの種別**

- **仮想デスクトップインフラストラクチャの一部**

  このドロップダウンリストで、次のいずれかのオプションを選択できます：
  - **該当なし**：条件は当てはまりません。
  - ［**いいえ**］。VDI の一部ではないデバイスを移動します。
  - **はい**VDI を構成するデバイスを移動します。

［ドメインコントローラー］タブ

このタブでは、ドメイン組織単位に含まれるデバイスを移動する必要があることを指定できます。指定したドメイン組織単位のすべての子組織単位からデバイスを移動することもできます：

- **デバイスが含まれている次の組織単位**

  このオプションをオンにすると、デバイス移動ルールは、オプションの下のリストで指定されたドメイン組織ユニットのデバイスに適用されます。

  既定では、このオプションはオフです。

- **子組織単位を含める**

このオプションをオンにすると、抽出には、指定したドメイン組織単位のすべての子組織単位（OU）のデバイスが含まれます。

既定では、このオプションはオフです。

- **子組織単位のデバイスを対応するサブグループへ移動する**
- **新しく検出されたデバイスの配置階層に対応するサブグループを作成する**
- **ドメインに存在しないサブグループを削除する**
- **デバイスが含まれている次のドメインセキュリティグループ**

  このオプションをオンにすると、デバイス移動ルールは、オプションの下のリストで指定されたドメインセキュリティグループのデバイスに適用されます。

  既定では、このオプションはオフです。

［クラウドセグメント］タブ

このタブでは、指定されたクラウドセグメントに属するデバイスを移動する必要があることを指定できます：

- **デバイスがクラウドセグメント内にある**

  このオプションをオンにすると、クラウドセグメントに属するクライアントデバイスにデバイス移動ルールが適用されます。オプションの下のリストで、必要なクラウドセグメントをサブネットまで選択できます。

  既定では、このオプションはオフです。

- **子オブジェクトも含む**

  このオプションをオンにすると、選択したクラウドセグメントだけでなく、このセグメントの子オブジェクトにもデバイス移動ルールが適用されます。

  既定では、このオプションはオフです。

- **デバイスをネストされたオブジェクトから対応するサブグループに移動する**
- **新しく検出されたデバイスの配置階層に対応するサブグループを作成する**
- **クラウドセグメントで何も検出されなかったサブグループを削除する**
- **API を使用して検出されたデバイス**

ドロップダウンリストで、API ツールによりデバイスが検出されるかどうかを選択できます：

- **AWS**：AWS API を使用して検出されたデバイスで、これはデバイスが間違いなく AWS クラウド環境にあることを意味します。
- **Azure**：Azure API を使用して検出されたデバイスで、これはデバイスが間違いなく Azure クラウド環境にあることを意味します。
- **Google Cloud**：Google API を使用して検出されたデバイスで、これはデバイスが間違いなく Google Cloud 環境にあることを意味します。
- ［**いいえ**］。デバイスは AWS API、Azure API、Google API のいずれでも検出できません。これはデバイスがクラウド環境外にあるか、クラウド環境内にあるが API では検出できないことを意味します。
- **値なし**：この条件は当てはまりません。

クラスターとサーバーアレイについて

Kaspersky Security Center はクラスターテクノロジーをサポートします。クライアントデバイスにインストールされたアプリケーションがサーバーアレイの一部であることを確認する情報が、ネットワークエージェントから管理サーバーに送信されると、このクライアントデバイスはクラスターノードになります。

管理グループにクラスターまたはサーバーアレイが含まれている場合、［**管理対象デバイス**］ページには 2 つのタブが表示されます。1つは個々のデバイス用で、もう1つはクラスターおよびサーバーアレイ用です。管理対象デバイスがクラスターノードとして検出されると、クラスターは個別のオブジェクトとして［**クラスターとサーバーアレイ**］タブに追加されます。

クラスターまたはサーバーアレイノードは、他の管理対象デバイスとともに［**デバイス**］タブに一覧表示されます。個別のデバイスとしてノードのプロパティを表示したり、他の操作を実行したりできますが、クラスターノードを削除したり、そのクラスターとは別に他の管理グループに移動したりすることはできません。クラスター全体の削除または移動のみが可能です。

クラスターまたはサーバーアレイで実行できる操作は次の通りです：

- プロパティを表示する
- クラスターまたはサーバーアレイを別の管理グループに移動する

  クラスターまたはサーバーアレイを別のグループに移動すると、そのすべてのノードも一緒に移動します。これは、クラスターとそのノードのいずれかが常に同じ管理グループに属しているためです。

- 削除

  クラスターまたはサーバーアレイの削除は、クラスターまたはサーバーアレイが組織のネットワークに存在しなくなった場合にのみ行うことを推奨します。クラスターがまだネットワーク上に表示され、ネットワークエージェントとカスペルスキーセキュリティ製品がまだクラスターノードにインストールされている場合、Kaspersky Security Center は、削除されたクラスターとそのノードを管理対象デバイスのリストに自動的に戻します。

クラスターまたはサーバーアレイのプロパティ

クラスターまたはサーバーアレイの設定を表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］→［**クラスターとサーバーアレイ**］の順に移動します。

   クラスターとサーバーアレイのリストが表示されます。

2. 必要なクラスターまたはサーバーアレイの名前をクリックします。

選択したクラスターまたはサーバーアレイのプロパティウィンドウが表示されます。

全般

［**全般**］セクションには、クラスターまたはサーバーアレイに関する一般情報が表示されます。情報は、管理サーバーでクラスターノードの前回の同期中に受信されたデータに基づいて提供されます。

- **名前**
- **説明**
- **Windows ドメイン**

  クラスターまたはサーバーアレイを含む Windows ドメインまたはワークグループ。

- **NetBIOS 名**

  クラスターまたはサーバーアレイの Windows ネットワーク名。

- **DNS 名**

  クラスターまたはサーバーアレイの DNS ドメインの名前。

タスク

［**タスク**］タブでは、既存タスクのリストの表示、新規タスクの作成、タスクの削除、開始、停止、タスク設定の変更、実行結果の表示など、クラスターまたはサーバーアレイに割り当てられたタスクを管理できます。リストされているタスクは、クラスターノードにインストールされているカスペルスキーセキュリティ製品に関連するものです。Kaspersky Security Center は、クラスターノードからタスクリストとタスクステータスの詳細を受け取ります。接続に失敗すると、ステータスは表示されません。

ノード

このタブには、クラスターまたはサーバーアレイに含まれるノードのリストが表示されます。ノード名をクリックすると、デバイスのプロパティウィンドウが表示されます。

カスペルスキー製品

プロパティウィンドウには、クラスターノードにインストールされているカスペルスキーセキュリティ製品に関連する情報と設定を含む追加のタブが含まれている場合もあります。

デバイスが不可視の時の処理の表示と設定

グループ内のクライアントデバイスがアクティブでない場合、通知を受け取ることができます。こうしたデバイスを自動的に削除することもできます。

グループ内のデバイスがアクティブでない場合の処理を表示したり設定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. 目的の管理グループの名前をクリックします。
   管理グループのプロパティウィンドウが開きます。
3. プロパティウィンドウで［**設定**］タブに移動します。
4. ［**継承**］セクションで、次のオプションの有効と無効を切り替えます：

   - **親グループから継承する**

     クライアントデバイスが属する親グループからこのセクションの設定が継承されます。このオプションをオンにすると、［**ネットワーク上のデバイスのアクティビティ**］の設定がロックされ変更できなくなります。

     このオプションは管理グループに親グループが存在する場合にのみ利用できます。

     既定では、このオプションはオンです。

   - **設定を子グループへ強制的に継承させる**

     設定値が子グループに配信され、子グループのプロパティではそれらの設定がロックされます。

     既定では、このオプションはオフです。

5. ［**デバイスのアクティビティ**］セクションで、次のオプションの有効と無効を切り替えます：

   - **次の期間デバイスが不可視の場合管理者に通知（日）**

     このオプションをオンにすると、管理者が非アクティブなデバイスについて通知を受け取ります。［**デバイスがネットワーク上で長期間アクティブになっていません**］イベントが作成されるまでの期間を指定できます。既定の期間は 7 日です。

     既定では、このオプションはオンです。

   - **次の期間デバイスが不可視の場合グループから削除（日）**

     このオプションをオンにすると、デバイスをグループから自動的に削除するまでの期間を指定できます。既定の期間は 60 日です。

     既定では、このオプションはオンです。

6. ［**保存**］をクリックします。

変更内容が保存され、適用されます。

デバイスのステータスの概要

Kaspersky Security Center は、各管理対象デバイスにステータスを割り当てます。特定のステータスは、ユーザーが定義した条件を満たしているかどうかによって異なります。場合によっては、デバイスにステータスを割り当てるときに、Kaspersky Security Center はネットワーク内のデバイスの可視性フラグを考慮します（下の表を参照）。Kaspersky Security Center が 2 時間以内にネットワーク内のデバイスを見つけられない場合、デバイスの可視性フラグは「*不可視*」に設定されます。

ステータスは次の通りです：

- *緊急*または*緊急 / 可視*
- *警告*または*警告 / 可視*
- *OK* または *OK / 可視*

次の表では、「*緊急*」または「*警告*」ステータスをデバイスに割り当てるために満たすべき既定の条件を、可能なすべての値とともに一覧で表示します。

デバイスにステータスを割り当てる条件

条件	条件の説明	設定可能な値
セキュリティ製品がインストールされていません	デバイスにネットワークエージェントはインストールされていますが、セキュリティ製品はインストールされていません。	• 切り替えスイッチをオン • 切り替えスイッチをオフ
ウイルスが多数検知されました	*マルウェアスキャン*タスクなどのウイルス検知タスクによりデバイスでウイルスが検知され、検知数が指定された値を超えました。	0 より大きい値
リアルタイム保護レベルが管理者の設定と異なります	デバイスはネットワーク上で可視ですが、リアルタイム保護レベルがデバイスのステータスの条件として管理者によって設定されたレベルと異なっています。	• 停止 • 一時停止 • 実行中
マルウェアスキャンが長期間実行されていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、*マルウェアのスキャン*タスクもローカルスキャンタスクも実行されていない状態が指定期間を越えて続いています。この条件は、7 日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。	1 日より大きい値
定義データベースがアップデートされていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、このデバイスで定義データベースがアップデートされていない状態が指定期間を越えて続いています。この条件は、1 日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。	1 日より大きい値
長期間接続されていません	デバイスにネットワークエージェントはインストールされていますが、デバイスがオフになっており、デバイスが管理サーバーに接続されていない状態が指定期間を越えて続いています。	1 日より大きい値
アクティブな脅威を検知しました	［**アクティブな脅威**］フォルダー内の未処理オブジェクトの数が指定の値を上回っています。	0 項目より大きい値
再起動が必要です	デバイスはネットワーク上で可視ですが、アプリケーションが選択した理由でデバイスの再起動を必要とする状態が指定期間を越えて続いています。	0 分より大きい値
競合アプリケーションがインストールされています	デバイスはネットワーク上で可視ですが、ネットワークエージェントから実行されたソフトウェアインベントリにより、競合するアプリケーションがデバイスにインストールされていることを検知しました。	• 切り替えスイッチをオフ • 切り替えスイッチをオン

ソフトウェアの脆弱性が検知されました	デバイスはネットワーク上で可視でネットワークエージェントもインストールされていますが、*脆弱性とアプリケーションのアップデートの検索*タスクが、デバイスにインストールされているアプリケーションで指定された重要度の脆弱性を検知しました。	• 緊急 • 高 • 中 • 脆弱性を修正できない場合は無視する • 修正プログラムがインストール用に割り当てられている場合は無視する
ライセンスの有効期間が終了しました	デバイスはネットワーク上で可視ですが、ライセンスの有効期間が終了しています。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
ライセンスの有効期間がまもなく終了します	デバイスはネットワーク上で可視ですが、ライセンスの有効期間の残り日数が指定した期間以下しかありません。	0 日より大きい値
Windows Update 更新プログラムのチェックが長期間実行されていません	デバイスはネットワーク上で可視ですが、*Windows Update の同期の実行*タスクが実行されていない状態が指定期間を越えて続いています。	1 日より大きい値
暗号化ステータスが無効です	デバイスにネットワークエージェントはインストールされていますが、デバイスの暗号化結果が割り当て条件として指定されているものと合致しました。	• ユーザーが拒否したため、ポリシーに準拠していない（外部デバイスのみ）。 • エラーにより、ポリシーに準拠していない。 • ポリシーを適用したら再起動する必要がある。 • 暗号化ポリシーが指定されていない。 • サポートされていない。 • ポリシーを適用するとき。
モバイルデバイスの設定がポリシーに適合していません	コンプライアンスルールをチェックしたところ、モバイルデバイスの設定が Kaspersky Endpoint Security for Android ポリシーで指定された設定と異なります。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
未処理のセキュリティ問題が検出されました	未処理のセキュリティ問題がデバイス上でいくつか見つかりました。セキュリティ問題は、クライアントデバイスにインストールしたカスペルスキー製品によって自動で作成されるか、管理者が手動で作成します。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
製品が定義したデバイスのステータ	デバイスのステータスが管理対象アプリケーションによって定義されています。	• 切り替えスイッチをオフ

ス		• 切り替えスイッチをオン
デバイスに空き容量がありません	デバイスの空き容量が指定された値未満またはデバイスと管理サーバーを同期できませんでした。デバイスが管理サーバーと正常に同期されなおかつデバイスの空き容量が指定値以上になった場合、ステータスが［*緊急*］または［*警告*］から［*OK*］に変更されます。	0 MB より大きい値。
デバイスが管理対象外になりました	デバイスの検索中、デバイスはネットワークで認識されましたが、管理サーバーとの同期に 3 回以上失敗しました。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
プロテクションが無効です	デバイスはネットワーク上で可視ですが、デバイス上でセキュリティ製品が無効になっている状態が指定期間を越えて続いています。 この場合、セキュリティ製品の状態は*停止中*または*エラー*となり、*開始中*、*実行中*、*中断中*とは異なります。	0 分より大きい値
セキュリティ製品が実行されていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、セキュリティ製品が実行されていません。	• 切り替えスイッチをオフ • 切り替えスイッチをオン

Kaspersky Security Center では、指定した条件が満たされると、管理グループのデバイスのステータスが自動的に切り替わるように設定できます。指定した条件が満たされると、クライアントデバイスには、「*緊急*」または「*警告*」のステータスのいずれかが割り当てられます。指定した条件を満たしていない場合、クライアントデバイスには「*OK*」ステータスが割り当てられます。

1 つの条件の複数の値に対して異なるステータスを対応させることができます。たとえば、［**定義データベースがアップデートされていません**］条件の値が「**3 日より大きい値**」の場合はクライアントデバイスに「*警告*」ステータスが割り当てられ、条件値が「**7 日より大きい値**」の場合は「*緊急*」ステータスが割り当てられます。

Kaspersky Security Center を以前のバージョンからアップグレードしても、ステータスを「*緊急*」または「*警告*」に割り当てるための［**定義データベースがアップデートされていません**］条件の値は変更されません。

Kaspersky Security Center によってデバイスにステータスが割り当てられると、一部の条件（条件説明の列を参照）で可視性フラグが考慮されます。たとえば、ある管理対象デバイスは［定義データベースがアップデートされていません］条件を満たしていたために「*緊急*」ステータスが割り当てられました。のちにデバイスには可視性フラグが設定され、その後、そのデバイスは「*OK*」ステータスが割り当てられます。

デバイスのステータスの切り替えの設定

デバイスに「*緊急*」または「*警告*」ステータスを割り当てる条件を変更できます。

デバイスのステータスの「緊急」への切り替えを有効にするには：

1. 次のいずれかの方法で、プロパティウィンドウを開きます：
   - ［**ポリシー**］フォルダーの管理サーバーポリシーのコンテキストメニューで［**プロパティ**］を選択します。
   - 管理グループのコンテキストメニューで［**プロパティ**］を選択します。

2. **プロパティ**ウィンドウが表示されたら、［**セクション**］ペインで［**デバイスのステータス**］を選択します。

3. 右側の［**ステータスを「緊急」にする条件**］セクションで、リスト内の各条件に隣接するチェックボックスをオンにします。

   親ポリシーでロック状態になっていない設定のみ変更できます。

4. 選択した条件に対して適切な値を設定します。
   一部の条件では値を指定できますが、値を指定できない条件もあります。

5. ［OK］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*緊急*」ステータスが割り当てられます。

デバイスのステータスの「警告」への切り替えを有効にするには：

1. 次のいずれかの方法で、プロパティウィンドウを開きます：

   - ［**ポリシー**］フォルダーの管理サーバーポリシーのコンテキストメニューで［**プロパティ**］を選択します。
   - 管理グループのコンテキストメニューで［**プロパティ**］を選択します。

2. **プロパティ**ウィンドウが表示されたら、［**セクション**］ペインで［**デバイスのステータス**］を選択します。

3. 右側の［**ステータスを「警告」にする条件**］セクションで、リスト内の各条件に隣接するチェックボックスをオンにします。

   親ポリシーでロック状態になっていない設定のみ変更できます。

4. 選択した条件に対して適切な値を設定します。
   一部の条件では値を指定できますが、値を指定できない条件もあります。

5. ［OK］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*警告*」ステータスが割り当てられます。

クライアントデバイスのデスクトップへのリモート接続

管理者は、デバイスにインストールされているネットワークエージェントを使用して、クライアントデバイスのデスクトップへのリモートアクセスを取得できます。ネットワークエージェントを使用したデバイスへのリモート接続は、クライアントデバイスの TCP ポートと UDP ポートが閉じている場合でも可能です。

デバイスとの接続を確立すると、管理者はそのデバイスに保存されている情報へのフルアクセス権を取得できます。そのため、そのデバイスにインストールされているアプリケーションを管理することが可能です。

対象の管理対象デバイスのオペレーティングシステム設定でリモート接続を許可する必要があります。たとえば、Windows 10 の場合、このオプションの名前は［**このコンピューターへのリモートアシスタンスの接続を許可する**］です（このオプションを表示するには、［**コントロールパネル**］-［**システムとセキュリティ**］-［**システム**］-［**リモートの設定**］の順に選択します）。脆弱性とパッチ管理機能のライセンスがある場合は、管理対象デバイスへの接続を確立した時に、このオプションを強制的にオンにできます。ライセンスがない場合は、対象の管理対象デバイス上でローカルでオンにします。このオプションをオフにすると、リモート接続を実行できません。

デバイスへのリモート接続を確立するには、2 個のユーティリティが必要です：

- カスペルスキーのユーティリティ klsctunnel：このユーティリティは管理者のワークステーションに保管されている必要があります。このユーティリティは、クライアントデバイスと管理サーバー間の接続のトンネリングに使用します。

  Kaspersky Security Center では、管理コンソールから管理サーバーを経由し、次にネットワークエージェントを経由して、管理対象デバイスの指定されたポートに到達する TCP 接続のトンネリングが可能です。トンネリングは、管理コンソールと管理対象デバイスを直接接続できない場合に、管理コンソールがインストールされたデバイスのクライアントアプリケーションを、管理対象デバイスの TCP ポートに接続するように設計されています。

  クライアントデバイスと管理サーバー間のトンネリング接続は、管理サーバーへの接続に使用するポートがデバイスで使用できない場合に必要です。デバイスのポートは、次の場合に利用できないことがあります：

  - リモートデバイスが NAT を使用するローカルネットワークに接続されている。
  - リモートデバイスが管理サーバーのローカルネットワークの一部であるが、ファイアウォールによりポートが閉じられている。

- リモートデスクトップ接続（Microsoft Windows 標準コンポーネント）。リモートデスクトップへの接続は、ユーティリティの設定に従い、Windows の標準のユーティリティ mstsc.exe を使用して確立されます。

  ユーザーの現在のリモートデスクトップのセッションへの接続は、ユーザーが認識することなく確立されます。管理者がセッションに接続すると、デバイスのユーザーは、事前の通知なくセッションから切断されます。

クライアントデバイスのデスクトップに接続するには：

1. 管理サーバーのコンテキストメニューにある MMC ベースの管理コンソールから［**プロパティ**］を選択します。
2. 表示された管理サーバーのプロパティウィンドウで、［**管理サーバー接続設定**］→［**接続ポート**］の順に選択します。
3. ［**Kaspersky Security Center Web コンソール用に RDP ポートを開く**］がオンになっていることを確認します。
4. Kaspersky Security Center Web コンソールで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
5. 管理対象デバイスのリストの上にある［**現在のパス**］フィールドで、パスリンクをクリックします。
6. 開いた左側のペインで、アクセスするデバイスを含む管理グループを選択します。
7. アクセスを取得するデバイスの名前の横にあるチェックボックスをオンにします。
8. ［**リモートデスクトップに接続**］をクリックします。

   ［リモートデスクトップ（Windows のみ）］ウィンドウが表示されます。

9. ［**管理対象デバイス上でリモートデスクトップ接続を許可する**］をオンにします。この場合、リモート接続が現時点で管理対象デバイスのオペレーティングシステム設定で禁止されていても、接続は確立されます。

脆弱性とパッチ管理機能のライセンスがないと、このオプションは使用できません。

10. ［**ダウンロード**］をクリックして、klsctunnel ユーティリティをダウンロードします。

11. ［**クリップボードへコピー**］をクリックして、テキストフィールドからテキストをコピーします。このテキストは、管理サーバーと管理対象デバイス間の接続を確立するために必要な設定を含む、バイナリラージオブジェクト（BLOB）です。

BLOB は 3 分間有効です。BLOB の有効期限が切れた場合は、［リモートデスクトップ（Windows のみ）］ウィンドウを再び開いて新しい BLOB を生成します。

12. klsctunnel ユーティリティを実行します。

ユーティリティウィンドウが開きます。

13. コピーしたテキストをテキストフィールドに貼り付けます。

14. プロキシサーバーを使用する場合は、［**プロキシサーバーを使用する**］をオンにして、プロキシサーバーの接続設定を指定します。

15. ［**ポートを開く**］をクリックします。

リモートデスクトップ接続のログインウィンドウが開きます。

16. Kaspersky Security Center Web コンソールに現在ログインしているアカウントの資格情報を指定します。

17. ［**接続**］をクリックします。

デバイスへの接続が確立されると、Microsoft Windows のリモートデスクトップ接続ウィンドウにデスクトップが表示されます。

Windows デスクトップ共有によるデバイスへの接続

管理者は、デバイスにインストールされているネットワークエージェントを使用して、クライアントデバイスのデスクトップへのリモートアクセスを取得できます。ネットワークエージェントを使用したデバイスへのリモート接続は、クライアントデバイスの TCP ポートと UDP ポートが閉じている場合でも可能です。

管理者は、このセッションのユーザーを切断することなく、クライアントデバイスでの既存のセッションに接続することができます。この場合、管理者とデバイスのセッションユーザーが、デスクトップのアクセスを共有します。

デバイスへのリモート接続を確立するには、2 個のユーティリティが必要です：

- カスペルスキーのユーティリティ klsctunnel：このユーティリティは管理者のワークステーションに保管されている必要があります。このユーティリティは、クライアントデバイスと管理サーバー間の接続のトンネリングに使用します。

Kaspersky Security Center では、管理コンソールから管理サーバーを経由し、次にネットワークエージェントを経由して、管理対象デバイスの指定されたポートに到達する TCP 接続のトンネリングが可能です。トンネリングは、管理コンソールと管理対象デバイスを直接接続できない場合に、管理コンソールがインストールされたデバイスのクライアントアプリケーションを、管理対象デバイスの TCP ポートに接続するように設計されています。

クライアントデバイスと管理サーバー間のトンネリング接続は、管理サーバーへの接続に使用するポートがデバイスで使用できない場合に必要です。デバイスのポートは、次の場合に利用できないことがあります：

- リモートデバイスが NAT を使用するローカルネットワークに接続されている。
- リモートデバイスが管理サーバーのローカルネットワークの一部であるが、ファイアウォールによりポートが閉じられている。

- Windows デスクトップ共有：リモートデスクトップの既存のセッションに接続する場合、デバイスのセッションユーザーは管理者から接続要求を受信します。デバイスのリモートからの動作とその結果に関する情報は、Kaspersky Security Center により作成されるレポートに保存されません。

  管理者はリモートクライアントデバイスでのユーザー操作の監査を設定できます。監査中に、管理者が開いている（または変更している）クライアントデバイスのファイルの情報が保存されます。

Windows デスクトップ共有を使用してクライアントデバイスのデスクトップに接続するには、次の条件を満たす必要があります：

- Microsoft Windows Vista 以降の Windows オペレーティングシステムが管理ステーションにインストールされている。管理サーバーをホストしているデバイスのオペレーティングシステムの種別により、Windows デスクトップ共有を使用した接続に制限が適用されることはありません。

  使用する Windows のエディションに Windows デスクトップ共有機能が含まれているかどうかを確認するには、Windows レジストリに CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} キーがあることを確認します。

- Microsoft Windows Vista 以降の Windows オペレーティングシステムがクライアントデバイスにインストールされている。

- Kaspersky Security Center が、脆弱性とパッチ管理ライセンスを使用している。

Windows デスクトップ共有を使用してクライアントデバイスのデスクトップに接続するには：

1. 管理サーバーのコンテキストメニューにある MMC ベースの管理コンソールから［**プロパティ**］を選択します。
2. 表示された管理サーバーのプロパティウィンドウで、［**管理サーバー接続設定**］→［**接続ポート**］の順に選択します。
3. ［**Kaspersky Security Center Web コンソール用に RDP ポートを開く**］がオンになっていることを確認します。
4. Kaspersky Security Center Web コンソールで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
5. 管理対象デバイスのリストの上にある［**現在のパス**］フィールドで、パスリンクをクリックします。
6. 開いた左側のペインで、アクセスするデバイスを含む管理グループを選択します。
7. アクセスを取得するデバイスの名前の横にあるチェックボックスをオンにします。
8. ［**Windows デスクトップ共有**］をクリックします。

Windows デスクトップ共有ウィザードが表示されます。

9. ［**ダウンロード**］をクリックして klsctunnel ユーティティをダウンロードし、ダウンロードプロセスが完了するまで待ちます。

   klsctunnel ユーティリティがある場合は、このステップをスキップします。

10. ［**次へ**］をクリックします。

11. 接続するデバイス上のセッションを選択するには、［**次へ**］をクリックします。

12. 対象デバイスで表示されるダイアログで、デスクトップ共有セッションをデバイスのユーザーが許可する必要があります。許可されない場合は、セッションを使用できません。

    デバイスのユーザーがデスクトップ共有セッションを確認すると、ウィザードの次のページが開きます。

13. ［**クリップボードへコピー**］をクリックして、テキストフィールドからテキストをコピーします。このテキストは、管理サーバーと管理対象デバイス間の接続を確立するために必要な設定を含む、バイナリラージオブジェクト（BLOB）です。

    BLOB は 3 分間有効です。有効期間が終了したら、新しい BLOB を生成してください。

14. klsctunnel ユーティリティを実行します。

    ユーティリティウィンドウが開きます。

15. コピーしたテキストをテキストフィールドに貼り付けます。

16. プロキシサーバーを使用する場合は、［**プロキシサーバーを使用する**］をオンにして、プロキシサーバーの接続設定を指定します。

17. ［**ポートを開く**］をクリックします。

デスクトップ共有が新しいウィンドウで開始されます。デバイスと対話する場合は、メニューアイコン（  ）をウィンドウの左上でクリックし、［**対話モード**］を選択します。

デバイスの抽出

*デバイスの抽出*は、特定の条件を指定してデバイスをフィルタリングできる機能です。デバイスの抽出を使用して、複数のデバイスを管理できます。たとえば、デバイスの抽出に含まれるデバイスのみを対象とするレポートを表示したり、デバイスの抽出に含まれるデバイスすべてを別のグループに移動したりできます。

Kaspersky Security Center では、様々な*定義済みの抽出*（例：**「緊急」ステータスのデバイス**、**プロテクションが無効です**、**アクティブな脅威を検知しました**）を使用できます。定義済みの抽出は削除できません。*ユーザー定義の抽出*を追加で作成し設定できます。

ユーザー定義の抽出では、抽出範囲を「すべてのデバイス」「管理対象デバイス」「未割り当てデバイス」から選択できます。抽出条件のパラメータを指定できます。デバイスの抽出では、異なるパラメータを指定した複数の抽出条件を作成できます。たとえば、2 つの条件を作成し、それぞれに異なる IP アドレス範囲を指定できます。複数の条件を指定した場合、デバイスの抽出はいずれかの条件に 1 つでも一致するデバイスを表示します。これに対して、1 つの条件内で複数のパラメータが指定されている場合、すべてのパラメータを満たすことが求められます。たとえば、1 つの条件内で IP アドレス範囲とインストールされている製品名の両方が指定されている場合、該当する製品がインストールされていてなおかつ IP アドレスが指定した範囲内のデバイスのみが表示されます。

デバイスの抽出からデバイスリストを表示

Kaspersky Security Center には、デバイスの抽出からデバイスのリストを表示できます。

デバイスの抽出からデバイスリストを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**デバイスの抽出**］、または［**検出と製品の導入**］→［**デバイスの抽出**］セクションの順に選択します。
2. 抽出リストで、デバイスの抽出の名前をクリックします。
   このページには、デバイスの抽出に含まれるデバイス関連情報のテーブルが表示されます。
3. デバイステーブルのデータは、次のようにしてグループ化およびフィルタリングできます：
   - 設定アイコン（ ）をクリックし、テーブルに表示する列を選択します。
   - フィルターアイコン（ ）をクリックしてから、呼び出したメニューでフィルター条件を指定して適用します。
     デバイスをフィルタリングしたテーブルが表示されます。

デバイスの抽出で1つまたは複数のデバイスを選択し、［**新規タスク**］をクリックして、これらのデバイスに適用されるタスクを作成できます。

デバイスの抽出で選択したデバイスを別の管理グループに移動するには、［**グループへ移動**］をクリックし、ターゲットの管理グループを選択します。

デバイスの抽出の作成

デバイスの抽出を作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**デバイスの抽出**］の順に移動します。
   デバイスの抽出のリストが表示されます。
2. ［**追加**］をクリックします。
   ［**デバイスの抽出の設定**］ウィンドウが表示されます。
3. 新しい抽出の名前を入力します。
4. デバイスの抽出に含めるデバイスを含むグループを指定します：
   - ［**デバイスの検索**］- 選択基準を満たし、［**管理対象デバイス**］または［**未割り当てデバイス**］グループに含まれるデバイスを検索します。
   - ［**管理対象デバイスの検索**］- 選択基準を満たし、［**管理対象デバイス**］グループに含まれるデバイスを検索します。
   - ［**未割り当てデバイスの検索**］- 選択基準を満たし、［**未割り当てデバイス**］グループに含まれるデバイスを検索します。

   ［**セカンダリ管理サーバーのデータを含める**］を有効にして、選択基準を満たし、セカンダリ管理サーバーによって管理されているデバイスを検索できるようにします。

5. ［**追加**］をクリックします。

6. 表示されたウィンドウで、この抽出に含めるデバイスが満たす必要のある条件を指定し、［**OK**］をクリックします。

7. ［**保存**］をクリックします。

デバイスの抽出が作成され、リストに追加されます。

デバイスの抽出の設定

デバイスの抽出を設定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**デバイスの抽出**］の順に移動します。
   デバイスの抽出のリストが表示されます。

2. 関連するユーザー定義のデバイス抽出を選択し、［**プロパティ**］をクリックします。
   ［**デバイスの抽出の設定**］ウィンドウが表示されます。

3. ［**全般**］タブで、［**新規の条件**］をクリックします。

4. この抽出に含めるデバイスが満たす必要のある条件を指定します。

5. ［**保存**］をクリックします。

設定が適用され保存されます。

以下に、デバイスを抽出に割り当てる条件について説明します。条件は論理演算子「OR」を使用して結合されます。抽出には、少なくとも1つの条件を満たすデバイスが含まれます。

全般

［**全般**］セクションでは、抽出条件の名前を変更したり、条件を反転させたりすることができます：

抽出の条件を反転させる

このオプションをオンにすると、指定した抽出条件の選択状態が反転します。指定した条件に合致しないすべてのデバイスが、抽出に含まれるようになります。

既定では、このオプションはオフです。

ネットワークインフラストラクチャ

［**ネットワーク**］サブセクションでは、ネットワークデータを基にデバイスを抽出に含める場合に使用する基準を指定できます：

- **デバイス名**

  デバイスの Windows ネットワーク名（NetBIOS 名）、あるいは IPv4 アドレスまたは IPv6 アドレス。

- **ドメイン**

  指定した Windows ドメインに含まれるデバイスをすべて表示します。

- **管理グループ**

  指定した管理グループに含まれるデバイスを表示します。

- **説明**

  デバイスのプロパティウィンドウ（［**全般**］セクションの［**説明**］）のテキスト。
  ［**説明**］で検索に使用する表現として、次の文字を使用できます：

  - 1つの単語：

    - ***** -文字数不定の任意の文字列を表します。

    例：

    Server または **Server's** などの単語を記述するには、**Server*** と入力します。

    - **?** -任意の1文字を表します。

    例：

    Window または **Windows** などの単語を記述するには、**Windo?** と入力します。
    アスタリスク（*****）または疑問符（**?**）は、クエリの先頭文字としては使用できません。

  - 複数の単語による検索：

    - スペース -指定した単語のいずれかがコメントに含まれているデバイスがすべて表示されます。

    例：

    Secondary または **Virtual** という単語が含まれている語句を検索する場合は、クエリに **Secondary Virtual** と入力します。

    - **+** -単語の前にプラス記号を付けると、すべての検索結果にその単語が含まれます。

    例：

    Secondary と **Virtual** の両方が含まれた語句を検索するには、クエリに **+Secondary+Virtual** と入力します。

    - **-** -単語の前にマイナス記号を付けると、すべての検索結果にその単語が含まれません。

    例：

    Secondary が含まれ、**Virtual** が含まれない語句を検索するには、クエリに **+Secondary-Virtual** と入力します。

    - **"<任意のテキスト>"** -引用符で囲まれたテキストを含むテキストが検索されます。

    例：

    Secondary Server という語句を検索する場合は、クエリに **"Secondary Server"** と入力します。

- **IP アドレス範囲**

  このオプションをオンにすると、検索されるデバイスが属する IP アドレス範囲の最初と最後の IP アドレスを入力できます。

  既定では、このオプションはオフです。

- **別の管理サーバーの管理対象**

  次のいずれかの値を選択します：

  - **はい**：デバイス移動ルールは、他の管理サーバーによって管理されているクライアントデバイスにのみ適用されます。これらのサーバーは、デバイス移動ルールを設定するサーバーとは異なります。
  - ［**いいえ**］。デバイス移動ルールは、現在の管理サーバーによって管理されているクライアントデバイスにのみ適用されます。
  - **値を選択しない**：条件は当てはまりません。

［**ドメインコントローラー**］サブセクションでは、ドメインメンバーシップに基づいてデバイスを選択範囲に含める基準を設定できます：

- **デバイスが配置されているドメイン組織単位**

  このオプションをオンにすると、入力フィールドで指定されたドメイン組織単位のデバイスが選択されます。

  既定では、このオプションはオフです。

- **デバイスが属しているドメインセキュリティグループ**

  このオプションをオンにすると、入力フィールドで指定されたドメインセキュリティグループのデバイスが選択されます。

  既定では、このオプションはオフです。

［**ネットワーク活動**］サブセクションでは、ネットワークアクティビティを基にデバイスを抽出に含める場合に使用する基準を指定できます：

- **ディストリビューションポイントとして動作**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：

  - **はい**：ディストリビューションポイントとして動作するデバイスが抽出に含まれます。
  - ［**いいえ**］。ディストリビューションポイントとして機能するデバイスが抽出に含まれません。
  - **値を選択しない**：基準は適用されません。

- **管理サーバーから切断しない**

検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：

- **有効**：［**管理サーバーから切断しない**］をオンにしたデバイスが抽出に含まれます。
- **無効**：［**管理サーバーから切断しない**］をオフにしたデバイスが抽出に含まれます。
- **値を選択しない**：基準は適用されません。

- **接続プロファイルが切り替えられました**

検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：

- **はい**：接続プロファイルを切り替えた結果として管理サーバーに接続されたデバイスが抽出に含まれます。
- ［**いいえ**］。接続プロファイルを切り替えた結果として管理サーバーに接続されたデバイスが抽出に含まれません。
- **値を選択しない**：基準は適用されません。

- **前回の管理サーバーへの接続**

このチェックボックスを使用して、管理サーバーに前回接続した日時によるデバイスの検索の基準を設定できます。

このチェックボックスをオンにすると、入力フィールドで、クライアントデバイスにインストールされたネットワークエージェントと管理サーバーとの間に前回接続が確立された日時の範囲を指定できます。指定された間隔内のデバイスが抽出に含まれます。

このチェックボックスをオフにすると、この基準は適用されません。

既定では、このチェックボックスはオフです。

- **ネットワークポーリングで検出された新規デバイス**

過去数日間のネットワークポーリングで検出された新規デバイスを検索します。

このオプションをオンにすると、［**検出期間（日）**］フィールドで指定した期間中のデバイスの検索で検出された新規デバイスのみが、抽出に含まれます。

このオプションをオフにすると、デバイスの検索で検出された新規デバイスがすべて抽出に含まれます。

既定では、このオプションはオフです。

- **デバイスが可視**

検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：

- **はい**：ネットワークで現在可視のデバイスを抽出に含めます。
- ［**いいえ**］。ネットワークで現在不可視のデバイスを抽出に含めます。
- **値を選択しない**：基準は適用されません。

［**クラウドセグメント**］サブセクションでは、それぞれのクラウドセグメントを基にデバイスを抽出に含めるための基準を設定できます：

- **デバイスがクラウドセグメント内にある**

  このオプションをオンにすると、AWS、Azure、Google クラウドセグメントからデバイスを選択できます。

  ［**子オブジェクトも含む**］オプションも有効にする場合は、選択したセグメントのすべての子オブジェクトに対して検索が実行されます。

  検索結果には、指定したセグメントのデバイスしか含まれません。

- **API を使用して検出されたデバイス**

  ドロップダウンリストで、API ツールによりデバイスが検出されるかどうかを選択できます：

  - **はい**：デバイスは、AWS、Azure、または Google API を使用して検出されます。
  - ［**いいえ**］。AWS、Azure、または Google API を使用してデバイスを検出できません。つまり、クラウド環境の外にあるか、クラウド環境内にあるデバイスは API で検出できません。
  - 値なし：この条件は当てはまりません。

デバイスのステータス

［**管理対象デバイスのステータス**］サブセクションでは、管理対象アプリケーションからのデバイスのステータスの説明を基にデバイスを抽出に含めるための基準を設定できます：

- **デバイスのステータス**

  ドロップダウンリストからデバイスのステータス（「*OK*」「*緊急*」「警告」）を選択します。

- **リアルタイム保護のステータス**

  リアルタイム保護のステータスを選択できるドロップダウンリスト。指定されたリアルタイム保護ステータスのデバイスが抽出に含まれます。

- **デバイスステータスの説明**

  このフィールドで、「*OK*」「*緊急*」「*警告*」のいずれかのステータスをデバイスに割り当てる条件に対応するチェックボックスをオンにできます。

［**管理対象アプリケーションのコンポーネントのステータス**］サブセクションでは、管理対象アプリケーションのコンポーネントのステータスを基にデバイスを抽出に含めるための基準を設定できます：

- **データ漏洩対策のステータス**

  データ漏洩対策のステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **コラボレーションサーバーの保護ステータス**

サーバーコラボレーションの保護ステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **メールサーバーの保護ステータス**

  メールサーバーの保護のステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **Endpoint Sensor ステータス**

  Endpoint Sensor のステータス（*不明*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

［**管理対象アプリケーションのステータスに影響がある問題**］サブセクションでは、管理対象アプリケーションで検知される可能性のある問題のリストを基にデバイスを抽出に含めるために使用する基準を設定できます：選択した問題のうち1つ以上の問題が存在するデバイスが抽出に含まれます複数のアプリケーションを対象とする問題については、同じ問題をすべてのアプリケーションのリストで自動的に選択するオプションがあります。

管理対象アプリケーションからのステータスの説明に対応するチェックボックスをオンにできます。これらのステータスが受信されると、デバイスが抽出に含まれます。複数のアプリケーションを対象とするステータスについては、同じステータスをすべてのアプリケーションのリストで自動的に選択するオプションがあります。

システムの詳細

［**オペレーティングシステム**］セクションでは、オペレーティングシステム種別を基にデバイスを抽出に含める場合に使用する基準を指定できます。

- **プラットフォームの種別**

  このチェックボックスをオンにすると、オペレーティングシステムをリストから選択できます。指定したオペレーティングシステムがインストールされたデバイスが検索結果に含まれます。

- **OS サービスパックのバージョン**

  このフィールドでは、オペレーティングシステムのパッケージバージョンを「*X.Y*」形式で指定できます。これによって、デバイスに対する移動ルールの適用方法が決定されます。既定では、バージョンの値は指定されていません。

- **OS のビット数**

  ドロップダウンリストで、オペレーティングシステムのアーキテクチャを選択できます。これによって、デバイスに対する移動ルールの適用方法が決定されます（［**不明**］、［**x86**］、［**AMD64**］、［**IA64**］）。既定では、リストでオプションが選択されていないため、オペレーティングシステムのアーキテクチャは定義されていません。

- **OS のビルド**

この設定は Windows オペレーティングシステムにのみ適用できます。

オペレーティングシステムのビルド番号です。選択したオペレーティングシステムのビルド番号が、入力したビルド番号と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したビルド番号を除くすべてのビルド番号を検索するようにも設定できます。

- **OS のリリース番号**

この設定は Windows オペレーティングシステムにのみ適用できます。

オペレーティングシステムのリリース ID です。選択したオペレーティングシステムのリリース ID が、入力したリリース ID と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したリリース ID を除くすべてのリリース ID を検索するようにも設定できます。

［**仮想マシン**］セクションでは、仮想マシンであるか仮想デスクトップインフラストラクチャ（VDI）の一部であるかによってデバイスを抽出に含めるための基準を設定できます：

- **仮想マシン**

このドロップダウンリストで、次のオプションを選択できます：

- **未定義**。
- ［**いいえ**］。仮想マシンでないデバイスを検索します。
- **はい**：仮想マシンであるデバイスを検索します。

- **仮想マシンの種別**

このドロップダウンリストで、仮想マシンの製造元を選択できます。

このドロップダウンリストは、［**仮想マシン**］の値が［**はい**］または［**判断しない**］である場合に使用できます。

- **仮想デスクトップインフラストラクチャの一部**

このドロップダウンリストで、次のオプションを選択できます：

- **未定義**。
- ［**いいえ**］。仮想デスクトップインフラストラクチャの一部でないデバイスを検索します。
- **はい**：仮想デスクトップインフラストラクチャ（VDI）の一部であるデバイスを検索します。

［**ハードウェアレジストリ**］サブセクションでは、取り付けたハードウェアを基にデバイスを抽出に含めるための基準を設定できます：

ハードウェアの詳細を取得する Linux デバイスに lshw ユーティリティがインストールされていることを確認してください。使用されているハイパーバイザーによっては、仮想マシンから取得されたハードウェアの詳細が不完全である場合があります。

- **デバイス**

  このドロップダウンリストでは、装置の種別を選択できます。その装置を備えたすべてのデバイスが検索結果に含まれます。

  このフィールドでは全文検索が可能です。

- **製造元**

  このドロップダウンリストで、装置の製造元の名前を選択できます。その装置を備えたすべてのデバイスが検索結果に含まれます。

  このフィールドでは全文検索が可能です。

- **デバイス名**

  デバイスの Windows ネットワークでの名前。指定された名前のデバイスが抽出に含まれます。

- **説明**

  デバイスまたはハードウェア装置の説明。このフィールドで指定された説明が付けられたデバイスが抽出に含まれます。

  デバイスの説明は、そのデバイスのプロパティウィンドウにあらゆる形式で入力できます。このフィールドでは全文検索が可能です。

- **デバイスの製造元**

  デバイスの製造元の名前。このフィールドで指定された製造元のデバイスが抽出に含まれます。

  コンピューターの製造元名は、デバイスのプロパティウィンドウで入力できます。

- **シリアル番号**

  このフィールドで指定されたシリアル番号が付けられたすべてのハードウェアユニットが抽出に含まれます。

- **インベントリ番号**

  このフィールドで指定されたインベントリ番号が付けられた機器が抽出に含まれます。

- **ユーザー**

  このフィールドで指定されたユーザーのすべてのハードウェアユニットが抽出に含まれます。

- **場所**

デバイスまたはハードウェアユニットの場所（本社、支社など）。このフィールドで指定された場所に導入されるコンピューターまたはその他のデバイスが抽出に含まれます。

デバイスの場所は、そのデバイスのプロパティウィンドウにおいて、あらゆる形式で記載できます。

- **CPU クロック周波数（MHz）（最小）**

  CPU の最小クロック周波数。入力フィールドで指定されたクロック周波数範囲と一致する CPU を搭載したデバイスが抽出に含まれます。

- **CPU クロック周波数（MHz）（最大）**

  CPU の最大クロック周波数。入力フィールドで指定されたクロック周波数範囲と一致する CPU を搭載したデバイスが抽出に含まれます。

- **仮想 CPU コア数（最小）**

  仮想 CPU コアの最小数。入力フィールドで指定された仮想コア数の範囲に一致する CPU を搭載したデバイスが抽出に含まれます。

- **仮想 CPU コア数（最大）**

  仮想 CPU コアの最大数。入力フィールドで指定された仮想コア数の範囲に一致する CPU を搭載したデバイスが抽出に含まれます。

- **ハードディスク容量（GB）（最小）**

  デバイス上のハードディスクの最小容量。入力フィールドで指定されたハードディスクの容量の範囲に適合するデバイスが抽出に含まれます。

- **ハードディスク容量（GB）（最大）**

  デバイス上のハードディスクの最大容量。入力フィールドで指定されたハードディスクの容量の範囲に適合するデバイスが抽出に含まれます。

- **RAM サイズ（MB）（最小）**

  デバイスの RAM の最小サイズ。入力フィールドで指定されたサイズ範囲に一致する RAM を搭載したデバイスが抽出に含まれます。

- **RAM サイズ（MB）（最大）**

  デバイスの RAM の最大サイズ。入力フィールドで指定されたサイズ範囲に一致する RAM を搭載したデバイスが抽出に含まれます。

サードパーティ製ソフトウェアの詳細

［**アプリケーションレジストリ**］サブセクションでは、インストール済みのアプリケーションを基にデバイスを検索するための基準を設定できます：

- **アプリケーション名**

  アプリケーションを選択できるドロップダウンリスト。指定したアプリケーションがインストールされているデバイスが抽出に含まれます。

- **アプリケーションのバージョン**

  選択したアプリケーションのバージョンを指定できる入力フィールド。

- **製造元**

  デバイスにインストールされているアプリケーションの製造元を選択できるドロップダウンリスト。

- **アプリケーションのステータス**

  アプリケーションのステータス（*インストール済み*、*未インストール*）を選択できるドロップダウンリスト。指定のアプリケーションがインストール済みまたは未インストールのデバイスが、選択したステータスに応じて抽出に含まれます。

- **アップデートによって検索**

  このオプションをオンにすると、該当するデバイスにインストールされているアプリケーションのアップデートに関する情報を使用して検索が実行されます。このチェックボックスをオンにすると、［**アプリケーション名**］、［**アプリケーションのバージョン**］、［**アプリケーションのステータス**］というフィールドがそれぞれ、［**アップデート名**］、［**アップデートのバージョン**］、［**ステータス**］に変わります。

  既定では、このオプションはオフです。

- **互換性がないセキュリティ製品**

  サードパーティのセキュリティ製品を選択できるドロップダウンリスト。指定したアプリケーションがインストールされているデバイスが、検索時に抽出に含まれます。

- **アプリケーションタグ**

  このドロップダウンリストでは、アプリケーションタグを選択できます。選択したタグが説明にあるアプリケーションをインストール済みのすべてのデバイスが、デバイスの抽出に含まれます。

- **指定したタグのないデバイスに適用する**

  このオプションをオンにすると、選択したタグがいずれも説明に含まれないデバイスが抽出に含まれます。

  このオプションをオフにすると、基準が適用されません。

  既定では、このオプションはオフです。

［**脆弱性とアップデート**］サブセクションでは、Windows Update をどこから取得するかを基にデバイスを抽出に含める場合に使用する基準を指定できます：

WUA の管理サーバーへの切り替え

このドロップダウンリストから、次のいずれかを選択できます：

- **はい**：これを選択すると、Windows Update の更新プログラムを管理サーバーから受信するデバイスが検索結果に含まれます。
- ［**いいえ**］。これを選択すると、Windows Update の更新プログラムを他の提供元から受信するデバイスが検索結果に含まれます。

カスペルスキー製品の詳細

［**カスペルスキー製品**］サブセクションでは、選択した管理対象アプリケーションを基にデバイスを抽出に含めるための基準を設定できます：

- **アプリケーション名**

  カスペルスキー製品の名前で検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます。

  リストには、管理コンピューターに管理プラグインがインストールされているアプリケーションの名前のみが表示されます。

  アプリケーションが選択されていない場合、この基準は適用されません

- **アプリケーションのバージョン**

  カスペルスキー製品のバージョン番号で検索を実行する場合、抽出に含めるデバイスの基準を、入力フィールドで設定できます。

  バージョン番号が指定されていない場合、この基準は適用されません。

- **重要なアップデート名**

  アプリケーションのステータス（*インストール済み*、*未インストール*）を選択できるドロップダウンリスト。指定のアプリケーションがインストール済みまたは未インストールのデバイスが、選択したステータスに応じて抽出に含まれます。

  製品の名前またはアップデートパッケージ番号で検索する場合の、抽出に含めるデバイスの基準を、入力フィールドで設定できます。

  このフィールドが空白の場合、この基準は適用されません。

- **モジュールの最終アップデート期間を選択**

  このオプションを使用して、デバイスにインストールされているソフトウェアモジュールの前回のアップデート日時でデバイスを検索する基準を設定できます。

  このチェックボックスをオンにすると、入力フィールドで、デバイスにインストールされているアプリケーションモジュールの前回のアップデートが実行された日時の範囲を指定できます。

  このチェックボックスをオフにすると、この基準は適用されません。

  既定では、このチェックボックスはオフです。

- **デバイスを管理サーバーで管理する**

  ドロップダウンリストで、Kaspersky Security Center で管理されているデバイスを抽出に含めることができます：

  - **はい**Kaspersky Security Center で管理されているデバイスが抽出に含まれます。
  - ［**いいえ**］。Kaspersky Security Center により管理されていないデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

- **セキュリティ製品がインストールされています**

  ドロップダウンリストで、セキュリティ製品がインストールされているすべてのデバイスを抽出に含めることができます：

  - **はい**：セキュリティ製品がインストールされているすべてのデバイスが抽出に含まれます。
  - ［**いいえ**］。セキュリティ製品がインストールされていないすべてのデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

［**アンチウイルスによる保護**］サブセクションでは、保護ステータスを基にデバイスを抽出に含めるための基準を設定できます：

- **定義データベースの公開日時**

  このオプションをオンにすると、定義データベースの公開日時でクライアントデバイスを検索できます。入力フィールドで設定した期間に基づいて検索が実行されます。

  既定では、このオプションはオフです。

- **定義データベースのレコード数**

  このオプションを有効にすると、定義データベースのレコード数でクライアントデバイスを検索できます。入力フィールドで、定義データベースのレコード数の上下のしきい値を設定できます。

  既定では、このオプションはオフです。

- **前回のスキャン**

  このオプションをオンにすると、前回マルウェアスキャンを実行した日時でクライアントデバイスを検索できます。入力フィールドで、前回マルウェアスキャンを実行した期間を指定できます。

  既定では、このオプションはオフです。

- **検知された脅威**

  このオプションをオンにすると、検知されたウイルスの数でクライアントデバイスを検索できます。入力フィールドで、ウイルス検知数の上下のしきい値を設定できます。

  既定では、このオプションはオフです。

［**暗号化**］サブセクションでは、選択した暗号化アルゴリズムを基にデバイスを抽出に含めるための基準を設定できます：

暗号化アルゴリズム

Advanced Encryption Standard（AES）対称ブロック暗号アルゴリズム。ドロップダウンリストから、暗号化キーのサイズ（56 ビット、128 ビット、192 ビット、または 256 ビット）を選択できます。

指定可能な値：*AES56*、*AES128*、*AES192*、または *AES256*。

［**製品コンポーネント**］サブセクションには、対応する管理プラグインが Kaspersky Security Center Web コンソールにインストールされているアプリケーションのコンポーネントのリストが含まれています。

［**製品コンポーネント**］サブセクションでは、選択したアプリケーションの管理下にあるコンポーネントのステータスとバージョン番号を基にデバイスを抽出に含めるための基準を設定できます：

- **ステータス**

  アプリケーションから管理サーバーに送信されたコンポーネントのステータスに基づいてデバイスを検索します。次のステータスのいずれかを選択できます：*N/A*、*停止*、*一時停止*、*開始中*、*実行中*、*失敗*、*インストールされていない*、*ライセンスでサポートされていない*。管理対象デバイスにインストールされたアプリケーションの選択したコンポーネントのステータスが指定したステータスと一致する場合、そのデバイスが抽出に含まれます。

  製品から送信されるステータス：

  - *停止* - コンポーネントが無効で、現在動作していません。
  - *一時停止* - コンポーネントの動作が中断中です（例：管理対象製品でユーザーが保護を一時停止した）。
  - *開始中* - コンポーネントが利用開始プロセスを実行中です。
  - *実行中* - コンポーネントが有効で正常に動作しています。
  - *エラー* - コンポーネントの動作中にエラーが発生しました。
  - *未インストール* - 製品のカスタムインストールの設定時に、ユーザーがコンポーネントをインストール対象として選択しませんでした。
  - *ライセンスでサポートされていない* - ライセンスは選択したコンポーネントをカバーしていません。

  他のステータスとは異なり、［*N/A*］ステータスはアプリケーションから送信されたものではありません。このステータスは、選択したコンポーネントのステータスについて、アプリケーションに情報がないことを示します。たとえば、デバイスにインストールされているアプリケーションのいずれにも選択したコンポーネントが属していない場合や、デバイスの電源がオフの場合などです。

- **バージョン**

リストで選択したコンポーネントのバージョン番号に基づいてデバイスを検索します。`3.4.1.0` などのバージョン番号を入力し、選択したコンポーネントのバージョン番号がこれと「等しい」「それより古い」「それより新しい」かを指定できます。また、指定したバージョンを除くすべてのバージョンを検索するようにも設定できます。

タグ

［**タグ**］セクションでは、管理対象デバイスの説明に追加済みのキーワード（タグ）を基にデバイスを抽出に含めるための基準を設定できます：

少なくとも 1 個のタグが一致する場合に適用する

このオプションをオンにすると、選択されたタグを 1 つ以上説明に含むデバイスが検索結果に表示されます。

このオプションをオフにすると、選択されたすべてのタグを説明に含むデバイスのみが検索結果に表示されます。

既定では、このオプションはオフです。

基準にタグを追加するには、［**追加**］をクリックし、［**タグ**］入力フィールドをクリックしてタグを選択します。選択したタグを持つデバイスをデバイスの抽出に含めるか除外するかを指定します。

- **All devices that have this tag**

  このオプションをオンにすると、検索結果には、選択したタグが説明内に含まれるデバイスが表示されます。デバイスを検索するため、文字数不定の任意の文字列を表すアスタリスクを使用できます。

  既定では、このオプションがオンです。

- **All devices that do not have this tag**

  このオプションをオンにすると、検索結果には、選択したタグが説明内に含まれないデバイスが表示されます。デバイスを検索するため、文字数不定の任意の文字列を表すアスタリスクを使用できます。

ユーザー

［**ユーザー**］セクションでは、オペレーティングシステムにログインしたユーザーのアカウントを基にデバイスを抽出に含めるための基準を設定できます。

- **前回システムにログインしたユーザー**

  このオプションをオンにすると、基準を設定するためのユーザーアカウントを選択できます。選択したユーザーがシステムの前回のログインを実行したデバイスが検索結果に含まれます。

- **少なくとも 1 回システムにログインしたユーザー**

  このオプションをオンにする場合は、［**参照**］をクリックしてユーザーアカウントを指定します。指定したユーザーがシステムに少なくとも 1 回ログインしたデバイスが検索結果に含まれます。

デバイスの抽出からデバイスリストをエクスポート

Kaspersky Security Center には、デバイスの抽出からデバイスに関する情報を CSV または TXT ファイルに保存できます。

デバイスの抽出からデバイスリストを表示するには：

1. デバイスの抽出からデバイスを含むテーブルを開きます。
2. 次のいずれかの方法を使用して、抽出するデバイスを選択します：
   - 特定のデバイスを選択するには、その横にあるチェックボックスをオンにしてください。
   - 現在のテーブルページからすべてのデバイスを抽出するには、デバイステーブルヘッダーのチェックボックスをオンにし、［**現在のページをすべて選択**］をオンにします。
   - テーブルからすべてのデバイスを抽出するには、デバイステーブルヘッダーのチェックボックスをオンにし、［**すべて選択**］をオンにします。
3. ［**CSV へエクスポート**］または［**TXT へエクスポート**］をクリックします。テーブルに含まれる抽出したデバイスに関するすべての情報がエクスポートされます。

フィルター条件をデバイステーブルに適用した場合、エクスポートされるのは、表示された列からフィルター処理されたデータのみです。

抽出で管理グループからデバイスを削除

デバイスの抽出作業を行う場合は、デバイスを削除する必要がある管理グループに切り替えずに、この抽出に含まれる管理グループからデバイスを削除することができます。

管理グループからデバイスを削除するには：

1. メインメニューで、［**アセット（デバイス）**］→［**デバイスの抽出**］、または［**検出と製品の導入**］→［**デバイスの抽出**］セクションの順に選択します。
2. 抽出リストで、デバイスの抽出の名前をクリックします。
   このページには、デバイスの抽出に含まれるデバイス関連情報のテーブルが表示されます。
3. 削除するデバイスを選択し、［**削除**］をクリックします。
   選択したデバイスが対応する管理グループから削除されます。

デバイスのタグ

Kaspersky Security Center では、デバイスに*タグ付け*できます。タグは、デバイスのグループ化、説明、または検索に使用することができるデバイスのラベルです。デバイスに割り当てられたタグは、抽出の作成、デバイスの検索、および各管理グループへのデバイスの割り当てに使用できます。

デバイスには、手動または自動でタグ付けできます。個々のデバイスにタグ付けする必要がある場合は、手動のタグ付けを使用することができます。自動タグ付けは、指定したタグ付けルールに従い、Kaspersky Security Center によって実行されます。

デバイスには、指定されたルールが適合する場合に自動的にタグ付けされます。個々のルールは各タグに対応します。ルールは、デバイス、オペレーティングシステム、デバイスにインストールされたアプリケーションのネットワークプロパティ、およびその他のデバイスのプロパティに適用されます。たとえば、社内のインフラストラクチャが物理マシン、Amazon EC2 インスタンス、Microsoft Azure 仮想マシンからなるハイブリッド環境の場合、すべての Microsoft Azure 仮想マシンに「[Azure]」タグを割り当てるルールを作成できます。その後、デバイスの抽出を作成する場合にこのタグを使用できます。これにより、Microsoft Azure 仮想マシンが実行されているすべてのデバイスを抽出することができます。

次の場合は、デバイスからタグが自動的に削除されます：

- タグの割り当てルールの条件をデバイスが満たさなくなった場合。
- タグを割り当てるルールがオフになったあるいは削除された場合。

管理サーバーごとのタグのリストとタグ付けルールのリストは、プライマリ管理サーバーとセカンダリ管理サーバーを含むその他のすべての管理サーバーとは影響関係を持ちません。タグ付けのルールは、ルールが作成された管理サーバーのデバイスに対してのみ適用されます。

デバイスタグの作成

デバイスのタグを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. ［**追加**］をクリックします。
   新規タグの入力ウィンドウが表示されます。
3. ［**タグ**］にタグ名を入力します。
4. ［**保存**］をクリックして変更内容を保存します。

   デバイスタグのリストに新しいタグが表示されます。

デバイスタグの名前変更

デバイスタグの名前を変更するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. 名前を変更するタグの名前をクリックします。
   タグのプロパティウィンドウが表示されます。
3. ［**タグ**］でタグ名を変更します。
4. ［**保存**］をクリックして変更内容を保存します。

   デバイスタグのリストに更新したタグが表示されます。

デバイスタグの削除

デバイスタグを削除するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. リストから削除するデバイスタグを選択します。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**はい**］をクリックします。

デバイスタグが削除されます。削除されたタグが割り当てられていたすべてのデバイスから、このタグが自動的に削除されます。

削除したタグは、自動タグルールから自動的に削除されません。タグの削除後も、タグを割り当てるルールの条件に初めて合致した場合にのみ、新規デバイスに対してタグが割り当てられます。

このタグがアプリケーションまたはネットワークエージェントによってデバイスに割り当てられている場合、削除されたタグはデバイスから自動的に削除されません。デバイスからタグを削除するには、klscflag ユーティリティを使用します。

タグを割り当てられているデバイスの表示

タグを割り当てられているデバイスを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. 割り当て先のデバイスを確認するタグの横の［**デバイスの表示**］をクリックします。

   メインメニューの［**管理対象デバイス**］セクションにリダイレクトされ、［**デバイスの表示**］リンクをクリックしたタグでデバイスがフィルタリングされます。
3. デバイスタグのリストに戻るには、ブラウザーの［**戻る**］をクリックします。

タグが割り当てられているデバイスを表示した後、新しいタグを作成して割り当てるか、既存のタグを他のデバイスに割り当てることができます。この場合、タグによるフィルターを削除し、デバイスを抽出してからタグを割り当てる必要があります。

デバイスに割り当てられているタグの表示

デバイスに割り当てられているタグを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
2. タグを表示するデバイスの名前をクリックします。

3. デバイスのプロパティウィンドウが開いたら、［**タグ**］タブをクリックします。

選択したデバイスに割り当てられているタグのリストが表示されます。［**タグの割り当て**］列では、タグがどのように割り当てられたかを確認できます。

デバイスに別のタグを割り当てたり、割り当て済みのタグを削除することができます。管理サーバーに存在するすべてのデバイスタグを表示することもできます。

デバイスへの手動でのタグ付け

デバイスを手動でタグ付けするには：

1. メニューを移動して、別のタグを追加するデバイスに割り当てられているタグを表示します。
2. ［**追加**］をクリックします。
3. 表示されたウィンドウで、次のいずれかを実行します：
   - 新しいタグを作成して割り当てるには、［**新しいタグを作成する**］を選択して新しいタグの名前を入力します。
   - 既存のタグを選択するには、［**既存のタグを割り当てる**］を選択し、ドロップダウンリストから目的のタグを選択します。
4. ［**OK**］をクリックして変更を適用します。
5. ［**保存**］をクリックして変更内容を保存します。

選択したタグがデバイスに割り当てられます。

デバイスに割り当てたタグの削除

デバイスからタグを削除するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. タグを表示するデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**タグ**］タブをクリックします。
4. 削除するタグに隣接するチェックボックスをオンにします。
5. リストの上部にある［**タグを解除しますか？**］をクリックします。
6. 表示されたウィンドウで［**はい**］をクリックします。

タグがデバイスから削除されます。

解除されたタグ自身は削除されません。必要に応じて、手動で削除できます。

アプリケーションまたはネットワークエージェントによってデバイスに割り当てられたタグを手動で削除することはできません。これらのタグを削除するには、klscflag ユーティリティを使用します。

デバイスの自動タグルールの表示

デバイスの自動タグルールを表示するには：

次のいずれかの手順を実行します：

- メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**自動タグルール**］の順に選択します。
- メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に移動し、［**自動タグルールの設定**］をクリックします。
- デバイスに割り当てられているタグを確認し、［**設定**］をクリックします。

デバイスの自動タグルールのリストが表示されます。

デバイスの自動タグルールの編集

デバイスの自動タグルールを編集するには：

1. デバイスの自動タグルールを表示します。
2. 編集するルールの名前をクリックします。
   ルールの設定ウィンドウが表示されます。
3. ルールのプロパティ全般を編集します：
   a. ［**ルール名**］で、ルール名を変更します。
      名前は 256 文字以下でなければなりません。
   b. 次のいずれかの手順を実行します：
      - スイッチを［**ルールが有効**］に切り替えるとルールを有効にできます。
      - スイッチを［**ルールが無効**］に切り替えるとルールを無効にできます。
4. 次のいずれかの手順を実行します：
   - 新しい条件を追加する場合は、［**追加**］をクリックし、開いたウィンドウで新しい条件の設定を指定します。
   - 既存の条件を編集するには、編集する条件の名前をクリックし、条件設定を編集します。
   - 条件を削除するには、削除する条件の横のチェックボックスを選択し、［**削除**］をクリックします。
5. 設定ウィンドウで、［OK］をクリックします。

6. ［**保存**］をクリックして変更内容を保存します。

編集後のルールがリストに表示されます。

デバイスの自動タグルールの作成

デバイスの自動タグルールを作成するには：

1. デバイスの自動タグルールを表示します。
2. ［**追加**］をクリックします。
新規ルールの設定ウィンドウが表示されます。
3. ルールのプロパティ全般を設定します：
   a. ［**ルール名**］で、ルール名を入力します。
   名前は 256 文字以下でなければなりません。
   b. 次のいずれかの手順を実行します：
      - スイッチを［**ルールが有効**］に切り替えるとルールを有効にできます。
      - スイッチを［**ルールが無効**］に切り替えるとルールを無効にできます。
   c. ［**タグ**］で、新しいデバイスタグの名前を入力するか、リストから既存のデバイスタグを選択します。
   名前は 256 文字以下でなければなりません。
4. 条件セクションで［**追加**］をクリックして新しい条件を追加します。
新しい条件の設定ウィンドウが表示されます。
5. 条件の名前を入力します。
名前は 256 文字以下でなければなりません。名前は、1 つのルール内で一意である必要があります。
6. 次の条件によりルールのトリガーを設定します：複数の条件を選択できます。
   - **ネットワーク** - デバイスのネットワークプロパティ（Windows ネットワーク上のデバイス名、デバイスがドメインまたは IP サブネットに含まれるかなど）。

     Kaspersky Security Center で使用するデータベースに大文字と小文字を区別する照合が設定されている場合は、デバイスの DNS 名の指定時に大文字と小文字を区別してください。そうしないと、自動タグ付けルールが機能しません。

   - **アプリケーション** - デバイス上のネットワークエージェントの存在、オペレーティングシステムの種別、バージョン、アーキテクチャ。
   - **仮想マシン** - デバイスが仮想マシンの特定の種別に属しているかどうか。
   - ［**ドメインコントローラー**］- Active Directory 組織単位でのデバイスの存在、および Active Directory グループでのデバイスのメンバーシップ。
   - **アプリケーションレジストリ** - デバイス上の異なる製造元によるアプリケーションの存在。

7. ［**OK**］をクリックして変更内容を保存します。

   必要に応じて、1つのルールに対して複数の条件を設定できます。この場合、タグは少なくとも1つの条件を満たすデバイスに割り当てられます。

8. ［**保存**］をクリックして変更内容を保存します。

新しく作成されたルールは、選択した管理サーバーによって管理されているデバイスに適用されます。デバイスの設定がルールの条件を満たす場合、そのデバイスにタグが割り当てられます。

設定後、ルールは次の状況で適用されます：

- サーバーの負荷に応じて、自動的かつ定期的に適用
- ルールの編集後に適用
- 手動でのルール実行時に適用
- ルールの条件に合致するデバイスの設定の変更やデバイスのグループの設定の変更を管理サーバーが検知した後に適用

複数のタグ付けルールを作成できます。複数のタグ付けルールを作成しており、それらのルールのそれぞれの条件が同時に満たされる場合は、1つのデバイスに複数のタグを割り当てることができます。すべての割り当てられたタグのリストは、デバイスのプロパティで確認できます。

デバイスの自動タグルールの実行

ルールを実行すると、ルールのプロパティで指定されたタグが、ルールのプロパティで指定された条件に合致するデバイスに割り当てられます。有効なルールのみを実行できます。

デバイスの自動タグルールを実行するには：

1. デバイスの自動タグルールを表示します。
2. 実行する有効なルールに隣接するチェックボックスをオンにします。
3. ［**ルールを実行**］をクリックします。

   選択したルールが実行されます。

デバイスの自動タグルールの削除

デバイスの自動タグルールを削除するには：

1. デバイスの自動タグルールを表示します。
2. 削除するルールに隣接するチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されるウィンドウで、もう一度［**削除**］をクリックします。

選択したルールが削除されます。このルールのプロパティで指定されていたタグは、このタグが割り当てられていたすべてのデバイスから割り当て解除されます。

解除されたタグ自身は削除されません。必要に応じて、手動で削除できます。

klscflag ユーティリティを使用したデバイスタグの管理

このセクションでは、klscflag ユーティリティを使用してデバイスタグを割り当てまたは削除する方法について説明します。

デバイスタグの割り当て

タグを割り当てるクライアントデバイスで klscflag ユーティリティを実行する必要があることに注意してください。

klscflag ユーティリティを使用してデバイスにタグを割り当てるには：

1. Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、ネットワークエージェントがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Lab\NetworkAgent。

2. 次のコマンドを入力します：

   ```
   klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"タグ名\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
   ```

   タグ名は、デバイスに割り当てるタグの名前です。例：

   ```
   klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" エンタープライズ \"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
   ```

3. ネットワークエージェントサービスを再起動します。

指定されたタグは、お使いのデバイスに割り当てられます。タグが正常に割り当てられたことを確認するには、デバイスに割り当てられたタグを表示します。

または、デバイスタグを手動で割り当てることもできます。

デバイスタグの削除

アプリケーションまたはネットワークエージェントによってデバイスにタグが割り当てられている場合、このタグを手動で削除することはできません。この場合、klscflag ユーティリティを使用して、割り当てられたタグをデバイスから削除します。

タグを削除するクライアントデバイスで klscflag ユーティリティを実行する必要があることに注意してください。

klscflag ユーティリティを使用してデバイスからタグを削除するには：

1. Windows コマンドプロンプトを管理者権限で実行し、現在のディレクトリを klscflag ユーティリティのあるディレクトリに変更します。klscflag ユーティリティは、ネットワークエージェントがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Lab\NetworkAgent。

2. 次のコマンドを入力します：

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "
[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

3. ネットワークエージェントサービスを再起動します。

タグがデバイスから削除されます。

ポリシーとポリシーのプロファイル

Kaspersky Security Center Web コンソールを使用して、カスペルスキー製品のポリシーを作成できます。このセクションでは、ポリシーおよびポリシーのプロファイルの概要、作成方法、編集方法を説明しています。

ポリシーとポリシープロファイルについて

*ポリシー*とは、管理グループとそのサブグループに適用される一連のカスペルスキー製品の設定です。管理グループのデバイスに複数のカスペルスキー製品をインストールできます。Kaspersky Security Center は、管理グループ内のカスペルスキー製品ごとに1つのポリシーを提供します。ポリシーには、次のいずれかのステータスがあります（以下の表を参照）。

ポリシーのステータス

ステータス	説明
アクティブ	現在デバイスに適用されているポリシー。各管理グループ内のカスペルスキー製品に対してアクティブにできるポリシーは1つだけです。デバイスは、カスペルスキー製品のアクティブポリシーの設定値を適用します。
非アクティブ	現在デバイスに適用されていないポリシー。
モバイルユーザー	このオプションをオンにすると、デバイスが企業ネットワークから離れるとポリシーがアクティブになります。

ポリシーは、次のルールに従って機能します：

- 1つのアプリケーションに対して、異なる値を持つ複数のポリシーを定義することができます。
- 現在のアプリケーションに対してアクティブにできるポリシーは1つだけです。
- 特定のイベントが発生した時に、非アクティブポリシーを有効化できます。たとえば、ウイルスアウトブレイク中に、より厳格なアンチウイルスによる保護設定を適用することができます。
- ポリシーには子ポリシーを設定できます。

一般には、ウイルス攻撃などの緊急事態への備えとしてポリシーを使用できます。たとえば、フラッシュドライブを介した攻撃が発生した場合は、フラッシュドライブへのアクセスをブロックするポリシーを有効化できます。この場合、現在アクティブなポリシーは自動的に非アクティブになります。

異なる状況で複数の設定の変更のみが想定される場合などで、複数のポリシーを管理することを防ぐために、ポリシープロファイルを使用できます。

*ポリシープロファイル*とは、ポリシーの設定値の代わりに使用される、指定されたポリシー設定値のサブセットです。ポリシープロファイルは、管理対象デバイスでの有効な設定の形成に影響を与えます。*有効な設定*とは、デバイスに現在適用されている一連のポリシー設定、ポリシープロファイル設定、およびローカルアプリケーション設定です。

ポリシープロファイルは、次のルールに従って機能します：

- ポリシープロファイルは、特定の有効化条件下で有効になります。
- ポリシープロファイルには、ポリシー設定とは異なる設定値が含まれます。
- ポリシープロファイルを有効化すると、管理対象デバイスの有効な設定が変更されます。
- 1つのポリシーに最大100個のポリシープロファイルを含めることができます。

「ロック」属性とロックされた設定の概要

各ポリシー設定には、ロックのアイコン（）があります。次の表は、ロックのステータスを示しています。

ロックのステータス

ステータス	説明
編集を許可	設定の横に開いたロックが表示され、切り替えスイッチが無効になっている場合、その設定はポリシーで指定されていません。ユーザーは管理対象アプリケーションのインターフェイスを使用してこれらの設定を変更できます。このような設定を「*ロック解除*」と呼びます。
強制適用	設定の横に閉じたロックが表示され、切り替えスイッチが有効になっている場合、その設定はポリシーが適用されるデバイスに適用されます。ユーザーは、管理対象アプリケーションのインターフェイスでこれらの設定の値を変更することはできません。このような設定を「*ロック*」と呼びます。

管理対象デバイスに適用するポリシー設定のロックを閉じておくことを強く推奨します。ロックが解除されたポリシー設定は、管理対象デバイスのカスペルスキーのアプリケーション設定によって再度割り当てられます。

ロックを使用して、次の操作を実行します：

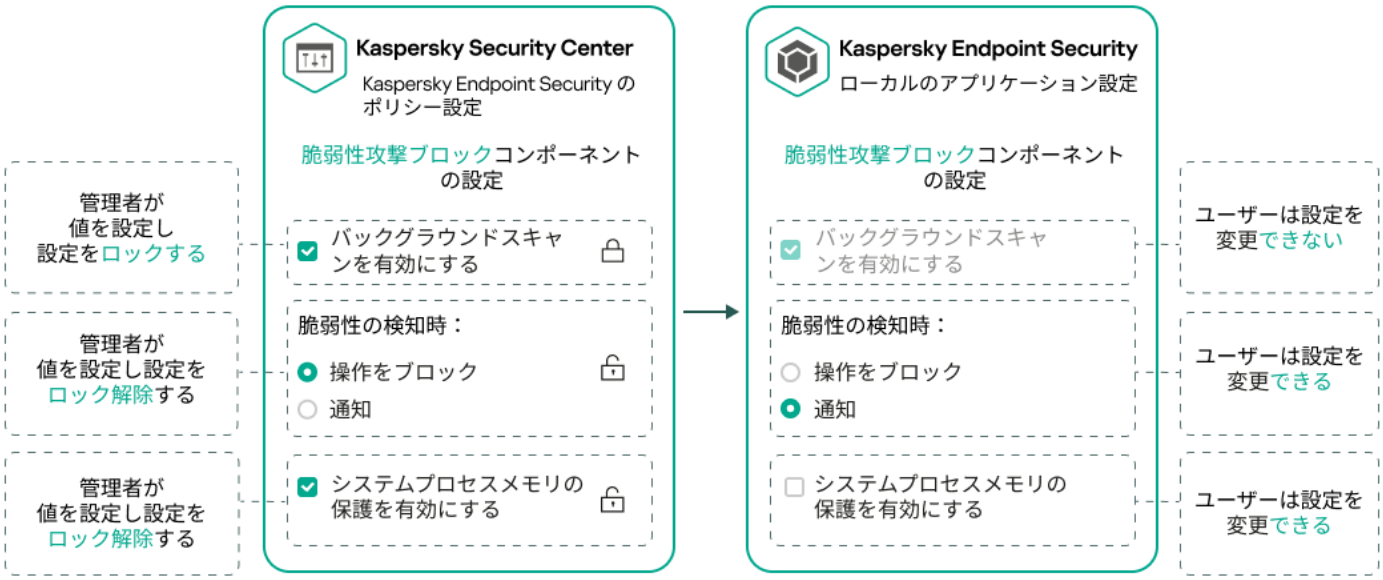
- 管理サブグループのポリシーの設定をロックする
- 管理対象デバイス上のカスペルスキー製品の設定をロックする

したがって、ロックされた設定は、有効な設定を管理対象デバイスに実装するために使用されます。

有効な設定の実装プロセスには、次の操作が含まれます：

- 管理対象デバイスが、カスペルスキー製品の設定値を適用する
- 管理対象デバイスが、ポリシーのロックされた設定の値を適用する

ポリシーおよび管理対象のカスペルスキー製品には、同じ設定内容が含まれています。ポリシー設定を構成すると、管理対象デバイスでカスペルスキー製品設定値が変更されます。管理対象デバイスのロックされた設定をユーザーが調整することはできません（下図を参照）：



ロックとカスペルスキー製品の設定

ポリシーとポリシーのプロファイルの継承

このセクションでは、ポリシーとポリシープロファイルの階層と継承について説明します。

ポリシーの階層

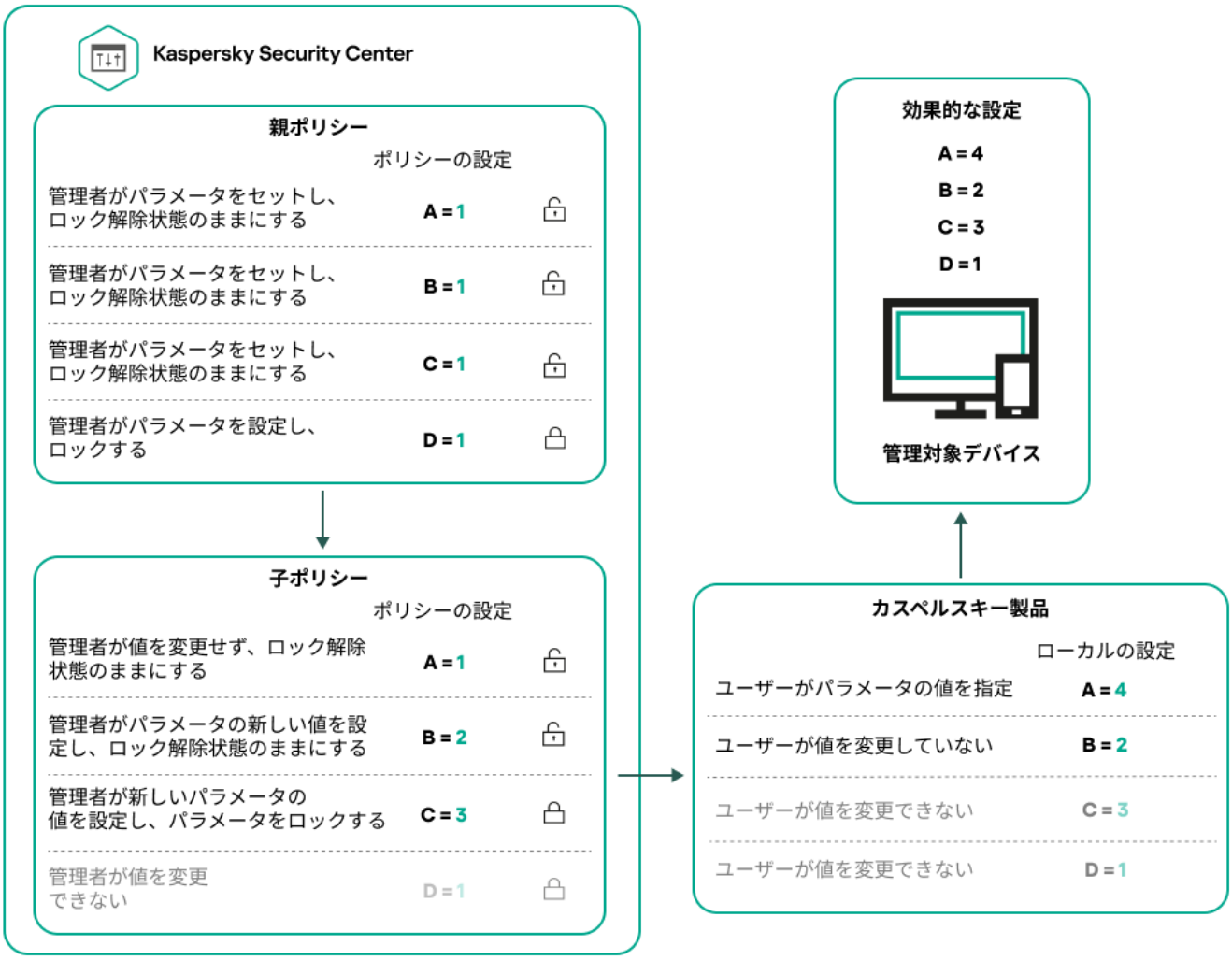
デバイスごとに異なる設定が必要な場合は、デバイスを管理グループに整理できます。

単一の管理グループにポリシーを1つ指定できます。ポリシー設定は*継承できます*。継承とは、上位（親）の管理グループのポリシーからサブグループ（子グループ）にポリシー設定値を受け取ることを意味します。

以降の説明では、親グループで設定されているポリシーを「*親ポリシー*」と表記する場合があります。サブグループ（子グループ）のポリシーを「*子ポリシー*」と表記する場合があります。

既定では、管理サーバーには少なくとも1つの管理対象デバイスグループが存在します。カスタムグループを作成する場合、それらは管理対象デバイスグループ内のサブグループ（子グループ）として作成されます。

同じアプリケーションのポリシーは、管理グループの階層に従って互いに影響を与えます。上位（親）管理グループのポリシーのロック済みの設定は、サブグループのポリシー設定値を再割り当てします（下の図を参照）。

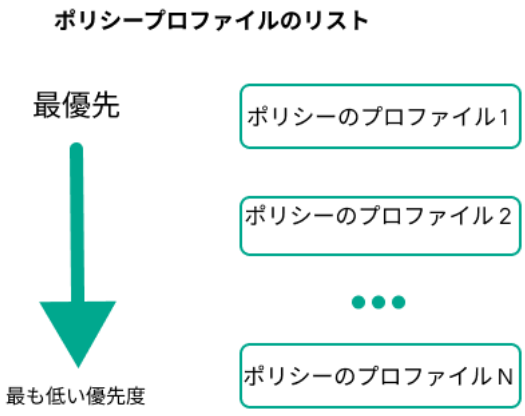


ポリシーの階層

ポリシーの階層内のポリシープロファイル

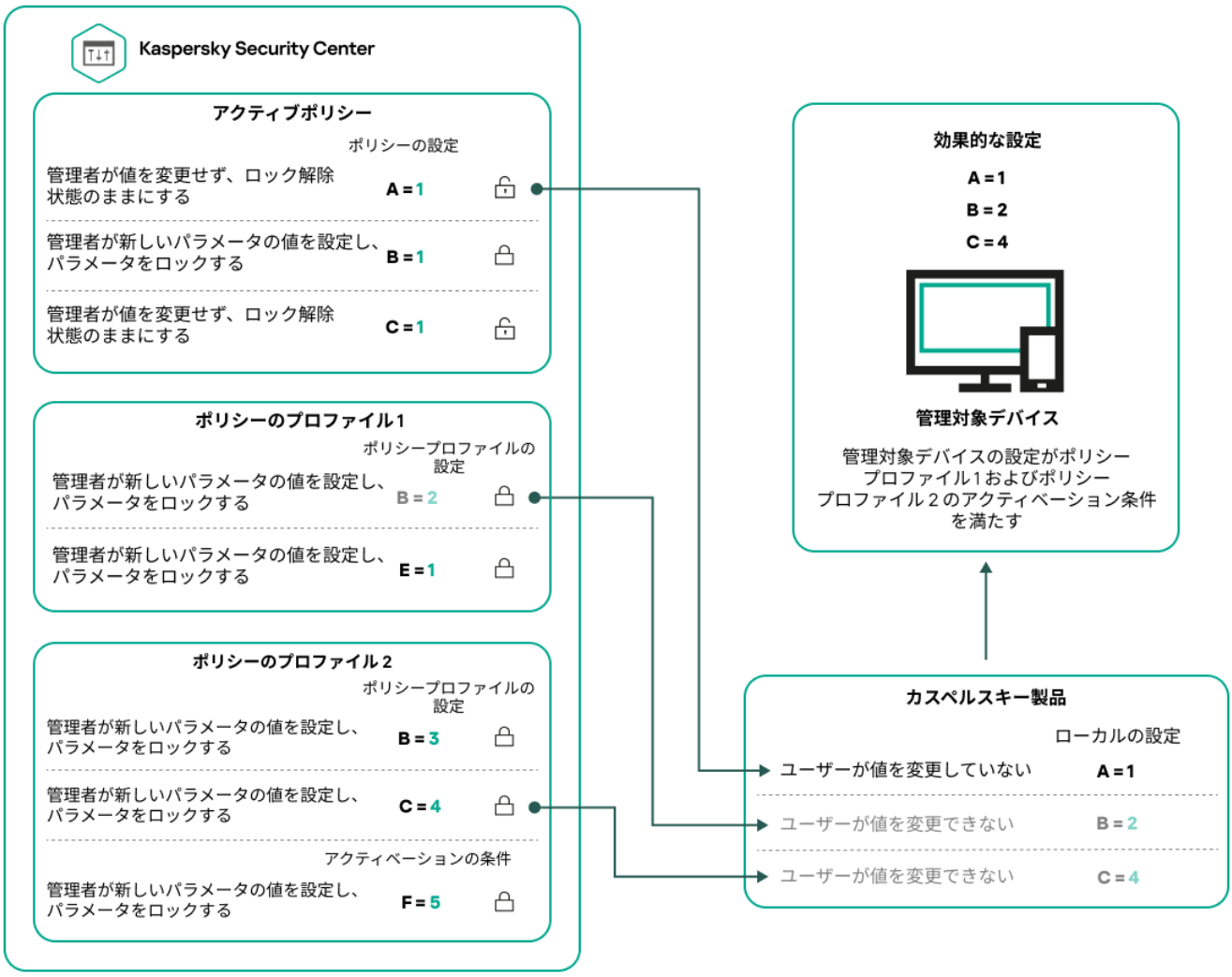
ポリシープロファイルでの優先順位の割り当て条件は次の通りです：

- ポリシープロファイルリスト内のプロファイルの位置は、そのプロファイルの優先度を示します。ポリシーのプロファイルの優先順位を変更できます。リストの一番上にある場合、優先順位が最も高くなります（下の図を参照）。



ポリシープロファイルの優先度の定義

- ポリシープロファイルの有効化条件は相互に依存しません。複数のポリシープロファイルを同時に有効化できます。複数のポリシープロファイルが同じ設定に影響を与える場合、デバイスは最も優先度の高いポリシープロファイルから設定値を取得します（下の図を参照）。



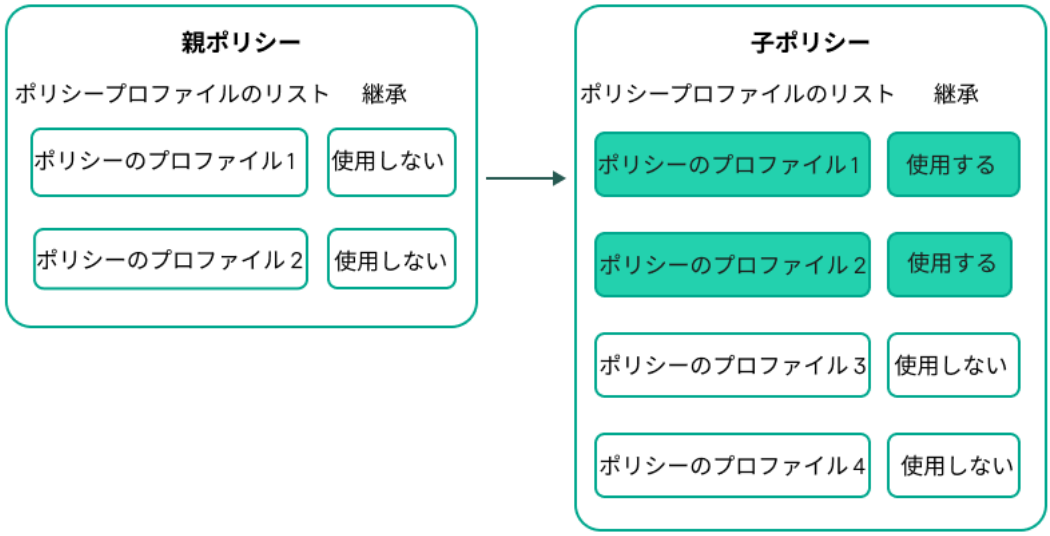
管理対象デバイスの構成が、複数のポリシープロファイルの有効化条件を満たしている

継承の階層におけるポリシープロファイル

様々な階層レベルにあるポリシーのポリシープロファイルは、次の条件を満たします：

- 下位のポリシーは、上位のポリシーからポリシープロファイルを継承します。上位のポリシーから継承されたポリシープロファイルは、元のポリシープロファイルのレベルよりも優先度が高くなります。

- 継承されたポリシープロファイルの優先度を変更することはできません（下の図を参照）。

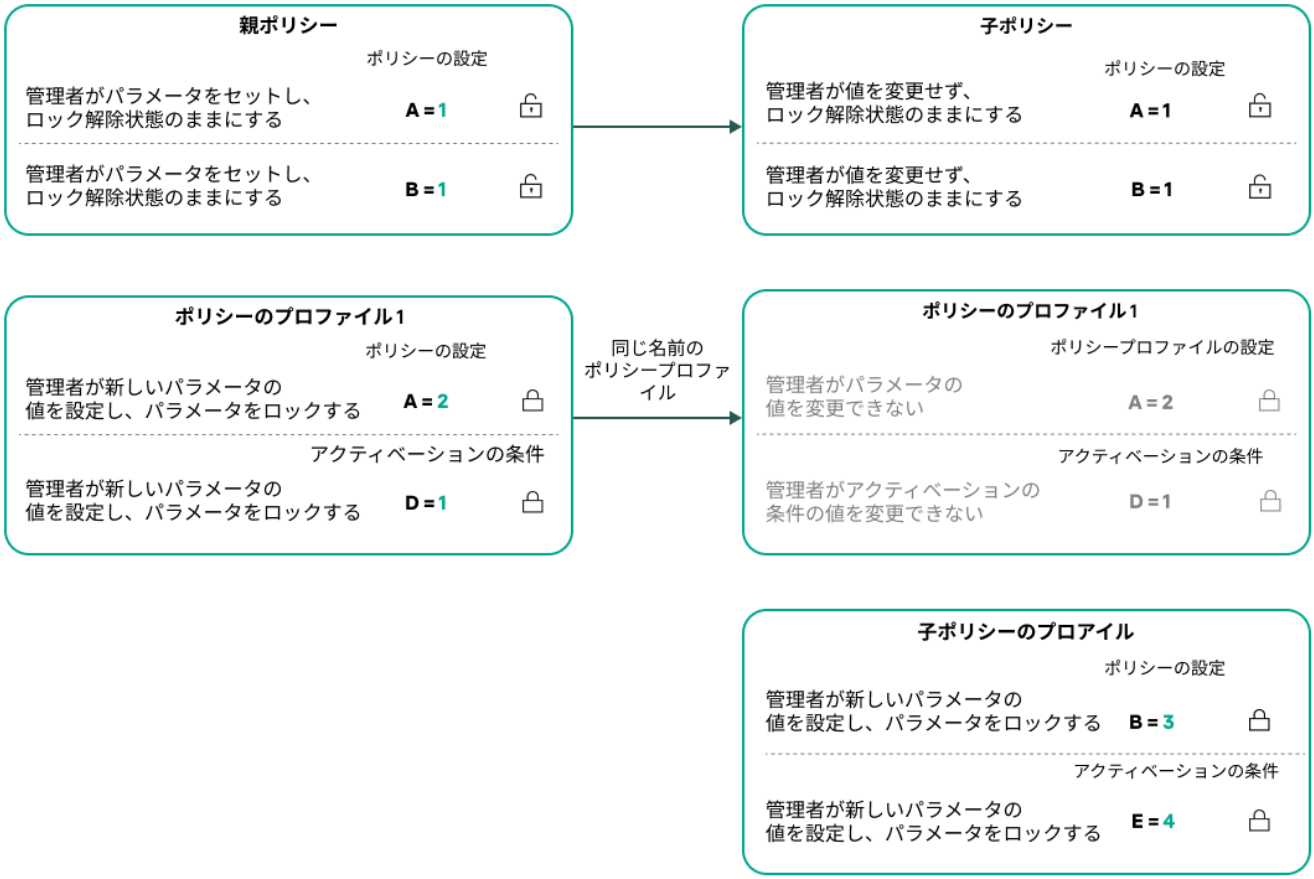


ポリシープロファイルの継承

同じ名前のポリシープロファイル

異なる階層レベルに、同じ名前の 2 つのポリシーがある場合、これらのポリシーは次のルールに従って機能します：

- ロックされた設定および上位のポリシープロファイルのプロファイル有効化条件により、下位のポリシープロファイルの設定およびプロファイル有効化条件が変更されます（下図を参照）。



子プロファイルは親ポリシープロファイルから設定値を継承する

- ロック解除された設定および上位のポリシープロファイルのプロファイル有効化条件により、下位のポリシープロファイルの設定およびプロファイル有効化条件が変更されません。

管理対象デバイスに設定が実装される方法

管理対象デバイスでの有効な設定の実装は、次のように説明できます：

- ロックされていないすべての設定の値は、有効なポリシーから取得されます。
- 次に、管理対象アプリケーション設定の値で上書きされます。
- 次に、有効なポリシーのロックされた設定値が適用されます。ロックされた設定値は、ロックされていない有効な設定値を変更します。

ポリシーの管理

このセクションでは、ポリシーの管理について説明します。ポリシーのリストの表示、ポリシーの作成、ポリシーの変更、ポリシーのコピー、ポリシーの移動、強制同期、ポリシー導入ステータス図の表示、およびポリシーの削除に関する情報を提供します。

ポリシーのリストの表示

管理サーバーまたは任意の管理グループを対象に作成されたポリシーのリストを表示できます。

ポリシーのリストを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. 管理グループのリストで、ポリシーのリストを表示する管理グループを選択します。

   ポリシーのリストが表形式で表示されます。ポリシーが存在しない場合、表は空です。表の列の表示と非表示の切り替え、列の順序の変更、指定した値を含む行のみの表示、検索の使用などを実行できます。

ポリシーの作成

ポリシーの作成と、既存のポリシーの変更と削除を行うことができます。

ポリシーを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. ポリシーを作成する管理グループを選択します。
   - ルートグループ用。
     この場合は次のステップに進むことができます。
   - サブグループの場合：
     a. ウィンドウの上部にある現在のパスリンクをクリックします。

b. 開いたパネルで、必要なサブグループの名前のリンクをクリックします。

現在のパスは、選択したサブグループを反映して変更されます。

3. ［**追加**］をクリックします。
［**アプリケーションの選択**］ウィンドウが表示されます。

4. ポリシーを作成するアプリケーションを選択します。

5. ［**次へ**］をクリックします。
新規ポリシーの設定ウィンドウの［**全般**］タブが表示されます。

6. 必要に応じて、ポリシーの既定の名前、ステータス、継承設定を変更します。

7. ［**アプリケーション設定**］タブを選択します。
あるいは、［**保存**］をクリックして作成を完了します。ポリシーのリストに新しいポリシーが表示されます。ポリシーの設定は後で編集できます。

8. ［**アプリケーション設定**］タブの左側のペインで目的のカテゴリを選択し、右側の結果ペインでポリシーの設定を編集します。ポリシーの各カテゴリ（セクション）の設定を編集できます。
設定内容は、作成するポリシーの対象となる製品に応じて異なります。詳細は、次を参照してください：

- 管理サーバーの設定
- ネットワークエージェントのポリシー設定
- Kaspersky Endpoint Security for Windows のヘルプ

その他のカスペルスキー製品の設定の詳細については、該当する製品のヘルプまたはガイドを参照してください。
設定の編集時、［**キャンセル**］をクリックすると、最後に行った操作を取り消すことができます。

9. ［**保存**］をクリックしてポリシーを保存します。

ポリシーのリストに新しいポリシーが表示されます。

ポリシーの変更

ポリシーを変更するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。

2. 変更するポリシーを選択します：
ポリシーの設定ウィンドウが表示されます。

3. 作成するポリシーの一般設定とアプリケーションの設定を指定します。詳細については、次を参照してください：

- 管理サーバーの設定
- ネットワークエージェントのポリシー設定

- Kaspersky Endpoint Security for Windows のヘルプ

その他のカスペルスキー製品の設定の詳細については、該当する製品のヘルプまたはガイドを参照してください。

4. ［**保存**］をクリックします。

ポリシーに加えた変更は、ポリシーのプロパティに保存され、［**変更履歴**］セクションに表示されます。

ポリシーの全般的な設定

全般

［**全般**］タブでは、ポリシーステータスを変更したり、継承ポリシーを設定したりすることができます：

- ［**ポリシーのステータス**］セクションで、ポリシーのステータスを選択します：
  - **アクティブ**

    このオプションをオンにすると、ポリシーがアクティブになります。
    既定では、このオプションがオンです。

  - **モバイルユーザー**

    このオプションをオンにすると、デバイスが企業ネットワークから離れるとポリシーがアクティブになります。

  - **非アクティブ**

    このオプションをオンにすると、ポリシーは非アクティブになりますが［**ポリシー**］フォルダーに保持されます。必要に応じて、ポリシーをアクティブにすることができます。

- ［**設定の継承**］セクションでは、ポリシーの継承を設定できます。
  - **親ポリシーから設定を継承する**

    このオプションをオンにすると、ポリシーの設定値は上位レベルグループのポリシーから継承されるため、ロックされます。
    既定では、このオプションはオンです。

  - **設定を子ポリシーへ強制的に継承させる**

このオプションをオンにすると、ポリシーの変更を適用した後に次の処理が実行されます：

- 管理サブグループのポリシー（子ポリシー）に、ポリシーの設定値が継承されます。
- 各子ポリシーのプロパティウィンドウの［**全般**］セクションにある［**設定の継承**］ブロックで、［**親ポリシーから設定を継承する**］が自動的にオンになります。

このオプションをオンにすると、子ポリシーの設定はロックされます。

既定では、このオプションはオフです。

イベントの設定

［**イベントの設定**］タブでは、イベントの記録と通知を設定できます。イベントは、重要度に応じて次のタブに分類されます：

- **緊急**
  ［**緊急**］セクションは、ネットワークエージェントのポリシーのプロパティに表示されません。
- **機能エラー**
- **警告**
- **情報**

それぞれのセクションのリストには、イベントの種別と、管理サーバーでイベントが保存される既定の日数が表示されます。イベントの種別をクリックすると、次の設定を指定できます：

- **イベント登録**
  イベントの保存期間を指定し、保存場所を選択できます：
  - **Syslog 経由で SIEM システムにエクスポートする**
  - **デバイスの OS イベントログに保存**
  - **管理サーバーの OS イベントログに保存**
- **イベント通知**
  次の通知方法ごとに、通知を受け取るかどうかを指定できます：
  - **メールで通知**
  - **SMS で通知**
  - **実行ファイルまたはスクリプトの実行で通知**
  - **SNMP 経由で通知**

  既定では、通知に利用する設定（受信アドレスなど）は、管理サーバーのプロパティで指定された設定を使用します。［**メール**］タブ、［**SMS**］タブ、［**実行ファイル**］タブで、必要に応じてそれぞれの設定を変更できます。

変更履歴

［**変更履歴**］タブでは、必要に応じて、ポリシーのリビジョンのリストを表示したり、ポリシーで行われた変更をロールバックすることができます。

ポリシー継承オプションの有効化と無効化

ポリシーで継承オプションを有効または無効にするには：

1. 必要なポリシーを開きます。
2. ［**全般**］タブを開きます。
3. ポリシーの継承をオンまたはオフにします。
   - 子ポリシーで［**親ポリシーから設定を継承する**］をオンにし、管理者が親ポリシーの設定の一部をロック状態にすると、子ポリシーでこれらの設定を変更することはできません。
   - 子ポリシーで［**親ポリシーから設定を継承する**］をオフにすると、親ポリシーでロック状態の設定も含めて、子ポリシー側ですべての設定を変更できます。
   - 親グループで［**設定を子ポリシーへ強制的に継承させる**］をオンにすると、各子ポリシーで［**親ポリシーから設定を継承する**］がオンになります。この場合、子ポリシーの側でこのオプションをオフにすることはできません。親ポリシーでロックされている設定はすべて強制的に子ポリシーに継承され、子グループ側でこれらの設定を変更することはできません。
4. ［**保存**］ボタンをクリックして変更を保存するか、［**キャンセル**］ボタンをクリックして変更を破棄します。

既定では、新規に作成したポリシーでは［**親ポリシーから設定を継承する**］はオンです。

ポリシーにポリシープロファイルが存在する場合、子ポリシーでもこれらのプロファイルが継承されます。

ポリシーのコピー

ポリシーを任意の管理グループから別の管理グループにコピーできます。

ポリシーを別の管理グループにコピーするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. コピーするポリシーに隣接するチェックボックスをオンにします。
3. ［**コピー**］をクリックします。
   画面の右側に管理グループのツリーが表示されます。
4. ツリーで、ポリシーのコピー先となるグループ（ターゲットグループ）を選択します。
5. ページの一番下にある［**コピー**］をクリックします。
6. ［OK］をクリックして処理内容を確定します。

すべてのプロファイルと合わせてターゲットグループにポリシーのコピーが作成されます。ターゲットグループにコピーして作成したポリシーのステータスは［**非アクティブ**］です。いつでもステータスを［**アクティブ**］に変更できます。

新たに移動されるポリシー名と同じ名前のポリシーがターゲットグループに既に存在している場合、新たに移動されるポリシー名に、たとえば (1)、(2) のようなインデックス「(<次の連番>)」が追加されます。

ポリシーの移動

ポリシーを任意の管理グループから別の管理グループに移動できます。たとえば、削除したいグループがあるが、そのグループのポリシーは別のグループで使用したいとします。その場合、グループを削除する前に、ポリシーを別のグループに移動できます。

ポリシーを別の管理グループに移動するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. 移動するポリシーに隣接するチェックボックスをオンにします。
3. ［**移動**］をクリックします。
   画面の右側に管理グループのツリーが表示されます。
4. ツリーで、ポリシーの移動先となるグループ（ターゲットグループ）を選択します。
5. ページの一番下にある［**移動**］をクリックします。
6. ［OK］をクリックして処理内容を確定します。

ポリシーがソースグループから継承されていない場合、ポリシーはすべてのプロファイルと合わせてターゲットグループに（コピーではなく）移動されます。ターゲットグループに作成したポリシーのステータスは［**非アクティブ**］です。いつでもステータスを［**アクティブ**］に変更できます。

ポリシーがソースグループから継承されている場合、ポリシーは元のグループにも残ります。そして、すべてのプロファイルと合わせてターゲットグループにコピーが作成されます。ターゲットグループに作成したポリシーのステータスは［**非アクティブ**］です。いつでもステータスを［**アクティブ**］に変更できます。

新たに移動されるポリシー名と同じ名前のポリシーがターゲットグループに既に存在している場合、新たに移動されるポリシー名に、たとえば (1)、(2) のようなインデックス「(<次の連番>)」が追加されます。

ポリシーのエクスポート

Kaspersky Security Center を使用すると、ポリシーとその設定、ポリシープロファイルを KLP ファイルに保存できます。この KLP ファイルを使用して、Kaspersky Security Center Windows と Kaspersky Security Center Linux の両方に保存したポリシーをインポートできます。

ポリシーをエクスポートするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. エクスポートするポリシーの横のチェックボックスをオンにします。

複数のポリシーを同時にエクスポートすることはできません。複数のポリシーを選択すると、［**エクスポート**］が無効になります。

3. ［**エクスポート**］をクリックします。

4. 表示される［**名前を付けて保存**］ウィンドウで、ポリシーファイルの名前とパスを指定します。［**保存**］をクリックします。

   ［**名前を付けて保存**］ウィンドウは、Google Chrome、Microsoft Edge、または Opera を使用している場合にのみ表示されます。別のブラウザーを使用する場合、ポリシーファイルは自動的に［**Downloads**］フォルダーに保存されます。

ポリシーのインポート

Kaspersky Security Center を使用すると、KLP ファイルからポリシーをインポートできます。KLP ファイルには、エクスポートされたポリシー、その設定、およびポリシープロファイルが含まれています。

ポリシーをインポートするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. ［**インポート**］をクリックします。

3. ［**参照**］をクリックして、インポートするポリシーファイルを選択します。

4. 表示されたウィンドウで、KLP ポリシーファイルのパスを指定し、［**開く**］をクリックします。選択できるポリシーファイルは 1 つだけです。

   ポリシーの処理が始まります。

5. ポリシーが正常に処理されたら、ポリシーを適用する管理グループを選択します。

6. ［**完了**］をクリックしてポリシーのインポートを完了します。

インポート結果の通知が表示されます。ポリシーが正常にインポートされた場合は、［**詳細**］をクリックして、ポリシーのプロパティを表示できます。

インポートが成功すると、ポリシーがポリシーリストに表示されます。ポリシーの設定とプロファイルもインポートされます。エクスポート中に選択されたポリシーステータスにかかわらず、インポートされたポリシーは非アクティブです。ポリシーのプロパティでポリシーステータスを変更できます。

新しくインポートされたポリシーと同じ名前のポリシーが既に存在している場合、インポートされたポリシーの名前に、たとえば **(1)**、**(2)** のようなインデックス「**(<次の連番>)**」が付きます。

ポリシー導入ステータス図の表示

Kaspersky Security Center では、各デバイスのポリシー適用のステータスをポリシー導入ステータス図で表示できます。

各デバイスのポリシー導入ステータスを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. デバイスの導入ステータスを表示するポリシーの名前に隣接するチェックボックスをオンにします。

3. 表示されたメニューで、［**導入**］リンクを選択します。
［**<ポリシー名> 導入結果**］ウィンドウが開きます。

4. 開いた［**<ポリシー名> 導入結果**］ウィンドウに、ポリシーの**ステータスの説明**が表示されます。

ポリシーの導入結果のリストに表示されるデバイス数を変更できます。推奨されるデバイス数の上限は、100000 台です。

ポリシーの導入結果のリストに表示されるデバイスの数を変更するには：

1. メインメニューで、アカウント設定に移動して、［**インターフェイスのオプション**］をオンにします。

2. ［**ポリシーの導入結果に表示するデバイス数の上限**］に、デバイスの数（最大 100,000）を入力します。
既定では、この数は 5,000 です。

3. ［**保存**］をクリックします。
設定が保存され、適用されます。

［ウイルスアウトブレイク］イベント発生時におけるポリシーの自動アクティブ化

［ウイルスアウトブレイク］イベント発生時にポリシーの自動アクティベーションを実行するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（ ）をクリックします。
管理サーバーのプロパティウィンドウの［**全般**］タブが表示されます。

2. ［**ウイルスアウトブレイク**］セクションを選択します。

3. 右側のペインで、［［**ウイルスアウトブレイク］イベント発生時にアクティブ化するポリシーの設定**］をクリックします。
［**ポリシーのアクティブ化**］ウィンドウが表示されます。

4. ウイルスアウトブレイクを検知するコンポーネントの対象領域ごとに（ワークステーションおよびファイルサーバー向けアンチウイルス製品、メールサーバー向けアンチウイルス製品、境界防御向けアンチウイルス製品）、［**追加**］をクリックします。
［**管理対象デバイス**］管理グループウィンドウが表示されます。

5. ［**管理対象デバイス**］の横にあるアイコン（ ）をクリックします。
管理グループの階層とそれぞれの管理グループのポリシーが表示されます。

6. 管理グループの階層とポリシーから、ウイルスアウトブレイクの検知時にアクティブにするポリシーを選択します。
1つのグループのすべてのポリシーを有効にする場合は、該当するグループ名の横のチェックボックスをオンにします。

7. ［**保存**］をクリックします。
管理グループの階層とポリシーのウィンドウが閉じます。

選択したポリシーが、ウイルスアウトブレイクの検知時にアクティブ化されるポリシーのリストに追加されます。選択したポリシーは、その時点でアクティブか非アクティブかに関係なく、ウイルスアウトブレイクの発生時にアクティブになります。

［ウイルスアウトブレイク］イベントでポリシーがアクティブ化された場合は、手動モードを使用することによってのみ前のポリシーに戻ることができます。

ポリシーの削除

必要ないポリシーは削除できます。ただし、削除できるのは上位のグループから継承されたのではないポリシーのみです。上位のグループから継承されたポリシーは、そのポリシーが作成された上位のグループでのみ削除できます。

ポリシーを削除するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. 削除するポリシーの横のチェックボックスをオンにし、［**削除**］をクリックします。
   上位のポリシーから設定を継承したポリシーを選択した場合、［**削除**］はグレーアウトされ選択できなくなります。
3. ［**OK**］をクリックして処理内容を確定します。

ポリシーとそのすべてのプロファイルが削除されます。

ポリシーのプロファイルの管理

このセクションでは、ポリシープロファイルの管理について説明します。ポリシーのプロファイルの表示、ポリシープロファイルの優先度の変更、ポリシープロファイルの作成、ポリシープロファイルの変更、ポリシープロファイルのコピー、ポリシープロファイルの有効化ルールの作成、およびポリシープロファイルの削除に関する情報を提供します。

ポリシーのプロファイルの表示

ポリシーのプロファイルを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. プロファイルを表示するポリシーの名前をクリックします：
   ポリシーのプロパティウィンドウの［**全般**］タブが表示されます。
3. ［**ポリシーのプロファイル**］タブを開きます。

ポリシーのプロファイルのリストが表形式で表示されます。ポリシーにプロファイルが設定されていない場合、表は空です。

ポリシーのプロファイルの優先順位の変更

ポリシーのプロファイルの優先順位を変更するには：

1. 目的のポリシーのプロファイルのリストに移動します。

   ポリシーのプロファイルのリストが表示されます。

2. ［**ポリシーのプロファイル**］タブで、優先度を変更するポリシープロファイルの横にあるチェックボックスをオンにします。

3. ［**優先度を高く設定**］または［**優先度を低く設定**］をクリックして、ポリシープロファイルの新しい位置を指定します。

   リスト内でポリシーの位置が上にあるほど、優先度も高くなります。

4. ［**保存**］をクリックします。

選択したポリシーのプロファイルの優先順位が変更され、適用されます。

ポリシーのプロファイルの作成

ポリシーのプロファイルを作成するには：

1. 目的のポリシーのプロファイルのリストに移動します。

   ポリシーのプロファイルのリストが表示されます。ポリシーにプロファイルが設定されていない場合、表は空です。

2. ［**追加**］をクリックします。

3. 必要に応じて、プロファイルの既定の名前と継承設定を変更します。

4. ［**アプリケーション設定**］タブを選択します。

   または、［**保存**］をクリックして完了します。ポリシープロファイルのリストに作成したプロファイルが表示されます。プロファイルの設定は後で編集できます。

5. ［**アプリケーション設定**］タブの左側のペインで目的のカテゴリを選択し、右側の結果ペインでプロファイルの設定を編集します。ポリシーのプロファイルの各カテゴリ（セクション）の設定を編集できます。

   設定の編集時、［**キャンセル**］をクリックすると、最後に行った操作を取り消すことができます。

6. ［**保存**］をクリックしてプロファイルを保存します。

ポリシーのプロファイルのリストに新しいプロファイルが表示されます。

ポリシーのプロファイルの編集

ポリシーのプロファイルの編集機能は、Kaspersky Endpoint Security for Windows のポリシーにのみ使用可能です。

ポリシーのプロファイルを変更するには：

1. 目的のポリシーのプロファイルのリストに移動します。

   ポリシーのプロファイルのリストが表示されます。

2. ［**ポリシーのプロファイル**］タブで、変更するポリシープロファイルをクリックします。

   ポリシーのプロファイルのプロパティウィンドウが開きます。

3. プロパティウィンドウでプロファイルを設定します。

   - 必要に応じて、［**全般**］タブでプロファイル名を変更したり、プロファイルを有効または無効にします。
   - プロファイルの有効化ルールを編集します。
   - アプリケーション設定を編集します。

   カスペルスキー製品の設定の詳細については、該当する製品のヘルプまたはガイドを参照してください。

4. ［**保存**］をクリックします。

デバイスが管理サーバーと同期した後（ポリシーのプロファイルが有効な場合）、または有効化ルールが適合した時（ポリシーのプロファイルが無効な場合）、変更した設定が有効になります。

ポリシーのプロファイルのコピー

ポリシーのプロファイルを現在の割り当て先のポリシーや別のポリシーにコピーして、同じポリシーを別のポリシーで使用できます。また、プロファイルのコピー機能は、一部の設定だけが異なる複数のプロファイルを作成する場合にも活用できます。

ポリシーのプロファイルをコピーするには：

1. 目的のポリシーのプロファイルのリストに移動します。

   ポリシーのプロファイルのリストが表示されます。ポリシーにプロファイルが設定されていない場合、表は空です。

2. ［**ポリシーのプロファイル**］タブで、コピーするポリシープロファイルを選択します。

3. ［**コピー**］をクリックします。

4. 表示されるウィンドウで、プロファイルのコピー先にするポリシーを選択します。

   ポリシーのプロファイルを、現在割り当てられているのと同じポリシーまたは指定した別のポリシーにコピーできます。

5. ［**コピー**］をクリックします。

ポリシーのプロファイルが指定したポリシーにコピーされます。コピーして作成された新しいプロファイルには、最も低い優先度が設定されます。プロファイルを現在割り当てられているのと同じポリシーにコピーした場合、プロファイル名に (1)、(2) のようなインデックス「<数字>」が追加されます。

コピーの完了後、プロファイル名や優先度も含めてプロファイルの設定を変更できます。この変更によりコピー元のプロファイルが影響を受けることはありません。

ポリシーのプロファイルの有効化ルールの作成

ポリシーのプロファイルの有効化ルールを作成するには：

1. 目的のポリシーのプロファイルのリストに移動します。
   ポリシーのプロファイルのリストが表示されます。
2. ［**ポリシーのプロファイル**］タブで、有効化ルールを作成するポリシープロファイルをクリックします。
   ポリシープロファイルのリストが空の場合は、ポリシーのプロファイルを作成できます。
3. ［**有効化ルール**］タブで、［**追加**］をクリックします。
   ポリシーのプロファイルの有効化ルールのウィンドウが表示されます。
4. ルールの名前を入力します。
5. 作成しているポリシープロファイルの有効化に作用する条件の横にあるチェックボックスをオンにします：

   - **ポリシープロファイルの有効化に対する全般ルール**

     このチェックボックスをオンにすると、デバイスのオフラインモードのステータス、管理サーバーへの接続ルール、デバイスに割り当てられているタグに応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

     このオプションでは、次の項目を設定できます：

     - **デバイスのステータス**

       ネットワーク内にデバイスが存在するかどうかを指定します：
       - **オンライン** - デバイスはネットワーク内にあるため、管理サーバーを使用できます。
       - **オフライン** - デバイスは外部ネットワーク内にあるため、管理サーバーは使用できません。
       - **該当なし** - 基準は適用されません。

     - **管理サーバー接続のルールがこのデバイスでアクティブです**

       ポリシーのプロファイルを有効化する条件（ルールを実行する条件）を選択し、ルールの名前を指定します。

       ルールでは、管理サーバーへの接続に関するデバイスのネットワークロケーションを指定します。ポリシープロファイルを有効にするためにネットワークロケーションの説明の条件を満たす（または満たさない）必要があります。

       管理サーバーへの接続に関するデバイスのネットワークロケーションの説明は、ネットワークエージェント切り替えルールで作成または設定できます。

   - **特定のデバイス所有者向けのルール**

     このオプションでは、次の項目を設定できます：

- **デバイスの所有者**

  このオプションをオンにして、デバイスの所有者に応じたプロファイルの有効化ルールを設定を有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

  - デバイスが特定の所有者のものである（「=」記号）
  - デバイスが特定の所有者のものでない（「#」記号）

    このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。このオプションをオンにすると、デバイスの所有者を指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **デバイスの所有者が属する内部セキュリティグループ**

  このオプションをオンにして、デバイスの所有者の Kaspersky Security Center の内部セキュリティグループの所属に応じたプロファイルの有効化ルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

  - デバイスの所有者が特定のセキュリティグループのメンバーである（「=」記号）
  - デバイスの所有者が特定のセキュリティグループのメンバーでない（「?」記号）

    このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。Kaspersky Security Center のセキュリティグループを指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **ハードウェアの仕様のルール**

  このチェックボックスをオンにすると、メモリサイズと論理プロセッサの数に応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

  このオプションでは、次の項目を設定できます：

  - **RAM サイズ（MB）**

    このオプションをオンにして、デバイスで使用可能な RAM サイズに応じたプロファイルの有効化のルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

    - デバイスの RAM サイズは指定された値以下である（「<」記号）。
    - デバイスの RAM サイズは指定された値以上である（「>」記号）。

    このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。デバイスの RAM ボリュームを指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

  - **論理プロセッサの数**

このオプションをオンにして、デバイスの論理プロセッサの数に応じたプロファイルの有効化ルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

- デバイスの論理プロセッサの数は指定された値以下である（「<」記号）。
- デバイスの論理プロセッサの数は指定された値以上である（「>」記号）。

このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。デバイス上の論理プロセッサの数を指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **ロールの割り当てルール**

  このオプションでは、次の項目を設定できます：

  デバイス所有者のロールに応じてポリシープロファイルを有効化する

  このオプションをオンにすると、デバイスの所有者のロールに応じたプロファイルの有効化ルールを設定し、オンにすることができます。既存のロールのリストからロールを手動で選択して追加します。

  このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。

- **タグの使用ルール**

  このチェックボックスをオンにすると、デバイスに割り当てられたタグに応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。選択したタグが割り当てられているデバイスまたは割り当てられていないデバイスのいずれかで、ポリシーのプロファイルを有効にできます。

  このオプションでは、次の項目を設定できます：

  - **タグ**

    このタグのリストで、目的のタグのチェックボックスをオンにすると、ポリシーのプロファイルにデバイスを含めるためのルールを指定できます。

    リストの上のフィールドに新しいタグを入力して、［**追加**］をクリックすると、新しいタグをリストに追加できます。

    選択したタグのすべてを説明に含むデバイスがポリシーのプロファイルに含まれます。チェックボックスをオフにすると、基準は適用されません。既定では、これらのチェックボックスはオフです。

  - **指定したタグのないデバイスに適用する**

    タグの選択状態を反転させる必要がある場合は、このオプションをオンにします。

    このオプションをオンにすると、選択されたタグのいずれも説明に含まないデバイスがポリシープロファイルに含まれます。このオプションをオフにすると、基準が適用されません。

    既定では、このオプションはオフです。

- **Active Directory 使用のルール**

このチェックボックスをオンにすると、Active Directory 組織単位（OU）内にデバイスが属しているか、または Active Directory セキュリティグループにデバイス（またはその所有者）が属しているかに応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

このオプションでは、次の項目を設定できます：

- **Active Directory セキュリティグループのデバイス所有者メンバーシップ**

  このオプションを有効にすると、所有者が指定されたセキュリティグループに所属しているデバイスで、ポリシーのプロファイルが有効化されます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **デバイスが属している Active Directory セキュリティグループ**

  このオプションを有効にすると、デバイスでポリシープロファイルが有効化されます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **デバイスが割り当てられている Active Directory 組織単位**

  このオプションを有効にすると、指定された Active Directory 組織単位（OU）に属するデバイスで、ポリシーのプロファイルが有効化されます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。

  既定では、このオプションはオフです。

ウィザードで表示されるウィンドウ数は、最初のステップで選択した設定によります。ポリシープロファイルの有効化ルールは後で変更することができます。

6. 設定したパラメータのリストを確認します。リストのパラメータが正しいことが確認できたら、［**作成**］をクリックします。

プロファイルが保存されます。プロファイルは、有効化ルールが適合すると、デバイスで有効になります。

プロファイル用に作成したポリシープロファイルの有効化ルールが、［**有効化ルール**］タブのポリシープロファイルのプロパティに表示されます。ポリシープロファイルの有効化ルールはいずでも変更または削除することができます。

複数の有効化ルールを同時に適合させることができます。

ポリシーのプロファイルの削除

ポリシーのプロファイルを削除するには：

1. 目的のポリシーのプロファイルのリストに移動します。

   ポリシーのプロファイルのリストが表示されます。

2. ［**ポリシーのプロファイル**］タブで、削除するポリシープロファイルに隣接するチェックボックスをオンにし、［**削除**］をクリックします。

3. 表示されるウィンドウで、もう一度［**削除**］をクリックします。

ポリシープロファイルが削除されます。下位のグループでこのポリシーが継承されている場合、該当する下位のグループでプロファイルが維持されますが、プロファイルの所属先がこの下位のグループのポリシーに変更されます。この処理は、下位グループのデバイスにインストールされている管理対象製品の設定が大幅に変更されてしまわないようにするために実装されています。

データ暗号化と保護機能

データ暗号化により、ノート PC やハードディスクの盗難や紛失、不正なユーザーやアプリケーションによるアクセスなどによる思いがけない情報漏洩の危険性を低減できます。

以下のカスペルスキー製品が暗号化をサポートします：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

ユーザーインターフェイス設定を使用して、暗号化管理の機能に関連するインターフェイス要素の一部を表示または非表示にすることができます。

Kaspersky Endpoint Security for Windows でのデータ暗号化

次の種別の暗号化を管理できます：

- サーバー用の Windows オペレーティングシステムを実行しているデバイスでの BitLocker ドライブ暗号化
- ワークステーション用の Windows オペレーティングシステムを実行しているデバイスでの Kaspersky Disk Encryption

Kaspersky Endpoint Security for Windows のこれらのコンポーネントを使用すると、暗号化を有効または無効にする、暗号化されたドライブのリストを表示する、暗号化に関するレポートを生成して表示する、などの操作を実行できます。

Kaspersky Security Center で Kaspersky Endpoint Security for Windows のポリシーを設定することで、暗号化の設定を編集できます。Kaspersky Endpoint Security for Windows は、アクティブなポリシーに基づいて、暗号化と復号化を実行します。ルールの編集方法と暗号化機能の詳細については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

Kaspersky Endpoint Security for Mac でのデータ暗号化

macOS デバイスで FileVault 暗号化を使用できます。Kaspersky Endpoint Security for Mac の使用中に、暗号化を有効化または無効化できます。

Kaspersky Security Center で Kaspersky Endpoint Security for Mac のポリシーを設定することで、暗号化の設定を編集できます。Kaspersky Endpoint Security for Mac は、アクティブなポリシーに基づいて、暗号化と復号化を実行します。詳細は、Kaspersky Endpoint Security for Mac のヘルプを参照してください。

暗号化されたドライブのリストの表示

Kaspersky Security Center で、暗号化されたドライブの詳細や、ドライブレベルで暗号化されたデバイスの詳細を表示できます。ドライブ上の情報が復号されると、そのドライブはリストから自動的に削除されます。

暗号化されたドライブのリストを表示するには、

メインメニューで、［**操作**］→［**データ暗号化と保護機能**］→［**暗号化されたドライブ**］の順に移動します。

セクションがメニューにない場合、非表示になっています。セクションを表示させるには、ユーザーインターフェイスの設定で、［**データ暗号化と保護機能の表示**］を有効にします。

暗号化されたドライブのリストを CSV ファイルまたは TXT ファイルにエクスポートできます。これを行うには、［**CSV へエクスポート**］または［**TXT へエクスポート**］をクリックします。

暗号化イベントのリストの表示

デバイス上でデータの暗号化または復号化タスクを実行する時、Kaspersky Endpoint Security for Windows は、次の種類のイベントに関する Kaspersky Security Center 情報を送信します：

- ディスクの空き容量が不足しているため、ファイルの暗号化または復号化ができないか、暗号化されたファイルを作成できない
- ライセンスの問題で、ファイルの暗号化または復号化ができないか、暗号化されたファイルを作成できない
- アクセス権がないため、ファイルの暗号化または復号化ができないか、暗号化されたファイルを作成できない
- アプリケーションが暗号化されたファイルへのアクセスをブロックされている
- 不明なエラー

デバイスでのデータの暗号化中に発生したイベントのリストを表示するには：

メインメニューで、［**操作**］→［**データ暗号化と保護機能**］→［**暗号化イベント**］の順に移動します。

セクションがメニューにない場合、非表示になっています。セクションを表示させるには、ユーザーインターフェイスの設定で、［**データ暗号化と保護機能の表示**］を有効にします。

暗号化されたドライブのリストを CSV ファイルまたは TXT ファイルにエクスポートできます。これを行うには、［**CSV へエクスポート**］または［**TXT へエクスポート**］をクリックします。

または、すべての管理対象デバイスの暗号化イベントのリストを確認することができます。

管理対象デバイスの暗号化イベントを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

2. 管理対象デバイスの名前をクリックします。

3. ［**全般**］タブで、［**プロテクション**］セクションに移動します。

4. ［**データ暗号化エラーの表示**］をクリックします。

暗号化レポートの作成と表示

次のレポートを作成できます：

- 管理対象デバイスの暗号化ステータスレポート：様々な管理対象デバイスのデータ暗号化について詳細を確認できます。たとえば、暗号化ルールが設定されたポリシーが適用されるデバイスの数が表示されます。また、再起動が必要なデバイスの数なども確認できます。さらに、各デバイスの暗号化技術とアルゴリズムに関する情報も含まれています。

- 大容量ストレージデバイスの暗号化ステータスレポート：管理対象デバイスの暗号化ステータスレポートと類似の情報が含まれますが、大容量ストレージデバイスとリムーバブルドライブのデータのみが表示されます。

- 暗号化されたドライブへのアクセス権に関するレポート：暗号化されたドライブへのアクセス権を持つユーザーアカウントが表示されます。

- ファイル暗号化のエラーに関するレポート：デバイスでデータの暗号化または復号化タスクを実行した時に発生したエラーの情報を含みます。

- 暗号化されたファイルへのアクセスのブロックに関するレポート：暗号化されたファイルへのアクセスのブロックに関する情報を含みます。このレポートは、暗号化されたファイルやドライブに不正なユーザーまたはアプリケーションがアクセスしようとした場合に役立ちます。

［**監視とレポート**］→［**レポート**］セクションの順に移動して、レポートを生成できます。または、［**操作**］→［**データ暗号化と保護機能**］セクションの順に移動して、次の暗号化レポートを生成できます：

- 大容量ストレージデバイスの暗号化ステータスレポート

- 暗号化されたドライブへのアクセス権に関するレポート

- ファイル暗号化のエラーに関するレポート

*［**データ暗号化と保護機能**］セクションで暗号化レポートを生成するには：*

1. インターフェイスのオプションで、［**データ暗号化と保護機能の表示**］がオンであることを確認します。

2. メインメニューで、［**操作**］→［**データ暗号化と保護機能**］の順に移動します。

3. 次のいずれかのセクションを開きます：

   - **暗号化されたドライブ**：大容量ストレージデバイスの暗号化ステータスレポート、または暗号化されたドライブへのアクセス権に関するレポートが生成されます。

   - **暗号化イベント**：ファイル暗号化エラーのレポートが生成されます。

4. 生成するレポートの名前をクリックします。

レポート作成が開始されます。

暗号化されたドライブへのオフラインモードでのアクセス権の付与

管理対象デバイスに Kaspersky Endpoint Security for Windows がインストールされていない場合などに、ユーザーは、暗号化されたデバイスへのアクセスを要求できます。要求を受信したら、アクセスキーファイルを作成してユーザーに送信できます。すべてのユースケースと詳細な手順については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

暗号化されたドライブへのオフラインモードでのアクセス権を付与するには：

1. ユーザーからアクセス要求ファイル（拡張子が FDERTC のファイル）を取得します。Kaspersky Endpoint Security for Windows でファイルを生成するには、Kaspersky Endpoint Security for Windows のヘルプの指示に従ってください。
2. メインメニューで、［**操作**］→［**データ暗号化と保護機能**］→［**暗号化されたドライブ**］の順に移動します。

   暗号化されたドライブのリストが表示されます。
3. ユーザーがアクセスを要求したドライブを選択します。
4. ［**オフラインモードでのデバイスへのアクセスを許可**］をクリックします。
5. 表示されるウィンドウで、選択したドライブの暗号化に使用したカスペルスキー製品に対応するプラグインを選択します。

   > Kaspersky Security Center Web コンソールでサポートされないカスペルスキー製品を使用して暗号化されたドライブの場合は、MMC ベースの管理コンソールを使用してオフラインモードでのアクセス権を付与します。
6. Kaspersky Endpoint Security for Windows のヘルプの指示に従ってください（セクションの最後にある項目を展開して参照してください）。

その後、受信したファイルを適用して暗号化されたドライブにアクセスし、ドライブに保存されているデータを読み取ることができます。

ユーザーとユーザーロール

このセクションでは、ユーザーとユーザーロールの概要および作成と編集の手順、ユーザーへのロールとグループの割り当て方法、ポリシーのプロファイルとロールの関連付けの方法について説明しています。

ユーザーロールの概要

ユーザーロール（省略して「*ロール*」とも表記）は、複数の権限をまとめたものと捉えることができます。ロールは、ユーザーのデバイスにインストールされているカスペルスキー製品の設定と関連付けることができます。ロールは、管理グループ、管理サーバー、または特定のオブジェクトのレベルのユーザーまたはセキュリティグループの階層構造の任意のレベルに位置する一連のユーザーまたは一連のセキュリティグループに割り当てることができます。

仮想管理サーバーを含む管理サーバーの階層を介してデバイスを管理する場合は、物理管理サーバーからのみユーザーロールを作成、変更、または削除できることに注意してください。次に、仮想サーバーを含むセカンダリ管理サーバーにユーザーロールを適用できます。

ユーザーロールはポリシーのプロファイルに関連付けることができます。ユーザーにロールを割り当てることで、このユーザーには、担当業務を実行する上で必要なセキュリティ設定が適用されます。

ユーザーロールは、特定の管理グループのデバイスのユーザーに関連付けることができます。

ユーザーロールの対象範囲

*ユーザーロールの対象範囲*は、「ユーザーへの割り当て」と「管理グループへの関連付け」の 2 つの要素の組み合わせとして定義されます。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

ロールを使用する利点

ロールを使用する利点として、管理対象デバイスごとあるいはユーザーごとに個別にセキュリティ設定を指定しなくて済む点があります。社内のユーザー数とデバイス数は組織の規模に応じて膨大になる場合がありますが、個別のセキュリティ設定を指定すべき担当業務の区分の数はそれほど多くはないはずです。

ポリシーのプロファイルの使用との相違点と関連性

ポリシーのプロファイルは、各カスペルスキー製品に対して個別に作成されているポリシーのプロパティとして指定されています。ロールは、そうした様々なカスペルスキー製品に対して作成されている多数のプロファイルに 1 つのロールを関連付けることができます。つまり、ロールは、特定の種別のユーザーを対象とする複数の製品の設定を一元的に管理する目的で使用できます。

ユーザーアカウントおよびセッションの表示

Kaspersky Security Center では、ユーザーアカウントとアカウントグループを管理できます。次の 2 種類のアカウントをサポートしています。

- 組織の従業員のアカウント。管理サーバーは、組織のネットワークをポーリングする時に、ユーザーのアカウントのデータを取得します。
- 内部ユーザーのアカウントこのアカウントは、仮想管理サーバーの使用時に用いられます。内部ユーザーのアカウントは、Kaspersky Security Center 内でのみ作成および使用されます。

次のいずれかの方法でユーザーアカウントおよびセッションのリストを表示できます。

- メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動します。
- メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］→<デバイス名> リンク →［**全般**］タブ →［**全般**］セクション →［**セッション**］ブロックに移動します。

  ［**セッション**］セクションには、Windows を実行しているデバイス上でアクティブなセッションを持つユーザーアカウントが表示されます。

次の要件が満たされている場合、ユーザーアカウントとセッションのリストが正しく表示されます。

- 管理サーバーと同じバージョン以降のネットワークエージェントを使用します。
- ドメインユーザーのアカウントを表示するために、Active Directory ポーリングが有効になっています。
- Windows を実行している管理対象デバイスでは、［**サーバー**］（**LanmanServer**）サービスが実行されています。

製品機能のアクセス権の設定：ロールベースのアクセス制御

Kaspersky Security Center には、Kaspersky Security Center と管理対象のカスペルスキー製品の機能へロールに基づくアクセスを提供する機能があります。

Kaspersky Security Center ユーザーのアプリケーション機能へのアクセス権は、次のいずれかの方法で設定できます：

- 各ユーザーまたはユーザーグループに対する権限を個別に設定します。
- 事前定義された一連の権限を持つ標準のユーザーロールを作成し、職務の範囲に応じてそれらのロールをユーザーに割り当てる。

ユーザーロールの適用は、アプリケーション機能に対するユーザーのアクセス権を設定する定型的な手順を簡素化および短縮することを目的としています。ロール内のアクセス権は、標準タスクとユーザーの職務範囲に従って設定されます。

ユーザーロールには、それぞれの目的に対応する名前を割り当てることができます。作成できるロール数に制限はありません。

事前定義されたユーザーロールを設定済みの権限セットで使用することも、新しいロールを作成して必要な権限を自分で設定することもできます。

アプリケーション機能へのアクセス権

次の表は、関連するタスク、レポート、設定を管理し、関連するユーザー操作を実行するためのアクセス権を備えた Kaspersky Security Center の機能を示しています。

表に一覧表示されているユーザー操作を実行するには、ユーザーは操作内容の横に指定された権限を有している必要があります。

［**読み取り**］、［**書き込み**］、および［**実行**］の各権限は、あらゆるタスク、レポート、設定に適用されます。これらの権限に加えて、ユーザーは、デバイスの抽出でタスクとレポートおよび設定を管理するため、**デバイスの抽出操作を実行**する権限を持っている必要があります。

一般的な機能：**ACL に関係なくオブジェクトにアクセスする**機能領域は、監査を目的としています。この機能領域でユーザーに**読み取り**権限が付与されると、すべてのオブジェクトに対する完全な**読み取り**アクセス権が付与され、ローカル管理者権限（Linux の場合は root）を使用してネットワークエージェント経由で管理サーバーに接続されたデバイスの選択に対して作成されたタスクを実行できるようになります。これらの権限は、公務を遂行するために権限を必要とする限られたユーザーに慎重に付与することを推奨します。

表にないすべてのタスク、レポート、設定、およびインストールパッケージは、**一般的な機能：基本機能**にあります。

製品機能のアクセス権

機能領域	権限	ユーザー操作：操作を実行するために必要な権限	タスク	レポート	その他
一般的な機能：管理グループの管理	**書き込み**	• デバイスを管理グループに追加：**書き込み** • 管理グループからデバイスを削除：**書き込み** • 管理グループを別の管理グループに追加：**書き込み** • 別の管理グループから管理グループを削除：**書き込み**	なし	なし	なし
一般的な機能：ACL にかかわらずオブジェクトにアクセスする	**読み取り**	すべてのオブジェクトへの読み取り権限の取得：**読み取り**	なし	なし	他の権限によって特定のオブジェクトへの読み取りアクセスが禁止されている場合でも、アクセスは許可されます。
一般的な機能：基本的な機能	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• 仮想サーバーのデバイス移動ルール（作成、変更、または削除）：**書き込み**、**デバイスの選択に対する操作を実行** • モバイル（LWNGT）プロトコルのカスタム証明書の取得：**読み取り** • モバイル（LWNGT）プロトコルのカスタム証明書の取得：**書き込み** • NLA 定義のネットワークリストの取得：**読み取り** • NLA 定義のネットワークリストの追加、変更、または削除：**書き込み** • グループのアクセスコントロールリストの表示：**読み取り** • Kaspersky イベントログの表示：**読み取り**	• ［管理サーバーのリポジトリへのアップデートのダウンロード］ • ［レポートの配信］ • ［インストールパッケージの配布］ • ［セカンダリ管理サーバーへのアプリケーションのリモートインストール］	• ［保護ステータスレポート］ • ［脅威レポート］ • ［感染が多いデバイスのレポート］ • ［定義データベースのステータスレポート］ • ［エラーレポート］ • ［ネットワーク攻撃のレポート］ • ［インストールされているメールシステム保護製品のサマリーレポート］ • ［インストールされている境界防御製品のサマリーレポート］ • ［インストールされているアプリケーションの種別のサマリーレポート］ • ［感染したデバイスのユーザーに関するレポート］ • ［インシデントのレポート］	なし

				• ［イベントのレポート］ • ［ディストリビューションポイントのアクティビティレポート］ • 「セカンダリ管理サーバーのレポート」 • ［デバイスコントロールイベントのレポート］ • ［脆弱性レポート］ • ［ブロック対象アプリケーションのレポート］ • 「ウェブコントロールレポート」 • ［管理対象デバイスの暗号化ステータスレポート］ • ［大容量ストレージデバイスの暗号化ステータスレポート］ • ［ファイル暗号化エラーのレポート］ • ［暗号化されたファイルへのアクセスのブロックに関するレポート］ • ［暗号化されたドライブへのアクセス権に関するレポート］ • 「有効なユーザー権限のレポート」 • ［ユーザー権限のレポート］	
一般的な機能：削除されたオブジェクト	• **読み取り** • **書き込み**	• ごみ箱に削除されたオブジェクトの表示：**読み取り** • ごみ箱からオブジェクトを削除：**書き込み**	なし	なし	なし
一般的な機能：イベント処理	• **イベントの削除** • **イベント通知設定の編集**	• イベント登録設定の変更：**イベントログ設定の編集** • イベント通知設定の変更：**イベント通知設定の編集**	なし	なし	設定： • ウイルスアウトブレイク の設定：ウイルスアウトブレイクイベントの作成に必要なウイルスアウトブレイクの検知数

	• **イベントログ設定の編集** • **書き込み**	• イベントの削除：**イベントの削除**			• ウイルスアウトブレイクの設定：ウイルス検知の評価期間 • データベース内に保存されるイベント数の上限 • 削除されたデバイスからのイベントを保存する期間
一般的な機能：管理サーバー上での操作	• **読み取り** • **書き込み** • **実行** • **オブジェクト ACL の変更** • **デバイスの抽出での操作の実行**	• ネットワークエージェント接続用の管理サーバーのポートを指定：**書き込み** • 管理サーバーで起動した Activation Proxy のポートを指定：**書き込み** • 管理サーバー上で開始したモバイル用の Activation Proxy のポートを指定：**書き込み** • スタンドアロンパッケージの配布用の Web サーバーのポートを指定：**書き込み** • MDM プロファイル配布用の Web サーバーのポートを指定：**書き込み** • Kaspersky Security Center Web コンソール経由で接続するための管理サーバーの SSL ポートを指定：**書き込み** • モバイル接続用の管理サーバーのポートを指定：**書き込み** • 管理サーバーデータベースに記録するイベント数の上限を指定：**書き込み** • 管理サーバーが送信可能なイベント数の上限を指定：**書き込み** • 管理サーバーがイベントを送信できる期間を指定：**書き込み**	• ［管理サーバーデータのバックアップ］ • データベースのメンテナンス	なし	なし
一般的な機能：カスペルスキー製品の導入	• **カスペルスキー製品のパッチの管理** • **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	パッチのインストールの承認または拒否：**カスペルスキー製品のパッチの管理**	なし	• ［仮想管理サーバーによるライセンス使用のレポート］ • ［カスペルスキー製品バージョンレポート］ • ［互換性のないアプリケーションのレポート］ • ［カスペルスキー製品のモジュールアップデートのバージョンに関するレポート］	インストールパッケージ：「カスペルスキー」

				• ［製品導入レポート］	
一般的な機能：ライセンス管理	• **ライセンス情報ファイルのエクスポート** • **書き込み**	• ライセンス情報ファイルのエクスポート：**ライセンス情報ファイルのエクスポート** • 管理サーバーのライセンス設定を変更：**書き込み**	なし	なし	なし
一般的な機能：適用されたレポートの管理	• **読み取り** • **書き込み**	• ACL にかかわらずレポートを作成：**書き込み** • ACL にかかわらずレポートを実行：**読み取り**	なし	なし	なし
一般的な機能：管理サーバーの階層構造	**管理サーバー階層の設定**	セカンダリ管理サーバーの登録、アップデート、または削除：**管理サーバー階層の設定**	なし	なし	なし
一般的な機能：ユーザー権限	**オブジェクト ACL の変更**	• 任意のオブジェクトのセキュリティプロパティの変更：**オブジェクト ACL の変更** • ユーザーロールの管理：**オブジェクト ACL の変更** • 内部ユーザーの管理：**オブジェクト ACL の変更** • セキュリティグループの管理：**オブジェクト ACL の変更** • エイリアスの管理：**オブジェクト ACL の変更**	なし	なし	なし
一般的な機能：仮想管理サーバー	• **仮想管理サーバーの管理** • **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• 仮想管理サーバーのリストの取得：**読み取り** • 仮想管理サーバーに関する情報の取得：**読み取り** • 仮想管理サーバーの作成、更新、または削除：**仮想管理サーバーの管理** • 仮想管理サーバーの別のグループへの移動：**仮想管理サーバーの管理** • 仮想管理サーバーの権限の設定：**仮想管理サーバーの管理**	なし	［サードパーティソフトウェアのアップデートのインストール結果に関するレポート］	なし
全般的な機能：暗号化鍵の管理	**書き込み**	暗号化鍵をインポート：**書き込み**	なし	なし	なし
モバイルデバイス管理：全般	• **新しいデバイスの接続** • **モバイルデバイスへの情報コマンド**	• ライセンス管理サービスの復元データの取得：**読み取り** • ユーザー証明書の削除：**証明書の管理**	なし	なし	なし

	のみの送信 • **モバイルデバイスへのコマンドの送信** • **証明書の管理** • **読み取り** • **書き込み**	• ユーザー証明書の公開部分の取得：**読み取り** • 公開鍵インフラストラクチャが有効になっているかどうかの確認：**読み取り** • 公開鍵インフラストラクチャアカウントの確認：**読み取り** • 公開鍵インフラストラクチャテンプレートの入手：**読み取り** • 拡張キー使用証明書による公開キーインフラストラクチャテンプレートの取得：**読み取り** • 公開鍵インフラストラクチャが取り消されているかどうかの確認：**読み取り** • ユーザー証明書の発行設定の更新：**証明書の管理** • ユーザー証明書の発行設定の取得：**読み取り** • アプリケーション名とバージョンによるパッケージの取得：**読み取り** • ユーザー証明書の設定またはキャンセル：**証明書の管理** • ユーザー証明書の更新：**証明書の管理** • ユーザー証明書タグの設定：**証明書の管理** • MDM インストールパッケージ生成の実行、 MDM インストールパッケージ生成のキャンセル：**新しいデバイスの接続**			
システム管理：接続性	• **RDP セッションの開始** • **既存の RDP セッションへの接続** • **トンネリングの開始** • **デバイスから管理者のワークステーションへのファイルの保存** • **読み取り** • **書き込み**	• デスクトップ共有セッションの作成：**デスクトップ共有セッションの作成権限** • RDPセッションの作成：**既存の RDP セッションへの接続** • トンネルの作成：**トンネリングの開始** • コンテンツネットワークリストの保存：**デバイスから管理者のワークステーションへのファイルの保存**	なし	［デバイスのユーザーに関するレポート］	なし

	• **実行** • **デバイスの抽出での操作の実行**				
システム管理：ハードウェアインベントリ	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• ハードウェアインベントリオブジェクトの取得またはエクスポート：**読み取り** • ハードウェアインベントリオブジェクトの追加、設定、または削除：**書き込み**	なし	• ［ハードウェアレジストリレポート］ • ［設定変更レポート］ • ［ハードウェアレポート］	なし
システム管理：ネットワークアクセスコントロール	• **読み取り** • **書き込み**	• CISCO の設定の表示：**読み取り** • CISCO の設定の変更：**書き込み**	なし	なし	なし
システム管理：オペレーティングシステムの導入	• **PXE サーバーの導入** • **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• PXE サーバーの導入：**PXE サーバーの導入** • PXE サーバーのリストの表示：**読み取り** • PXE クライアントでのインストールプロセスの開始または停止：**実行** • WinPE およびオペレーティングシステムイメージのドライバーの管理：**書き込み**	［基準デバイスの OS イメージに基づくインストールパッケージの作成］	なし	インストールパッケージ：［OS イメージ］
システム管理：脆弱性とパッチ管理	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• サードパーティのパッチプロパティの表示：**読み取り** • サードパーティのパッチプロパティを変更：**書き込み**	• ［Windows Update の同期の実行］ • ［Windows Update 更新プログラムのインストール］ • ［脆弱性の修正］ • ［アップデートのインストールと脆弱性の修正］	［ソフトウェアアップデートレポート］	なし
システム管理：リモートインストール	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• サードパーティの脆弱性とパッチ管理に基づくインストールパッケージのプロパティの表示：**読み取り** • サードパーティの脆弱性とパッチ管理に基づくインストールパッケージのプロパティの変更：**書き込み**	なし	なし	インストールパッケージ： • ［カスタムアプリケーション］ • ［VAPM パッケージ］

システム管理：ソフトウェアインベントリ	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	なし	なし	• ［インストール済みアプリケーションのレポート］ • ［アプリケーションのレジストリ履歴のレポート］ • ［ライセンス認証済みアプリケーショングループのステータスレポート］ • ［サードパーティ製品のライセンスに関するレポート］	なし
システム管理：スクリプトをリモートで実行	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	ユーザーはタスクのプロパティを表示できます：**読み取り** ユーザーはインストールパッケージを作成、削除、または変更できます：**書き込み** ユーザーは［**書き込み**］タスクを実行できます。クライアント Linux デバイスでは、スクリプトはルート権限で実行されます。 ユーザーはタスクを実行したり、実行をスケジュールしたりできます：**実行** ユーザーは選択したデバイスでタスクを実行できます：**デバイスの抽出操作を実行**	「スクリプトをリモートで実行」	なし	なし

事前定義済みのユーザーロール

Kaspersky Security Center のユーザーに割り当てられたユーザーロールによって、アプリケーション機能への一連のアクセス権がユーザーに付与されます。

仮想サーバー上で作成されたユーザーには、管理サーバー上のロールを割り当てることはできません。

事前定義のユーザーロールを設定済みの権限セットで使用することも、新しいロールを作成して必要な権限を自分で設定することもできます。Kaspersky Security Center で利用可能な事前定義済みのユーザーロールの一部は、**監査**、**セキュリティ責任者**、**監督者**などの特定の役職（これらのロールは、バージョン 11 以降の Kaspersky Security Center に設定されています）に関連付けることができます。これらのロールのアクセス権は、関連する役職の標準タスクと職務の範囲に従って事前設定されています。次の表に、役割を特定の職位に関連付ける方法を示します。

特定の職位の役割の例

ロール	コメント
監査	削除されたオブジェクトの表示を含む、すべてのタイプのレポートでのすべての操作、すべての表示操作を許可します（［**削除されたオブジェクト**］領域で［**読み取り**］および［**書き込み**］の許可を付与します）。他の操作は許可されません。このロールは、組織の監査を実行する人に割り当てることができます。
上長・	すべての表示操作を許可します。他の操作は許可されません。組織の IT セキュリティを担当しているセキュリティ責任者やその

監督者	他のマネージャーにこのロールを割り当てることができます。
セキュリティ責任者	すべての表示操作を許可し、レポート管理を許可します。**システム管理**：**接続**領域で制限付きのアクセス許可を付与します。組織の IT セキュリティを担当しているセキュリティ責任者にこのロールを割り当てることができます。

次の表に、事前定義された各ユーザーロールに割り当てられているアクセス権を示します。

事前定義されたユーザーロールのアクセス権

ロール	説明
管理サーバーの管理者	次の機能領域でのすべての操作を許可します： • **一般的な機能**： • **基本機能** • **イベント処理** • **管理サーバーの階層構造** • **仮想管理サーバー** • **システム管理**： • **接続** • **ハードウェアインベントリ** • **ソフトウェアインベントリ** **一般的な機能：暗号化鍵の管理**機能領域における［**読み取り**］と［**書き込み**］の権限を付与します。
管理サーバーのオペレーター	次のすべての機能領域で**読み取り**および**実行**権限を付与します： • **一般的な機能**： • **基本機能** • **仮想管理サーバー** • **システム管理**： • **接続** • **ハードウェアインベントリ** • **ソフトウェアインベントリ**
監査	**一般的な機能**の機能領域で、すべての動作を許可します： • **ACL にかかわらずオブジェクトにアクセスする** • **削除されたオブジェクト** • **適用されたレポートの管理** このロールは、組織の監査を実行する人に割り当てることができます。
インストールの管理者	次の機能領域でのすべての操作を許可します： • **一般的な機能**： • **基本機能** • **カスペルスキー製品の導入** • **ライセンス管理** • **システム管理**： • **オペレーティングシステムの導入：** • **脆弱性とパッチ管理**

	• **リモートインストール** • **ソフトウェアインベントリ** ［**一般的な機能：仮想管理サーバー**］機能領域における**読み取り**と**実行**の権限を付与します。
インストールのオペレーター	次のすべての機能領域で**読み取り**および**実行**権限を付与します： • **一般的な機能**： • **基本機能** • **カスペルスキー製品の導入**（この領域で**カスペルスキー製品のパッチの管理**も許可されます） • **仮想管理サーバー** • **システム管理**： • **オペレーティングシステムの導入：** • **脆弱性とパッチ管理** • **リモートインストール** • **ソフトウェアインベントリ**
Kaspersky Endpoint Security の管理者	次の機能領域でのすべての操作を許可します： • **一般的な機能：基本的な機能** • すべての機能を含む Kaspersky Endpoint Security のエリア **一般的な機能：暗号化鍵の管理**機能領域における［**読み取り**］と［**書き込み**］の権限を付与します。
Kaspersky Endpoint Security オペレーター	次のすべての機能領域で**読み取り**および**実行**権限を付与します： • **一般的な機能：基本的な機能** • すべての機能を含む Kaspersky Endpoint Security のエリア
メインの管理者	次の領域を*除く*、**一般的な機能**の機能領域でのすべての操作を許可します。 • **ACL にかかわらずオブジェクトにアクセスする** • **適用されたレポートの管理** **一般的な機能：暗号化鍵の管理**機能領域における［**読み取り**］と［**書き込み**］の権限を付与します。
メインのオペレーター	次のすべての機能領域で**読み取り**および**実行**（該当する場合）権限を付与します： • **一般的な機能**： • **基本機能** • **削除されたオブジェクト** • **管理サーバー上での操作** • **カスペルスキー製品の導入** • **仮想管理サーバー** • **モバイルデバイス管理：全般** • すべての機能を含む**システム管理** • すべての機能を含む Kaspersky Endpoint Security のエリア
モバイルデバイス管理の管理者	次の機能領域でのすべての操作を許可します： • **一般的な機能：基本的な機能** • **モバイルデバイス管理：全般**
モバイルデバイス管	**一般的な機能**：**基本機能**機能領域で**読み取り**および**実行**権限を付与します。

理のオペレーター	［**モバイルデバイス管理**：**全般**］機能領域における**読み取り**権限と**モバイルデバイスに情報コマンドのみを送信する**権限を付与します。
セキュリティ責任者	［**一般的な機能**］の次の機能領域におけるすべての操作を許可します： • **ACL にかかわらずオブジェクトにアクセスする** • **適用されたレポートの管理** **システム管理：接続**機能領域の［**読み取り**］、［**書き込み**］、［**実行**］、［**デバイスから管理者のワークステーションにファイルを保存**］、［**デバイスの抽出を対象に処理を実行**］の各権限を付与します。 組織の IT セキュリティを担当しているセキュリティ責任者にこのロールを割り当てることができます。
セルフサービスポータルのユーザー	［**モバイルデバイス管理：セルフサービスポータル**］機能領域におけるすべての操作を許可します。この機能は、Kaspersky Security Center のバージョン 11 以降ではサポートされていません。
上長・監督者	［**一般的な機能**：**ACL に依存せずオブジェクトにアクセスする**］と［**一般的な機能**：**適用されたレポートの管理**］の機能領域における**読み取り**権限を付与します。 組織の IT セキュリティを担当しているセキュリティ責任者やその他のマネージャーにこのロールを割り当てることができます。
脆弱性とパッチ管理の管理者	［**一般的な機能**：**基本機能**］および［**システム管理**］（すべての機能を含む）機能領域でのすべての操作を許可します。
脆弱性とパッチ管理機能のオペレーター	［**一般的な機能**：**基本機能**］および［**システム管理**］（すべての機能を含む）機能領域で、**読み取り**および**実行**（該当する場合）の権限を付与します。

特定のオブジェクトへのアクセス権の割り当て

サーバーレベルでのアクセス権の割り当てに加えて、特定のオブジェクト（特定のタスクなど）へのアクセスを構成できます。本製品では、次のオブジェクトタイプへのアクセス権を指定できます：

- 管理グループ
- タスク
- レポート
- デバイスの抽出
- イベントの抽出

特定のオブジェクトへのアクセス権を割り当てるには：

1. オブジェクトタイプに応じて、メインメニューで、対応するセクションに移動します：
   - ［**アセット（デバイス）**］→［**グループ階層構造**］
   - ［**アセット（デバイス）**］→［**タスク**］
   - ［**監視とレポート**］→［**レポート**］
   - ［**アセット（デバイス）**］→［**デバイスの抽出**］
   - ［**監視とレポート**］→［**イベントの抽出**］
2. アクセス権を設定するオブジェクトのプロパティを開きます。
   管理グループまたはタスクのプロパティウィンドウを開くには、オブジェクト名をクリックします。ツールバーのボタンを使用して、他のオブジェクトのプロパティを開くことができます。

3. プロパティウィンドウで、［**アクセス権**］セクションを開きます。

   ユーザーリストが開きます。リストされたユーザーとセキュリティグループには、オブジェクトへのアクセス権があります。既定では、管理グループまたはサーバーの階層を使用する場合、リストとアクセス権は親管理グループまたはプライマリサーバーから継承されます。

4. リストを変更できるようにするには、［**カスタムの権限を使用する**］オプションを有効にします。

5. アクセス権を設定します：

   - リストを変更するには、［**追加**］と［**削除**］を使用します。
   - ユーザーまたはセキュリティグループのアクセス権を指定します。次のいずれかの手順を実行します：
     - アクセス権を手動で指定する場合は、ユーザーまたはセキュリティグループを選択し、［**アクセス権**］をクリックして、アクセス権を指定します。
     - ユーザーまたはセキュリティ グループにユーザーロールを割り当てる場合は、ユーザーまたはセキュリティグループを選択し、［**ロール**］をクリックして、割り当てるロールを選択します。

6. ［**保存**］をクリックします。

オブジェクトへのアクセス権が設定されます。

ユーザーとセキュリティグループへのアクセス権の割り当て

ユーザーおよびセキュリティグループに、Kaspersky Endpoint Security for Linux などの管理サーバーの様々な機能を使用するためのアクセス権を付与できます。

ユーザーまたはセキュリティグループへのアクセス権を割り当てるには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**アクセス権**］タブで、権限を割り当てるユーザーまたはセキュリティグループの名前の横にあるチェックボックスをオンにし、［**アクセス権**］をクリックします。

   複数のユーザーまたはセキュリティグループを同時に選択することはできません。複数のアイテムを選択すると、［**アクセス権**］がオフになります。

3. ユーザーまたはグループの権限セットを構成します：

   a. 管理サーバーまたは他のカスペルスキー製品の機能を含むノードを展開します。

   b. 必要な機能またはアクセス権の横にある［**許可**］または［**拒否**］をオンにします。

      例1：［**製品統合**］ノードの横にある［**許可**］を選択して、アプリケーション統合機能（［**読み取り**］、［**書き込み**］、および［**実行**］）に対する使用可能なすべてのアクセス権をユーザーまたはグループに付与します。

      例2：［**暗号化鍵の管理**］ノードを展開し、［**書き込み**］アクセス許可の横にある［**許可**］をオンにして、ユーザーまたはグループの暗号化鍵管理機能への［**書き込み**］アクセス権を付与します。

4. アクセス権のセットを構成した後、［OK］をクリックします。

ユーザーまたはユーザーグループに対する一連の権限が設定されます。

管理サーバー（または管理グループ）の権限は、次の領域から構成されます。

- 一般的な機能：
  - 管理グループの管理
  - ACL にかかわらずオブジェクトにアクセスする
  - 基本機能
  - 削除されたオブジェクト
  - 暗号化キーの管理
  - イベント処理
  - 管理サーバー上での操作（管理サーバーのプロパティウィンドウのみ）
  - デバイスのタグ
  - カスペルスキー製品の導入
  - ライセンス管理
  - アプリケーションの統合
  - 適用されたレポートの管理
  - 管理サーバーの階層
  - ユーザーのアクセス許可
  - 仮想管理サーバー
- モバイルデバイス管理：
  - 全般
  - セルフサービスポータル
- システム管理：
  - 接続
  - スクリプトをリモートで実行
  - ハードウェアインベントリ
  - ネットワークアクセスコントロール
  - オペレーティングシステムの導入
  - 脆弱性とパッチ管理
  - リモートインストール

- ソフトウェアインベントリ

［**許可**］と［**拒否**］のどちらもオンになっていない場合、アクセス権は［*未定義*］とみなされ、ユーザーに対して明示的に許可ないし拒否されるまでは拒否されます。

ユーザーの権限は次から構成されます：

- ユーザー自身の権限
- ユーザーに割り当てられたすべてのロールの権限
- ユーザーが属するすべてのセキュリティグループの権限
- ユーザーが属するセキュリティグループに割り当てられたすべてのロールの権限

これらの権限のうち1つでも［**拒否**］として設定されている場合、他の権限が許可または未定義でも、ユーザーは該当する権限が拒否されます。

また、ユーザーロールのスコープにユーザーとセキュリティグループを追加して、管理サーバーのさまざまな機能を使用することもできます。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

内部ユーザーのアカウントの追加

ユーザーアカウントを追加する場合は、アカウントに「一般機能：ユーザー権限」機能領域でオブジェクト ACL の変更権限があることを確認してください。

Kaspersky Security Center に新しい内部ユーザーアカウントを追加するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. ［**追加**］をクリックします。
3. ［**ユーザーを追加**］ウィンドウが開いたら、新しいユーザーアカウントの設定を指定します：
   - **名前**
   - **パスワード**
     パスワードは次のルールに従う必要があります：
     - パスワードは、8 文字以上 256 文字以下にしてください。
     - パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
       - アルファベット大文字（A-Z）
       - アルファベット小文字（a-z）
       - 数字（0 - 9）

- 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）

- パスワードに空白文字や Unicode 文字を含めることはできません。また「.」の後に続けて「@」を入力することは避けてください。

入力したパスワードを確認するには、をクリックしてください。

［**ユーザーは初回ログイン時にパスワードを変更する必要があります**］をオンにすると、最初のユーザー認証時にパスワードの変更を強制できます。

4. 変更を保存して、新しいユーザーアカウントの作成を完了します。

新しいユーザーがユーザーリストに追加されます。

セキュリティグループの作成

セキュリティグループを作成するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**グループ**］タブを選択します。
2. ［**追加**］をクリックします。
3. 開いた［**セキュリティグループの作成**］ウィンドウで、新しいセキュリティグループに次の設定を指定します：
   - **グループ名**
   - **説明**
4. ［**保存**］をクリックして変更内容を保存します。

新しいセキュリティグループがグループリストに追加されます。

内部ユーザーのアカウントの編集

ユーザーアカウントを編集する場合は、アカウントに「一般機能：ユーザー権限」機能領域でオブジェクト ACL の変更権限があることを確認してください。

Kaspersky Security Center で内部ユーザーアカウントを編集するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. 編集するユーザーアカウントの名前をクリックします。
3. ユーザー設定ウィンドウが表示されるので、［**全般**］タブで、ユーザーアカウントの設定を変更します：
   - **ユーザーステータス**

必要に応じて、スイッチを［**無効**］に切り替えることで、ユーザーの本製品への接続をブロックできます。たとえば、従業員が退職したあとなどにアカウントを無効化できます。

- **名前**
- **完全名**
- **説明**
- **メールアドレス**
- **電話番号**
- **パスワード**

必要に応じて、次のようにして Kaspersky Security Center へのユーザー接続用の新しいパスワードを設定できます。

a. ［**パスワードの変更**］をクリックし、ユーザーアカウントの新しいパスワードを設定します。
パスワードは次のルールに従う必要があります：

- パスワードは、8 文字以上 256 文字以下にしてください。
- パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
  - アルファベット大文字（A-Z）
  - アルファベット小文字（a-z）
  - 数字（0 - 9）
  - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）
- パスワードに空白文字や Unicode 文字を含めることはできません。また「.」の後に続けて「@」を入力することは避けてください。

入力したパスワードを確認するには、をクリックしてください。

b. 必要に応じて、［**ユーザーは初回ログイン時にパスワードを変更する必要があります**］をオンにして、次回のユーザー認証時にパスワードの変更を強制します。

c. ユーザーアカウントが不正な変更から保護されている場合は、このアカウントを変更する権限があることを確認する必要があります。［**アカウント保護**］ウィンドウで、「一般機能：ユーザー権限」機能領域でオブジェクト ACL の変更権限を持つアカウントの資格情報を指定します。

4. ［**認証セキュリティ**］タブで、このアカウントに対するセキュリティ設定を指定できます。
5. ［**グループ**］タブで、セキュリティグループにユーザーを追加できます。
6. ［**デバイス**］タブで、ユーザーにデバイスを割り当てることができます。
7. ［**ロール**］タブで、ユーザーにロールを割り当てることができます。
8. 変更を保存して、ユーザーアカウントの編集を完了します。

ユーザーのリストにアップデートしたユーザーアカウントが表示されます。

セキュリティグループの編集

セキュリティグループを編集するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**グループ**］タブを選択します。
2. 編集するセキュリティグループの名前をクリックします。
3. 開いたグループ設定ウィンドウで、セキュリティグループの設定を変更します：
   - ［**全般**］タブでは、［**名前**］と［**説明**］設定を変更できます。これらの設定は、内部セキュリティグループのみが使用できます。
   - ［**ユーザー**］タブでは、ユーザーをセキュリティグループに追加できます。この設定は、内部ユーザーおよび内部セキュリティグループのみが使用できます。
   - ［**ロール**］タブで、セキュリティグループにロールを割り当てることができます。
4. ［**保存**］をクリックして変更内容を保存します。

変更はセキュリティグループに適用されます。

ユーザーまたはセキュリティグループへのロールの割り当て

ユーザーまたはセキュリティグループへロールを割り当てるには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］に移動し、［**ユーザー**］または［**グループ**］タブを選択します。
2. ロールを割り当てるユーザーまたはセキュリティグループの名前を選択します。

   複数の名前を選択できます。
3. メニュー行で、［**ロールの割り当て**］をクリックします。

   ロールの割り当てウィザードが開始します。
4. ウィザードの手順に従います：選択したユーザーまたはセキュリティグループに割り当てるロールを選択し、ロールの範囲を選択します。

   ユーザーロールの対象範囲は、「ユーザーへの割り当て」と「管理グループへの関連付け」の 2 つの要素の組み合わせとして定義されます。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

管理サーバーを操作する一連の権限を持つロールは、ユーザー（または複数のユーザー、またはセキュリティグループ）に割り当てられます。ユーザーまたはセキュリティグループのリストで、［**ロール割り当て済み**］列にチェックボックスが表示されます。

仮想サーバー上で作成されたユーザーには、管理サーバー上のロールを割り当てることはできません。

内部セキュリティグループへのユーザーアカウントの追加

内部セキュリティグループに追加できるのは内部ユーザーのアカウントのみです。

ユーザーアカウントを内部セキュリティグループに追加するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. セキュリティグループに追加するユーザーアカウントに隣接するチェックボックスをオンにします。
3. ［**グループの割り当て**］をクリックします。
4. 開いた［**グループの割り当て**］ウィンドウで、ユーザーアカウントを追加するセキュリティグループを選択します。
5. ［**保存**］をクリックします。

ユーザーアカウントがセキュリティグループに追加されます。グループ設定を使用して、内部ユーザーをセキュリティグループに追加することもできます。

デバイスの所有者ユーザーの指定

ユーザーをモバイルデバイスの所有者として割り当てる方法の詳細については、Kaspersky Security for Mobile のヘルプを参照してください。

デバイスの所有者ユーザーを指定するには：

1. 仮想管理サーバーに接続されたデバイスの所有者を割り当てる場合は、まず仮想管理サーバーに切り替えます：
   a. メインメニューで、現在の管理サーバー名の右側にあるシェブロンアイコン（）をクリックします。
   b. 必要な管理サーバーを選択します。
2. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
   ユーザーリストが開きます。現在、仮想管理サーバーに接続している場合、リストには現在の仮想管理サーバーとプライマリ管理サーバーのユーザーが含まれています。
3. デバイスの所有者に割り当てるユーザーアカウントの名前をクリックします。
4. ユーザー設定ウィンドウが表示されたら、［**デバイス**］を選択します。
5. ［**追加**］をクリックします。
6. デバイスリストから、ユーザーに割り当てるデバイスを選択します。

7. ［**OK**］をクリックします。

   選択したデバイスが、ユーザーに割り当てられているデバイスのリストに追加されます。

［**アセット（デバイス）**］→［**管理対象デバイス**］で割り当てるデバイスをクリックし、［**デバイスの所有者の管理**］をクリックする方法でも、同じ処理を実行できます。

ユーザーとセキュリティグループの削除

削除できるのは内部ユーザーまたは内部セキュリティグループのみです。

ユーザーまたはセキュリティグループを削除するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］に移動し、［**ユーザー**］または［**グループ**］タブを選択します。
2. 削除するユーザーまたはセキュリティグループの隣にあるチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**OK**］をクリックします。

   選択したユーザーまたはセキュリティグループが削除されます。

ユーザーアカウントのパスワードを変更する

現在のパスワードの有効期限が近づいている場合、またはよりセキュアなパスワードに変更したい場合は、自分のアカウントまたは他のユーザーアカウントのパスワードを変更する必要がある場合があります。

パスワードは次のルールに従う必要があります：

- パスワードは、8 文字以上 256 文字以下にしてください。
- パスワードでは、次の文字種別のうち 3 つ以上を組み合わせてください。
  - アルファベット大文字（A-Z）
  - アルファベット小文字（a-z）
  - 数字（0 - 9）
  - 特殊文字（@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;）
- パスワードに空白文字や Unicode 文字を含めることはできません。また「.」の後に続けて「@」を入力することは避けてください。

自分のアカウントのパスワードを変更する

アカウントのパスワードを編集するには：

1. メインメニューで、アカウント設定に移動して、［**パスワードの変更**］を選択します。
2. 現在のパスワードを入力し、Kaspersky Security Center への接続用の新しいパスワードを指定します。
   入力したパスワードを確認するには、をクリックしてください。
3. アカウントが不正な変更から保護されている場合は、このアカウントを変更する権限があることを確認する必要があります。［**アカウント保護**］ウィンドウで、「一般機能：ユーザー権限」機能領域で、自分のアカウントまたはオブジェクト ACL の変更権限を持つアカウントの資格情報を指定します。
4. 前の手順で使用したアカウントで二段階認証が有効になっている場合は、モバイルデバイスの認証アプリによって生成されたセキュリティコードを入力します。

内部ユーザーアカウントのパスワードの変更

内部ユーザーアカウントのパスワードを編集するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. 編集するユーザーアカウントの名前をクリックします。
3. 開いたユーザー設定ウィンドウの［**全般**］タブで、［**パスワードの変更**］をクリックします。
4. 新しいパスワードを設定します：Kaspersky Security Center へのユーザー接続用。
   入力したパスワードを確認するには、をクリックしてください。
5. 必要に応じて、［**ユーザーは初回ログイン時にパスワードを変更する必要があります**］をオンにして、次回のユーザー認証時にパスワードの変更を強制します。
6. ユーザーアカウントが不正な変更から保護されている場合は、このアカウントを変更する権限があることを確認する必要があります。［**アカウント保護**］ウィンドウで、「一般機能：ユーザー権限」機能領域でオブジェクト ACL の変更権限を持つアカウントの資格情報を指定します。

サーバーフラグを使用してパスワードを変更するためのオプションを設定します

次のコマンドを使用して、klscflag ユーティリティでパスワードの変更を設定できます：

- パスワードローテーション期間の設定（LP_SplPwdChangePeriodDays フラグ）

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <rotation_period>
  ```

  <rotation_period> は、ユーザーパスワードの有効期限が切れるまでの日数です。可能な値：0～730。パラメータ値が 0 の場合、パスワードのローテーションは無効になります。

- パスワードを変更する必要があることを警告する前の時間を設定する（LP_SplPwdChangeNotificationHours フラグ）

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <warning_time>
  ```

  <warning_time> は、ユーザーパスワードの有効期限が切れるまでの時間です。この間、パスワード変更が必要であることを通知するメッセージが表示されます。可能な値：0～17520。パラメータ値が 0 の場合、警告時間はパスワードローテーション期間の 25% になります。

- 「**ユーザーは初回ログイン時にパスワードを変更する必要があります**」オプション（LP_SplPwdForceChange フラグ）の既定値を指定する

  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <value>

  <value>フラグに設定可能な値：

  1–［**ユーザーは初回ログイン時にパスワードを変更する必要があります**］がオンになっています。

  0–［**ユーザーは初回ログイン時にパスワードを変更する必要があります**］がオフになっています。

現在のフラグ値を表示するには、次のコマンドを実行します。

klscflag.exe -fget -pv klserver -n <flag> -t d

<flag>は、LP_SplPwdChangePeriodDays、LP_SplPwdChangeNotificationHours、または LP_SplPwdForceChange フラグです。

ユーザーロールの作成

ユーザーロールを作成するには：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. ［**追加**］をクリックします。
3. ［**新しいロール名**］ウィンドウが開いたら、新しいロールの名前を入力します。
4. ［**OK**］をクリックして変更を適用します。
5. ロールのプロパティウィンドウが開いたら、ロールの設定を変更します：
   - ［**全般**］タブで、ロール名を編集します。
     事前定義のロールの名前は編集できません。
   - ［**設定**］タブで、ロールの範囲とポリシー、ロールに関連付けられているプロファイルを編集します。
   - ［**アクセス権**］タブで、カスペルスキー製品へのアクセス権を編集します。
6. ［**保存**］をクリックして変更内容を保存します。

ユーザーロールのリストに新しいロールが表示されます。

ユーザーロールの編集

ユーザーロールを編集するには：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. 編集するロールの名前をクリックします。
3. ロールのプロパティウィンドウが開いたら、ロールの設定を変更します：

- ［**全般**］タブで、ロール名を編集します。
  事前定義のロールの名前は編集できません。
- ［**設定**］タブで、ロールの範囲とポリシー、ロールに関連付けられているプロファイルを編集します。
- ［**アクセス権**］タブで、カスペルスキー製品へのアクセス権を編集します。

4. ［**保存**］をクリックして変更内容を保存します。

ユーザーロールのリストに更新したロールが表示されます。

各ユーザーロールの対象範囲の編集

*ユーザーロールの対象範囲*は、「ユーザーへの割り当て」と「管理グループへの関連付け」の 2 つの要素の組み合わせとして定義されます。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

ユーザーロールの対象範囲にユーザー、セキュリティグループ、管理グループを追加するには、次のいずれかの方法を使用できます：

方法 1：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］に移動し、［**ユーザー**］または［**グループ**］タブを選択します。
2. ユーザーロールの対象範囲に追加するユーザーまたはセキュリティグループに隣接するチェックボックスをオンにします。
3. ［**ロールの割り当て**］をクリックします。
   ロールの割り当てウィザードが開始します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
4. ［**ロールの選択**］ステップで、割り当てるユーザーロールを選択します。
5. ［**範囲の定義**］ステップで、ユーザーロールの対象範囲に追加する管理グループを選択します。
6. ［**ロールの割り当て**］をクリックしてウィザードを終了します。

選択したユーザーまたはセキュリティグループと、選択した管理グループが、ユーザーロールの対象範囲に追加されます。

方法 2：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. 対象範囲を指定するロールの名前をクリックします。
3. ロールのプロパティウィンドウが開いたら、［**設定**］タブをクリックします。
4. ［**ロールの対象範囲**］セクションで、［**追加**］をクリックします。

ロールの割り当てウィザードが開始します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

5. ［**範囲の定義**］ステップで、ユーザーロールの対象範囲に追加する管理グループを選択します。

6. ［**ユーザーを選択してください**］ステップで、ユーザーロールの対象範囲に追加するユーザーとセキュリティグループを選択します。

7. ［**ロールの割り当て**］をクリックしてウィザードを終了します。

8. ［**閉じる**］ボタン（）をクリックして、ロールのプロパティウィンドウを閉じます。

選択したユーザーまたはセキュリティグループと、選択した管理グループが、ユーザーロールの対象範囲に追加されます。

方法 3：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
管理サーバーのプロパティウィンドウが開きます。

2. ［**アクセス権**］タブで、権限を割り当てるユーザーとロールスコープのユーザーまたはセキュリティグループの名前の横にあるチェックボックスをオンにし、［**ロール**]クリックします。
複数のユーザーまたはセキュリティグループを同時に選択することはできません。複数のアイテムを選択すると、［**ロール**］ボタンがオフになります。

3. ［**ロール**］ウィンドウで、割り当てたいユーザーとロールを選択し、変更を適用して保存します。
選択したユーザーまたはセキュリティグループが、ユーザーロールの対象範囲に追加されます。

ユーザーロールの削除

ユーザーロールを削除するには：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。

2. 削除するロールに隣接するチェックボックスをオンにします。

3. ［**削除**］をクリックします。

4. 表示されたウィンドウで［**OK**］をクリックします。

選択したユーザーロールが削除されます。

ポリシーのプロファイルとロールの関連付け

ユーザーロールはポリシーのプロファイルに関連付けることができます。この場合、ポリシーのプロファイルの有効化ルールがベースにしているのはロールです：ポリシーのプロファイルは、指定したロールを持つユーザーに対してアクティブにされます。

たとえば、管理グループ内のすべてのデバイスに対して GPS ナビゲーションソフトウェアの使用を禁止するポリシーがあるとします。管理グループ「ユーザー」内に配達担当者が所有するデバイスが 1 台存在しており、そのデバイスでのみ GPS ナビゲーションソフトウェアを使用する必要があるとします。この場合、デバイスの所有者に「配達担当者」ロールを割り当てて、「配達担当者」ロールが割り当てられた所有者のデバイスでのみ使用できるように、GPS ナビゲーションソフトウェアを許可するポリシーのプロファイルを作成できます。その他のポリシー設定はいずれも変更されません。「配達担当者」ロールが割り当てられたユーザーのみが、GPS ナビゲーションソフトウェアを使用できるようになります。後で別の担当者に「配達担当者」ロールを割り当てた場合、その新規担当者も組織のデバイスでナビゲーションソフトウェアを使用できるようになります。同じ管理グループ内の他のデバイスでは、GPS ナビゲーションソフトウェアの使用は禁止されたままになります。

ロールとポリシーのプロファイルを関連付けるには：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. ポリシーのプロファイルと関連付けるロール名をクリックします。
   ロールのプロパティウィンドウの［**全般**］タブが表示されます。
3. ［**設定**］タブを選択して、［**ポリシーとプロファイル**］セクションまでスクロールします。
4. ［**編集**］をクリックします。
5. ロールを関連付けるには：
   - **既存のポリシーのプロファイル**– 該当するポリシー名の横にあるアイコン（▶）をクリックして、ロールを関連付けるプロファイルの横にあるチェックボックスをオンにします。
   - **新しいポリシーのプロファイル**：
     a. プロファイルを作成するポリシーの横にあるチェックボックスをオンにします。
     b. ［**ポリシーのプロファイルの新規作成**］をクリックします。
     c. 新しいプロファイル名を指定して、プロファイルを設定します。
     d. ［**保存**］をクリックします。
     e. 新しいプロファイルの横にあるチェックボックスをオンにします。
6. ［**ロールへの割り当て**］をクリックします。

プロファイルがロールに関連付けられてロールのプロパティに表示されます。担当者が当該ロールに割り当てられているデバイスに対して、プロファイルが自動的に適用されます。

アカウントパスワードの変更

たとえば、ユーザーがローカルアカウントのパスワードを忘れた場合や、定期的なパスワードの変更を実行する場合に、ローカルアカウントのパスワードを変更できます。

ユーザーがアカウントにログインしていない場合でも、パスワードの変更は適用されます。ローカルルートアカウントのパスワードを変更することもできます。

このタスクは Linux デバイスでのみ実行できます。

特定のデバイスでローカルアカウントのパスワードを変更するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。
3. ［**タスク種別**］フィールドで、［**アカウントのパスワードの変更（Linux のみ）**］を選択します。
4. 次のいずれかのオプションをオンにします：

   - **管理グループにタスクを割り当てる**

     任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

     たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

     タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

   - **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

     タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

     特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

   - **デバイスの抽出にタスクを割り当てる**

     デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

     たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

   指定されたデバイスに対して、*アカウントパスワードの変更（Linux のみ）*タスクが作成されます。［**管理グループにタスクを割り当てる**］オプションを選択した場合、タスクはグループ 1 になります。
5. ［**タスク範囲**］ステップで、管理グループ、特定のアドレスを持つデバイス、またはデバイスの抽出を指定します。

   使用可能な設定は、前のステップでオンにしたオプションによって異なります。
6. **アカウント名と新しいパスワードの入力**ステップで、次の設定を指定します：

   - ［**アカウント名**］フィールドに、パスワードを変更するアカウントの名前を指定します。
   - ［**新しいパスワード**］フィールドに、前のフィールドで指定したアカウントに設定するパスワードを指定します。

入力した文字を表示するには、［**表示**］を押し続けます。

- 必要に応じて、［**ワンタイムパスワードとして設定（ユーザーは初回ログイン時にパスワードを変更する必要があります）**］をオンにします。

  - **ワンタイムパスワードとして設定（ユーザーは初回ログイン時にパスワードを変更する必要があります）**

    このチェックボックスをオンにすると、ユーザーは初回のログイン後に新しいパスワードを設定するよう要求されます。

    このチェックボックスをオフにすると、ユーザーは初回のログイン後に新しいパスワードを設定するように要求されません。

    既定では、このチェックボックスはオフです。

7. ［**タスク作成の終了**］ステップで、［**終了**］をクリックしてタスクを作成し、ウィザードを終了します。

   ［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスク設定ウィンドウが表示されます。このウィンドウでは、必要に応じて、タスクのパラメータの確認と変更、またはタスクの開始スケジュールの設定を行うことができます。

8. タスクリストで、作成したタスクを選択し、［**開始**］をクリックします。

   または、タスク設定で指定したスケジュールに従ってタスクが起動するまで待ちます。

アカウントパスワードの変更タスクが完了すると、指定されたデバイス上の指定されたローカルアカウントのパスワードが変更されます。

アカウントパスワード変更タスクが正しく実行されるようにするには、ユーザーデバイスで SELinux を無効にする必要があります。

ローカル管理者権限の取り消し

アカウントからローカル管理者権限を取り消すことができます。これにより、ユーザーアカウントをさらに細かく制御できるようになります。たとえば、1回限りの割り当ての完了後、ローカル管理者の権限を取り消すことができます。

このタスクを実行すると、指定されたローカルアカウントがローカル管理グループに属しているかどうかが確認されます。これらのグループは、ネットワークエージェントのポリシー設定で定義されます。ネットワークエージェントのポリシー設定で、ローカル管理グループのリストをカスタマイズできます。**特権付きのデバイスのユーザーに関するレポート（Linux のみ）**を使用して、特権ユーザーアカウントのリストを確認することもできます。

このタスクは Linux デバイスでのみ実行できます。

特定のデバイスのローカル管理者権限を取り消すには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。

3. ［**タスク種別**］フィールドで、［**ローカル管理者権限の取り消し（Linux のみ）**］を選択します。

4. 次のいずれかのオプションをオンにします：

- **管理グループにタスクを割り当てる**

  任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

  たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

  タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクプロパティウィンドウに［**セキュリティ**］タブは表示されません。

- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

  タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

  特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

- **デバイスの抽出にタスクを割り当てる**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

指定されたデバイスに対して、*ローカル管理者権限の取り消し（Linux のみ）*タスクが作成されます。［**管理グループにタスクを割り当てる**］オプションを選択した場合、タスクはグループ 1 になります。

5. ［**タスク範囲**］ステップで、管理グループ、特定のアドレスを持つデバイス、またはデバイスの抽出を指定します。

   使用可能な設定は、前のステップでオンにしたオプションによって異なります。

6. ウィザードのこのステップでは、次の操作を指定します：

- ［**動作モード**］設定グループで、動作モードを指定します：

  - **アカウントのリストからローカル管理者権限を取り消す**

    このオプションをオンにすると、指定されたローカルアカウントからローカル管理者権限が取り消されます。

    既定では、このオプションがオンです。

  - **アカウントのリストをローカル管理者権限の取り消し対象から除外する**

    このオプションをオンにすると、指定されたアカウントを除くすべてのローカルアカウントからローカル管理者権限が取り消されます。

    既定では、このオプションはオフです。

- ローカルアカウントを指定します：
  - ［**追加**］をクリックします。
  - 開いたウインドウで以下の操作を行います：
    - ［**アカウント名**］フィールドに、ローカルアカウントの名前を指定します。
    - ［**アカウントの処理**］設定グループ（［**アカウントのリストからローカル管理者権限を取り消す**］がオンの場合のみ使用可能）で、操作を指定します。
    - **アカウントを保持する**

      このオプションをオンにすると、ローカル管理者権限が取り消された後もローカルアカウントは削除されません。

      既定では、このオプションがオンです。
    - **アカウントを削除する**

      このオプションをオンにすると、ローカル管理者権限があるかどうかに関係なく、ローカルアカウントが削除されます。

      既定では、このオプションはオフです。

7. ［**タスク作成の終了**］ステップで、［**終了**］をクリックしてタスクを作成し、ウィザードを終了します。

   ［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスク設定ウィンドウが表示されます。このウィンドウでは、必要に応じて、タスクのパラメータの確認と変更、またはタスクの開始スケジュールの設定を行うことができます。

8. タスクリストで、作成したタスクを選択し、［**開始**］をクリックします。

   または、タスク設定で指定したスケジュールに従ってタスクが起動するまで待ちます。

ローカル管理者権限の取り消しタスクが完了すると、指定されたデバイス上の指定されたローカルアカウントからローカル管理者権限が取り消されます。

オブジェクトリビジョンの管理

このセクションでは、オブジェクトのリビジョン管理について説明します。Kaspersky Security Center では、オブジェクトの変更を追跡できます。オブジェクトに変更を加えるたびに、*リビジョン*が作成されます。各リビジョンには番号が付いています。

リビジョン管理に対応するアプリケーションオブジェクトは次の通りです：

- 管理サーバーのプロパティ
- ポリシー
- タスク
- 管理グループ
- ユーザーアカウント

- インストールパッケージ

オブジェクトのリビジョンには次の処理を行うことができます：

- 選択したリビジョンを表示する（ポリシーに対してのみ使用可能）
- オブジェクトに対して行った変更を、選択したリビジョンにロールバックする
- リビジョンを JSON ファイルとして保存する（ポリシーに対してのみ使用可能）

リビジョン管理に対応するオブジェクトのプロパティウィンドウの［**変更履歴**］セクションには、オブジェクトのリビジョンのリストが次の詳細とともに表示されます：

- **リビジョン**ーオブジェクトのリビジョン番号
- **時間**ーオブジェクトが変更された日時
- **ユーザー**ーオブジェクトを変更したユーザーの名前
- **ユーザーデバイスの IP アドレス**ーオブジェクトが変更されたデバイスの IP アドレス。
- **Web コンソールの IP アドレス**ーオブジェクトが変更された Kaspersky Security Center Web コンソールの IP アドレス。
- **処理**ーオブジェクトに対する操作
- **説明**ーオブジェクト設定に対して行われた変更に関連するリビジョンの説明

  既定では、オブジェクトのリビジョンの説明は空になっています。リビジョンに説明を追加するには、関連するリビジョンを選択して、［**説明の編集**］をクリックします。［説明］ウィンドウで、リビジョンの説明を入力します。

以前のリビジョンへのオブジェクトのロールバック

必要に応じて、オブジェクトの変更をロールバックできます。たとえば、ポリシーの設定を特定の日付の状態まで戻さなければならない場合があります。

オブジェクトの変更をロールバックするには：

1. オブジェクトのプロパティウィンドウで［**変更履歴**］タブを表示します。
2. オブジェクトのリビジョンのリストで、変更のロールバック先となるリビジョンを選択します。
3. ［**ロールバック**］をクリックします。
4. ［OK］をクリックして処理内容を確定します。

オブジェクトが、選択したリビジョンにロールバックされます。オブジェクトのリビジョンのリストには、実行された処理の記録が表示されます。リビジョンの説明には、オブジェクトを元に戻したリビジョン番号に関する情報が表示されます。

ロールバック操作は、ポリシーオブジェクトとタスクオブジェクトでのみ使用できます。

リビジョンの説明の追加

Kaspersky Security Center では、オブジェクトの変更を追跡できます。オブジェクトに変更を加えるたびに、リビジョンが作成されます。各リビジョンには番号が付いています。

リスト内でリビジョンが検索しやすくなるように、リビジョンに説明を追加することができます。

リビジョンに説明を追加するには：

1. オブジェクトのプロパティウィンドウで［**変更履歴**］タブを表示します。
2. オブジェクトのリビジョンのリストから、説明を追加するリビジョンを選択します。
3. ［**説明の編集**］をクリックします。
   ［**説明**］ウィンドウが開きます。
4. ［**説明**］ウィンドウで、リビジョンの説明を入力します。
   既定では、オブジェクトのリビジョンの説明は空になっています。
5. リビジョンの説明を保存します。

オブジェクトのリビジョンに説明が追加されます。

ポリシーレビジョンの表示と保存

Kaspersky Security Center では、一定期間にポリシーにどのような変更が加えられたかを確認したり、これらの変更に関する情報をファイルに保存したりできます。

対応する管理 Web プラグインがこの機能をサポートしている場合、ポリシーリビジョンの表示と保存が可能です。

ポリシーリビジョンを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. 表示したいリビジョンのポリシーをクリックし、［**変更履歴**］セクションに移動します。
3. ポリシーリビジョンのリストで、表示したいリビジョンの番号をクリックします。
   リビジョンのサイズが 10 MB を超える場合、Kaspersky Security Center Web コンソールを使用して表示することはできません。選択したリビジョンを JSON ファイルに保存するように要求されます。
   リビジョンサイズが 10 MB を超えない場合、選択したポリシーリビジョンの設定を含む HTML 形式のレポートが表示されます。レポートはポップアップウィンドウに表示されるため、ブラウザーでポップアップが許可されていることを確認してください。

ポリシーリビジョンを JSON ファイルに保存するには、

ポリシーリビジョンのリストで、保存するリビジョンを選択し、［**ファイルに保存**］をクリックします。

リビジョンが JSON ファイルに保存されます。

オブジェクトの削除

このセクションでは、オブジェクトの削除と、削除後にオブジェクトの情報を表示する方法について説明します。

次のオブジェクトを削除できます：

- ポリシー
- タスク
- インストールパッケージ
- 仮想管理サーバー
- ユーザー
- セキュリティグループ
- 管理グループ

オブジェクトを削除しても、オブジェクトの情報はデータベースに保存されます。削除されたオブジェクトの情報の保存期間は、オブジェクトの履歴の保存期間（推奨期間は 90 日）と同じです。［**削除されたオブジェクト**］領域の権限で**変更**権限を付与されたユーザーのみが、保存期間を変更できます。

クライアントデバイスの削除について

管理グループから管理対象デバイスを削除すると、アプリケーションはそのデバイスを未割り当てデバイスグループに移動します。デバイスの削除後、インストールされているカスペルスキー製品（ネットワークエージェント、Kaspersky Endpoint Security などのセキュリティ製品）はデバイス上に残ります。

Kaspersky Security Center は、次のルールに従って、未割り当てデバイスグループ内のデバイスを処理します：

- デバイス移動ルールを設定しており、デバイスが移動ルールの基準を満たしている場合、デバイスはルールに従って管理グループに自動的に移動されます。
- デバイスは未割り当てデバイスグループに保存され、デバイス保持ルールに従ってグループから自動的に削除されます。

  デバイスの保持ルールは、ディスク全体の暗号化で暗号化された1つ以上のドライブを備えたデバイスには影響しません。このようなデバイスは自動的に削除されず、手動でのみ削除できます。暗号化されたドライブを含むデバイスを削除する必要がある場合は、まずドライブを復号化してから、デバイスを削除します。

  > 暗号化されたドライブを含むデバイスを削除すると、ドライブの復号化に必要なデータも削除されます。このようなデバイス（［Unassigned devices**未割り当てデバイス**Managed Devices**管理対象デバイス**リスクを理解した上で、選択したデバイスを削除します］をオンにした場合は、その後のデータ削除を認識していることを意味します。

  ドライブを復号化するには、次の条件を満たす必要があります：

- デバイスは管理サーバーに再接続され、ドライブの復号化に必要なデータが復元されます。
- デバイスのユーザーは復号化パスワードを覚えています。
- ドライブの暗号化に使用されたセキュリティ製品（Kaspersky Endpoint Security for Windows など）は、デバイスにまだインストールされています。

ドライブが Kaspersky Disk Encryption 技術によって暗号化されている場合は、FDERT 復元ユーティリティを使用してデータの回復を試行することもできます。

未割り当てデバイスグループからデバイスを手動で削除すると、アプリケーションはそのデバイスをリストから削除します。デバイスを削除した後、インストールされているカスペルスキー製品はデバイス上に残ります。その後、デバイスがまだ管理サーバーに表示されており、定期的なネットワークポーリングを設定している場合、Kaspersky Security Center はネットワークポーリング中にデバイスを検出し、未割り当てデバイスグループに追加します。したがって、デバイスが管理サーバーに表示されない場合にのみ、デバイスを手動で削除することが合理的です。

Kaspersky Security Network（KSN）

このセクションでは、Kaspersky Security Network（KSN）というオンラインサービスのインフラストラクチャの使用方法を説明します。KSN の詳細、および KSN を有効にする方法、KSN へのアクセスの設定方法、KSN プロキシサーバーの使用の統計を表示する方法を説明します。

アップデート機能（ウイルス対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

KSN について

Kaspersky Security Network（KSN）は、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのナレッジベースへのオンラインアクセスを提供するオンラインサービスの基盤です。Kaspersky Security Network のデータを使用することにより、脅威に対するカスペルスキー製品の対応が迅速化され、一部の保護コンポーネントの効果が高まり、誤検知のリスクが低減されます。KSN によって、カスペルスキーの評価データベースを使用して、管理対象デバイスにインストールされたアプリケーションの情報を取得できます。

Kaspersky Security Center は、次のインフラストラクチャソリューションをサポートしています：

- *KSN*：Kaspersky Security Network との情報交換を可能にするソリューションです。KSN に参加すると、Kaspersky Security Center によって管理されるクライアントデバイス上にインストールされたカスペルスキー製品の動作に関する情報を、自動的にカスペルスキーに送信することに同意したことになります。情報は、現在の KSN アクセス設定に従って転送されます。カスペルスキーのアナリストは、受け取った情報をさらに分析し、Kaspersky Security Network の評価および統計データベースに追加します。Kaspersky Security Center は既定でこのソリューションを使用します。
- *Kaspersky Private Security Network（KPSN）*：カスペルスキー製品がインストールされたデバイスのユーザーが、自分のコンピューターからグローバル KSN にデータを送信することなく、Kaspersky Security Network の定義データベースやその他の統計データにアクセスすることを可能にするソリューションです。KPSN は、次のいずれかの理由で Kaspersky Security Network にアクセスできない法人ユーザーの方を対象として開発されています：

- ユーザーデバイスがインターネットに接続されていない。
- 国外や企業 LAN の外へのデータの送信が、法律で禁止されているか社内のセキュリティポリシーで制限されている。

管理サーバーのプロパティウィンドウの［**KSN プロキシ設定**］セクションで、Kaspersky Private Security Network のアクセス設定をセットアップできます。

クイックスタートウィザードの実行時には、KSN に参加するよう促されます。アプリケーションの使用時であればいつでも、KSN の使用を開始または停止できます。

お客様は KSN を有効にする際に同意した KSN に関する声明に従って KSN を使用するものとします。KSN 声明が更新された場合は、管理サーバーのバージョンをアップグレードする際に更新された声明が表示されます。更新された KSN に関する声明に同意することも拒否することも可能です。拒否した場合は、以前に同意した KSN 声明の以前のバージョンの内容に従って KSN の使用が継続されます。

KSN が有効になっている場合、Kaspersky Security Center は KSN サーバーがアクセス可能であるかどうかを確認します。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。これは、管理対象デバイスのセキュリティレベルを確実に管理するために必要です。

管理サーバーが管理するクライアントデバイスは、KSN プロキシサーバーを使用して KSN と対話します。KSN プロキシサーバーは次の機能を提供します：

- クライアントデバイスは、インターネットに直接アクセスできない場合でも、KSN に要求を送信し、KSN から情報を取得し、KSN に情報を転送することができます。
- KSN プロキシサーバーでは処理データをキャッシュに保存するため、送信チャネルの負荷が軽減され、クライアントデバイスから要求された情報を待つ時間が短縮されます。

［管理サーバーのプロパティ］ウィンドウの［**KSN プロキシ設定**］セクションで、KSN プロキシサーバーを設定できます。

KSN へのアクセスの設定

Kaspersky Security Network（KSN）へのアクセスを管理サーバーとディストリビューションポイントで設定できます。

KSN への管理サーバーのアクセスを設定するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**KSN プロキシ設定**］セクションを選択します。
3. 切り替えスイッチを［**KSN プロキシの管理サーバーでの有効化が［有効］です**］の位置まで移動します。

   このオプションをオンにすると、KSN プロキシサーバーはデータを KSN に送信し、Kaspersky Security Center コンポーネントの効率を高め、カスペルスキー製品のパフォーマンスを向上させます。クライアントデバイスでアクティブな Kaspersky Endpoint Security のポリシーに従って、クライアントデバイスから KSN にデータが送信されます。このスイッチをオフにすると、Kaspersky Security Center を経由して、管理サーバーおよびクライアントデバイスから KSN にデータが送信されなくなります。しかし、クライアントデバイスが、個々の設定に従って KSN に直接（Kaspersky Security Center を経由せずに）データを送信することがあります。クライアントデバイス上でアクティブな Kaspersky Endpoint Security ポリシーによって、それらのデバイスから直接（Kaspersky Security Center を経由せずに）KSN に送信するデータが決定されます。

4. スイッチを［**Kaspersky Security Network の使用が［有効］です**］の位置まで移動します。

   このオプションをオンにすると、クライアントデバイスがパッチのインストール結果をカスペルスキーに送信します。このオプションをオンにする際には、必ず KSN 声明の条項を読み、それに同意する必要があります。

   KPSN を使用している場合、スイッチを［**Kaspersky Private Security Network の使用が［有効］です**］の位置まで移動し、［**KSN プロキシの設定ファイルを選択**］をクリックして、KPSN の設定をダウンロードします（拡張子 pkcs7、pem のファイル）。設定のダウンロード後、インターフェイスにはプロバイダー名と連絡先が表示されます。また、KPSN が設定されたファイルの作成日も表示されます。

   > KPSN を有効にする場合、以前の設定で KSN リクエストを直接 KSN クラウドに送信するように指定していたディストリビューションポイントに注意してください。バージョン 11 以前のネットワークエージェントをインストールしているディストリビューションポイントでは、引き続き KSN リクエストを KSN クラウドに送信します。これらのディストリビューションポイントで KSN リクエストを KPSN に送信するように設定を編集するには、［**KSN リクエストを管理サーバーに転送する**］をオンにします。このオプションは、ディストリビューションポイントのプロパティまたはネットワークエージェントのポリシーでオンにできます。

   スイッチを［**Kaspersky Private Security Network の使用が［有効］です**］の位置まで移動すると、KPSN に関する詳細のメッセージが表示されます。

   以下のカスペルスキー製品が KPSN をサポートします：

   - Kaspersky Security Center
   - Kaspersky Endpoint Security for Windows
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
   - Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

   Kaspersky Security Center で KPSN をオンにすると、これらのカスペルスキー製品は KPSN の使用に関する通知を受け取ります。アプリケーション設定ウィンドウの［**先進の脅威対策**］セクションで、［**Kaspersky Security Network**］サブセクションに選択された KSN プロバイダーの情報が以下のように表示されています：KSN または KPSN。

   > KPSN を運用していて、Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 より前のバージョンまたは Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent より前のバージョンを使用する場合、KPSN の使用を無効にしたセカンダリ管理サーバーを使用してください。

   > 管理サーバーのプロパティウィンドウの［**KSN プロキシ設定**］セクションで KPSN が設定されている場合、Kaspersky Security Center は Kaspersky Security Network に統計データを送信しません。

5. 管理サーバーのプロパティでプロキシサーバー設定を構成済みだけれどもネットワークアーキテクチャで KPSN を直接使用する必要がある場合は、［**KPSN への接続時に プロキシサーバーの設定を無視する**］をオンにします。このオプションをオンにしないと、管理対象アプリケーションからのリクエストが KPSN に到達できません。

6. 管理サーバーの KSN プロキシサービスへの接続を設定します：

   - ［**接続設定**］の［**TCP ポート**］で、KSN プロキシサーバーへの接続に使用する TCP ポートの番号を指定します。KSN プロキシサーバーに接続する既定のポートは 13111 です。

- UDP ポートを経由して KSN プロキシサーバーと管理サーバーを接続する場合は、［**UDP ポートを使用する**］をオンにして、［**UDP ポート**］でポート番号を指定します。既定では、このオプションはオフで、TCP ポートが使用されます。KSN プロキシサーバーに接続する既定の UDP ポートは 15111 です。

- 管理サーバーが HTTPS ポート経由で KSN プロキシサーバーに接続する場合は、［**HTTPS を使用する**］をオンにし、［**HTTPS の使用時に経由するポート**］の番号を指定します。既定では、このオプションはオフで、TCP ポートが使用されます。このオプションがオンの場合、KSN プロキシサーバーに接続する既定の HTTPS ポートは 17111 です。

7. トグルスイッチを［**プライマリ管理サーバー経由でのセカンダリ管理サーバーと KSN の接続が［有効］です**］の位置まで移動します。

   このオプションをオンにすると、セカンダリ管理サーバーはプライマリ管理サーバーを KSN プロキシサーバーとして使用します。このオプションをオフにすると、セカンダリ管理サーバーは直接 KSN に接続します。その場合、管理対象デバイスはセカンダリ管理サーバーを KSN プロキシサーバーとして使用します。

   > セカンダリ管理サーバーのプロパティの［**KSN プロキシ設定**］セクションの右側で［**KSN プロキシの管理サーバーでの有効化が［有効］です**］の切り替えスイッチが有効の位置にある場合、セカンダリ管理サーバーはプライマリ管理サーバーをプロキシサーバーとして使用します。

8. ［**保存**］をクリックします。

KSN のアクセス設定が保存されます。

管理サーバーの負荷を軽減したい場合などに、ディストリビューションポイントから KSN へのアクセスを設定できます。KSN プロキシサーバーとして動作しているディストリビューションポイントは、管理サーバーを使用せずに、管理対象デバイスからの KSN リクエストをカスペルスキーに直接送信します。

Kaspersky Security Network（KSN）へのディストリビューションポイントのアクセスを設定するには：

1. ディストリビューションポイントが手動で割り当てられていることを確認します。

2. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（ ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

3. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。

4. ディストリビューションポイントの名前をクリックし、プロパティウィンドウを開きます。

5. ［**KSN プロキシ**］のディストリビューションポイントのプロパティウィンドウで［**ディストリビューションポイントで KSN プロキシを有効にする**］をオンにしてから［**インターネット経由で直接 KSN クラウド / KPSN にアクセスする**］をオンにします。

6. ［**OK**］をクリックします。

ディストリビューションポイントが KSN プロキシサーバーとして動作します。

KSN の使用の有効化と無効化

KSN の使用を有効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（ ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**KSN プロキシ設定**］セクションを選択します。

3. 切り替えスイッチを［**KSN プロキシの管理サーバーでの有効化が［有効］です**］の位置まで移動します。

KSN プロキシサーバーが有効になり、データを KSN に送信して、Kaspersky Security Center コンポーネントの効率を高め、カスペルスキー製品のパフォーマンスを向上させます。

1. 使用している KSN インフラストラクチャソリューションに応じて、対応するスイッチを有効にします。

   - グローバル KSN を使用している場合は、スイッチを［**Kaspersky Security Network の使用が［有効］です**］の位置まで移動します。

     KSN へのデータ送信が可能になりました。このオプションをオンにする際には、必ず KSN 声明の条項を読み、それに同意する必要があります。

   - KPSN を使用している場合、スイッチを［**Kaspersky Private Security Network の使用が［有効］です**］の位置まで移動し、［**KSN プロキシの設定ファイルを選択**］をクリックして、KPSN の設定をダウンロードします（拡張子 pkcs7、pem のファイル）。設定のダウンロード後、インターフェイスにはプロバイダー名と連絡先が表示されます。また、KPSN が設定されたファイルの作成日も表示されます。

     スイッチを［**Kaspersky Private Security Network の使用が［有効］です**］の位置まで移動すると、KPSN に関する詳細のメッセージが表示されます。

2. ［**保存**］をクリックします。

KSN の使用を無効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**KSN プロキシ設定**］セクションを選択します。

3. KSN プロキシサービスを無効にするには、スイッチを［**KSN プロキシの管理サーバーでの有効化が［無効］です**］の位置に切り替えます。

4. ［**保存**］をクリックします。

同意した KSN に関する声明の表示

Kaspersky Security Network (KSN) を有効にする際には、KSN に関する声明を読み、同意する必要があります。同意した KSN に関する声明はいつでも表示できます。

同意した KSN に関する声明を表示するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**KSN プロキシ設定**］セクションを選択します。

3. ［**Kaspersky Security Network に関する声明を表示**］をクリックします。

表示されたウィンドウで、同意した KSN に関する声明の内容を表示できます。

更新された KSN に関する声明の同意

お客様は KSN を有効にする際に同意した KSN に関する声明に従って KSN を使用するものとします。KSN 声明が更新された場合は、管理サーバーのバージョンをアップグレードする際に更新された声明が表示されます。更新された KSN に関する声明に同意することも拒否することも可能です。拒否した場合は、以前に同意した KSN 声明の以前のバージョンの内容に従って KSN の使用が継続されます。

管理サーバーのバージョンをアップグレードすると、更新された KSN 声明が自動的に表示されます。更新された KSN に関する声明を拒否した場合でも、後で表示して同意することができます。

更新された KSN 声明を表示して同意するには：

1. 製品のメインウィンドウの右上部にある[**通知の表示**]をクリックします。
   ［**通知**］ウィンドウが開きます。
2. ［**更新された KSN 声明を表示**］をクリックします。
   ［**Kaspersky Security Network に関する声明の更新**］ウィンドウが開きます。
3. KSN に関する声明を読み、次のうち 1 つを選択して対応を判断します：
   - **更新された KSN 声明の内容に同意する**
   - **更新前の声明の内容に従って KSN を使用する**

   選択に応じて、KSN は更新前の、もしくは更新された KSN 声明の規約に従い動作します。管理サーバーのプロパティからいつでも同意した KSN 声明の本文を表示できます。

ディストリビューションポイントが KSN プロキシサーバーとして機能するかどうかの確認

ディストリビューションポイントとして機能するように割り当てられた管理対象デバイスで、KSN プロキシサーバーを有効にできます。ksnproxy サービスがデバイスで実行されている場合、管理対象デバイスは KSN プロキシサーバーとして機能します。デバイスでこのサービスをローカルで確認し、オンまたはオフにできます。

Windows ベースまたは Linux ベースのデバイスをディストリビューションポイントとして割り当てることができます。ディストリビューションポイントのチェック方法は、このディストリビューションポイントのオペレーティングシステムによって異なります。

Windows ベースのディストリビューションポイントが KSN プロキシサーバーとして機能するかどうかを確認するには：

1. ディストリビューションポイントデバイスの Windows で、［**サービス**］（［**すべてのプログラム**］→［**管理ツール**］→［**サービス**］）を開きます。
2. サービスのリストで、ksnproxy サービスが実行されているかを確認します。
   ksnproxy サービスが実行されている場合、デバイス上のネットワークエージェントは Kaspersky Security Network に参加し、ディストリビューションポイントの範囲に含まれる管理対象デバイスの KSN プロキシサーバーとして機能します。

必要に応じて ksnproxy サービスをオフにできます。この場合、ディストリビューションポイントのネットワークエージェントは Kaspersky Security Network への参加を停止します。この操作にはローカル管理者権限が必要です。

Linux ベースのディストリビューションポイントが KSN プロキシサーバーとして機能するかどうかを確認するには：

1. ディストリビューションポイントのデバイスで、実行中のプロセスの一覧を表示します。
2. 実行中のプロセスのリストで、`/opt/kaspersky/ksc64/sbin/ksnproxy` プロセスが実行されているかどうかを確認します。

`/opt/kaspersky/ksc64/sbin/ksnproxy` プロセスが実行されている場合、デバイス上のネットワークエージェントは Kaspersky Security Network に参加し、ディストリビューションポイントの範囲に含まれる管理対象デバイスの KSN プロキシサーバーとして機能します。

Kaspersky Security Center および管理対象セキュリティ製品のアップグレードのシナリオ

Kaspersky Security Center の主要な導入シナリオの概要および管理対象セキュリティ製品のアップグレードについて説明します。

Kaspersky Security Center と管理対象アプリケーションのアップデートは、以下の手順で進みます：

1. **ハードウェアとソフトウェアの要件を確認する**

   ハードウェアが要件を満たしていることを確認し、必要なアップデートをインストールしてください。

2. **リソース計画**

   データベースがどの程度ディスク容量を使用するのかを見積もります。管理サーバーの設定とデータベースのバックアップコピーを保存するのに十分な空き容量があるかどうかを確認します。

3. **Kaspersky Security Center のインストーラーファイルの取得**

   最新バージョンの Kaspersky Security Center の実行ファイルを取得し、管理サーバーとして動作させる予定のデバイスに保存します。使用する Kaspersky Security Center のバージョンのリリースノートの内容を確認します。

4. **以前のバージョンのバックアップコピーの作成**

   データバックアップと復元用のユーティリティを使用して、管理サーバーのデータのバックアップコピーを作成します。バックアップタスクの作成も可能です。

   インストールされているプラグインのリストをエクスポートすることを推奨します。

5. **インストーラーの実行**

   Kaspersky Security Center の最新バージョンの実行ファイルを実行します。ファイルの実行時に、バックアップコピーを保有していることをウィザード内で指定し、ファイルの場所も指定します。バックアップからデータが復元されます。

6. **管理対象アプリケーションのアップグレード**

   より新しいバージョンが利用可能な場合、アプリケーションをアップグレードできます。サポート対象に含まれるカスペルスキー製品のリストを確認し、Kaspersky Security Center のバージョンが対象アプリケーションと互換性があるかどうかを確認します。確認後、リリースノートの説明に従ってアプリケーションのアップグレードを実行します。

結果

アップグレード手順が完了したら、Microsoft Management Console に新しいバージョンの管理サーバーがインストールされていることを確認します。［**ヘルプ**］→［**Kaspersky Security Center のバージョン情報**］の順にクリックします。バージョン情報が表示されます。

アップグレード後の新しいバージョンの管理サーバーが使用されていることを、Kaspersky Security Center Web コンソールから確認するには、ウィンドウ上部の管理サーバー名の横にある設定アイコン（ ）をクリックします。管理サーバーのプロパティウィンドウが表示されるので、［**全般**］タブの［**全般**］セクションに移動します。バージョン情報が表示されます。

管理サーバーのデータを回復する必要がある場合は、「対話モードでのデータのバックアップと回復」のトピックで説明されている手順に従います。

管理対象セキュリティ製品をアップグレードした場合は、それが管理対象デバイスに正しくインストールされていることを確認します。詳細については、該当する各製品のドキュメントを参照してください。

定義データベースとカスペルスキー製品のアップデート

このセクションでは、次の対象の定期的なアップデートに必要な手順について説明します。

- 定義データベースとソフトウェアモジュール
- インストール済みのカスペルスキー製品（Kaspersky Security Center コンポーネントとセキュリティ製品を含む）

アップデート機能（ウイルス対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

シナリオ：定義データベースとカスペルスキー製品の定期的なアップデート

このセクションでは、定義データベース、ソフトウェアモジュール、カスペルスキー製品の定期的なアップデートを行う手順について説明します。ネットワーク保護の設定手順の完了後、管理サーバーと管理対象デバイスがウイルス、ネットワーク攻撃、フィッシング攻撃などの様々な脅威から常に保護されるよう、保護システムの信頼性を維持する必要があります。

ネットワーク保護を最新の状態に維持する定期的なアップデートは次の通りです：

- 定義データベースとソフトウェアモジュール
- インストール済みのカスペルスキー製品（Kaspersky Security Center コンポーネントとセキュリティ製品を含む）

この手順を完了すると、次の状態を実現できます：

- ネットワークが最新のカスペルスキー製品（Kaspersky Security Center コンポーネントとセキュリティ製品を含む）で保護されている。

- ネットワークのセキュリティレベルにとって重要な定義データベースとその他のカスペルスキーのデータベースが常に最新である。

必須条件

管理対象デバイスが管理サーバーに接続している必要があります。接続していない場合は、定義データベース、ソフトウェアモジュール、カスペルスキー製品の手動アップデート、またはカスペルスキーのアップデートサーバーからの直接アップデートを検討してください。

管理サーバーはインターネットに接続している必要があります。

導入を開始する前に、次が完了していることを確認してください：

1. Kaspersky Security Center Web コンソールを使用したカスペルスキー製品の導入手順に従って、カスペルスキーのセキュリティ製品を管理対象デバイスに導入した。
2. ネットワーク保護の設定手順に従って、必要なすべてのポリシー、ポリシーのプロファイル、タスクを作成して設定した。
3. 管理対象デバイスの数とネットワークトポロジーに従って、適切な数のディストリビューションポイントを割り当てた。

定義データベースとカスペルスキー製品のアップデート手順は次の通りです：

1. **アップデートスキームの選択**

   Kaspersky Security Center コンポーネントとセキュリティ製品に対するアップデートのインストールには、複数のスキームを使用できます。ネットワークの要件に最も合致するスキームを選択してください（複数のスキームを組み合わせることもできます）。

2. **［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの作成**

   このタスクは、Kaspersky Security Center のクイックスタートウィザードによって自動的に作成されます。ウィザードを実行していない場合は、次の手順に進む前にタスクを作成してください。

   カスペルスキーのアップデートサーバーから管理サーバーのリポジトリへのアップデートのダウンロード、および定義データベースと Kaspersky Security Center のソフトウェアモジュールのアップデートには、このタスクが必要です。アップデートのダウンロード後、管理対象デバイスにこれらのアップデートを配信できます。

   ネットワークにディストリビューションポイントが割り当てられている場合、アップデートは管理サーバーのリポジトリからディストリビューションポイントのリポジトリに自動的にダウンロードされます。この場合、ディストリビューションポイントの範囲に含まれる管理対象デバイスは、管理サーバーのリポジトリではなくディストリビューションポイントのリポジトリからアップデートをダウンロードします。

   実行手順の説明：

   - 管理コンソール：［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの作成
   - Kaspersky Security Center Web コンソール：管理サーバーのリポジトリへのアップデートのダウンロードタスクの作成

3. **［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの作成（オプション）**

既定では、管理サーバーからディストリビューションポイントにアップデートがダウンロードされます。カスペルスキーのアップデートサーバーからディストリビューションポイントにアップデートを直接ダウンロードするように Kaspersky Security Center を設定できます。ディストリビューションポイントのリポジトリへのダウンロードが推奨されるのは、管理サーバーとディストリビューションポイント間の通信の方がディストリビューションポイントとカスペルスキーのアップデートサーバー間の通信よりも費用がかかる場合や、管理サーバーがインターネットにアクセスできない場合などです。

ネットワークにディストリビューションポイントが割り当てられており、*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクが作成されている場合、ディストリビューションポイントは、管理サーバーのリポジトリではなくカスペルスキーのアップデートサーバーからアップデートをダウンロードします。

実行手順の説明：

- 管理コンソール：ディストリビューションポイントのリポジトリにアップデートをダウンロードタスクの作成
- Kaspersky Security Center Web コンソール：ディストリビューションポイントのリポジトリにアップデートをダウンロードタスクの作成

4 ディストリビューションポイントの設定

ネットワークにディストリビューションポイントが割り当てられている場合、設定が必要なすべてのディストリビューションポイントのプロパティで［**アップデートの配信**］がオンになっていることを確認します。ディストリビューションポイントでこのオプションがオフになっていると、ディストリビューションポイントの範囲に含まれるデバイスは管理サーバーのリポジトリからアップデートをダウンロードします。

管理対象デバイスがディストリビューションポイントからのみアップデートを受信するようにする場合は、ネットワークエージェントポリシーで［**ディストリビューションポイント経由でのみファイルを配信する**］をオンにします。

5 オフライン方式のアップデートのダウンロードまたは差分ファイルの使用によるアップデート処理の最適化（オプション）

オフライン方式のアップデートのダウンロード（既定で有効）または差分ファイルを使用して、アップデート処理を最適化できます。これら 2 つの機能は同時に使用できないため、各ネットワークセグメントでどちらを有効にするか選択する必要があります。

オフライン方式のアップデートのダウンロードを有効にした場合、アップデートが管理サーバーのリポジトリにダウンロードされると、セキュリティ製品がアップデートを要求する前にネットワークエージェントが管理対象デバイスに必要なアップデートをダウンロードします。これによりアップデート処理の信頼性が向上します。この機能を使用するには、［**アップデートと定義データベースをあらかじめ管理サーバーからダウンロードする（推奨）**］をネットワークエージェントのポリシーでオンにします。

オフライン方式のアップデートのダウンロードを使用しない場合は、差分ファイルを使用して管理サーバーと管理対象デバイス間のトラフィックを最適化できます。この機能を有効にすると、管理サーバーまたはディストリビューションポイントは定義データベースまたはソフトウェアモジュールのファイル全体ではなく差分ファイルをダウンロードします。差分ファイルには、定義データベースファイルまたはソフトウェアモジュールファイルの異なる 2 バージョン間の変更点のみが含まれています。したがって、差分ファイルの方がファイル全体より容量が小さくなります。これにより、管理サーバーと管理対象デバイス間またはディストリビューションポイントと管理対象デバイス間のトラフィックを削減できます。この機能を使用するには、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクや、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスク、またはその両方のプロパティで［**差分ファイルのダウンロード**］をオンにします。

実行手順の説明：

- カスペルスキー製品の定義データベースとソフトウェアモジュールのアップデートでの差分ファイルの使用
- 管理コンソール：オフライン方式のアップデートのダウンロードの有効化と無効化
- Kaspersky Security Center Web コンソール：オフライン方式のアップデートのダウンロードの有効化と無効化

6 ダウンロードされたアップデートの検証（オプション）

ダウンロードされたアップデートをインストールする前に、*アップデート検証*タスクを使用してアップデートを検証できます。このタスクでは、設定で指定したテストデバイスを対象に、デバイスアップデートタスクとマルウェアスキャンタスクを順番に実行します。タスクの実行結果に基づいて、管理サーバーは残りのデバイスに対するアップデートの配信を開始またはブロックします。

*アップデート検証*タスクは、*管理サーバーのリポジトリへのアップデートのダウンロード*タスクの一部として実行できます。*管理サーバーのリポジトリへのアップデートのダウンロード*タスクのプロパティで、［**配信前にアップデートを検証する**］（管理コンソールの場合）または［**アップデートの検証の実行**］（Kaspersky Security Center Web コンソールの場合）をオンにします。

実行手順の説明：

- 管理コンソール：ダウンロードされたアップデートの検証
- Kaspersky Security Center Web コンソール：ダウンロードされたアップデートの検証

7 ソフトウェアアップデートの拒否と承認

既定では、ダウンロードされたソフトウェアアップデートのステータスは「*未定義*」です。ステータスは「*承認*」または「*拒否*」に変更できます。承認されたアップデートは常にインストールされます。使用許諾契約書の条項の確認と同意がアップデートに必要な場合は、最初に条項に同意する必要があります。その後、アップデートを管理対象デバイスに配信できます。未定義のアップデートは、ネットワークエージェントポリシーの設定に従って、ネットワークエージェントとその他の Kaspersky Security Center コンポーネントにのみインストールできます。「*拒否*」のステータスを設定したアップデートはデバイスにインストールされません。拒否に設定したセキュリティ製品のアップデートが以前にインストールされている場合、Kaspersky Security Center はすべてのデバイスからのアップデートのアンインストールを試行します。Kaspersky Security Center コンポーネントのアップデートはアンインストールできません。

実行手順の説明：

- 管理コンソール：ソフトウェアアップデートの拒否と承認
- Kaspersky Security Center Web コンソール：ソフトウェアアップデートの拒否と承認

8 Kaspersky Security Center コンポーネントのアップデートとパッチの自動インストールの設定

ネットワークエージェントとその他の Kaspersky Security Center コンポーネント用にダウンロードされたアップデートとパッチは自動的にインストールされます。ネットワークエージェントのプロパティで［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオンのままにした場合、アップデートはすべて、リポジトリにダウンロードされた後に自動的にインストールされます。このオプションをオフにすると、ダウンロードされたパッチのうちステータスが「*未定義*」のものは、管理者がステータスを「*承認*」に変更しない限りインストールされません。

実行手順の説明：

- 管理コンソール：Kaspersky Security Center コンポーネントの自動アップデートおよびパッチ適用の有効化と無効化
- Kaspersky Security Center Web コンソール：Kaspersky Security Center コンポーネントの自動アップデートおよびパッチ適用の有効化と無効化

9 管理サーバーのアップデートのインストール

管理サーバーのソフトウェアアップデートはアップデートのステータスに依存しません。これらのアップデートは自動的にインストールされず、事前に管理コンソールの［**監視**］タブ（［**管理サーバー** <サーバー名>］→［**監視**］）または Kaspersky Security Center Web コンソールの［**通知**］セクション（［**監視とレポート**］→［**通知**］）で管理者によって承認されている必要があります。その後、管理者が明示的にアップデートのインストールを実行する必要があります。

10 セキュリティ製品のアップデートとパッチの自動インストールの設定

管理対象アプリケーションの*アップデート*タスクを作成して、製品、ソフトウェアモジュール、および定義データベースをタイムリーにアップデートします。タイムリーなアップデートを確実に実行するために、タスクスケジュールの設定時に、［**新しいアップデートがリポジトリにダウンロードされ次第**］をオンにすることを推奨します。

ネットワークに IPv6 のみのデバイスが含まれていて、それらのデバイス上にインストールされているセキュリティ製品を定期的にアップデートする場合、管理対象デバイス上にバージョン 14 以降の管理サーバーとバージョン 14 以降のネットワークエージェントがインストールされていることを確認してください。

既定では、アップデートのステータスを*承認*に変更した後にのみ、Kaspersky Endpoint Security for Windows と Kaspersky Endpoint Security for Linux のアップデートがインストールされます。アップデートの設定は、*アップデート*タスクで変更することができます。

使用許諾契約書の条項の確認と同意がアップデートに必要な場合は、最初に条項に同意する必要があります。その後、アップデートを管理対象デバイスに配信できます。

実行手順の説明：

- 管理コンソール：Kaspersky Endpoint Security のアップデートをデバイスに自動インストール
- Kaspersky Security Center Web コンソール：Kaspersky Endpoint Security のアップデートをデバイスに自動インストール

結果

すべての手順を完了すると、管理サーバーのリポジトリまたはディストリビューションポイントのリポジトリにアップデートがダウンロードされた後で、定義データベースとインストール済みのカスペルスキー製品をアップデートするように Kaspersky Security Center が設定されます。続いて、ネットワークステータスの監視を設定できます。

定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデートの概要

管理サーバーと管理対象デバイスの保護が最新の状態であるようにするには、次の項目のタイムリーなアップデートが必要です：

- 定義データベースとソフトウェアモジュール

  Kaspersky Security Center は、カスペルスキーのデータベースとソフトウェアをダウンロードする前にカスペルスキーのサーバーがアクセス可能かどうかをチェックします。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。これは、定義データベースを最新の状態に保ち、管理対象デバイスのセキュリティレベルを確実に管理するために必要です。

- インストール済みのカスペルスキー製品（Kaspersky Security Center コンポーネントとセキュリティ製品を含む）

ネットワークの設定に応じて、管理対象デバイスへの必要なアップデートのダウンロードと配信に次のスキームを使用できます：

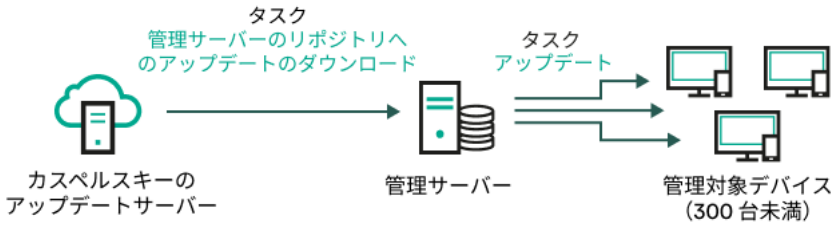
- 単一のタスク［*管理サーバーのリポジトリへのアップデートのダウンロード*］の使用
- 次の 2 つのタスクの使用：
  - *［管理サーバーのリポジトリへのアップデートのダウンロード］タスク*

- *ディストリビューションポイントのリポジトリにアップデートをダウンロードタスク*

- ローカルフォルダー、共有フォルダー、または FTP サーバーを使用して手動で実行
- カスペルスキーのアップデートサーバーから管理対象デバイスの Kaspersky Endpoint Security を直接アップデート
- 管理サーバーがインターネットに接続されていない場合は、ローカルまたはネットワークフォルダー経由

管理サーバーのリポジトリへのアップデートのダウンロードタスクの使用

このスキームでは、Kaspersky Security Center は *管理サーバーのリポジトリへのアップデートのダウンロード* タスクを使用してアップデートをダウンロードします。単一のネットワークセグメントで構成され管理対象デバイスが 300 台未満、または複数のセグメントに分かれているが各ネットワークセグメントに含まれる管理対象デバイスが 10 台未満の小規模ネットワークでは、管理サーバーのリポジトリから管理対象デバイスにアップデートが直接配信されます（次の図を参照）。

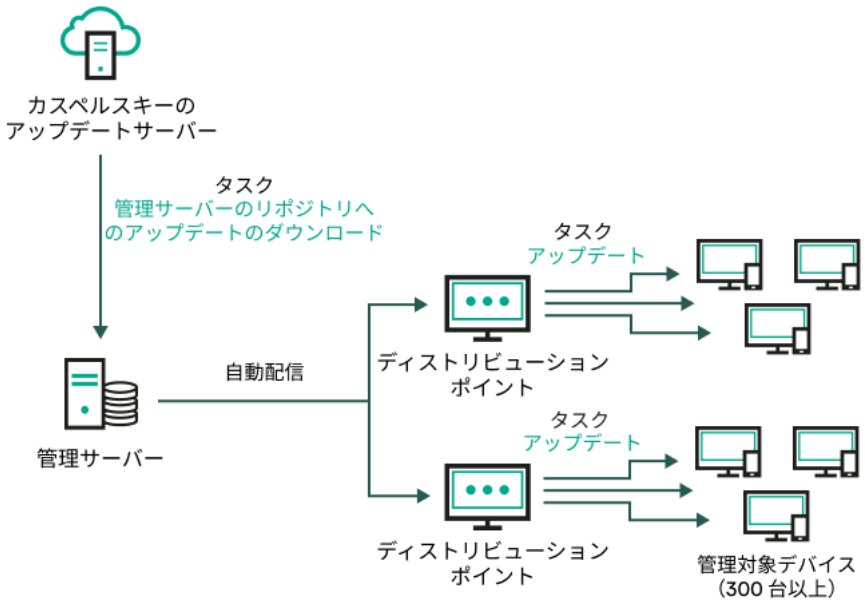


ディストリビューションポイントを使用しない、管理サーバーのリポジトリへのアップデートのダウンロードタスクによるアップデート

既定では、管理サーバーは HTTPS プロトコルを使用してカスペルスキーのアップデートサーバーに接続し、アップデートをダウンロードします。必要に応じて、管理サーバーで HTTPS プロトコルの代わりに HTTP プロトコルを使用するように設定を編集できます。

単一のネットワークセグメントで構成され管理対象デバイスが 300 台以上、または複数のセグメントに分かれていて各ネットワークセグメントに含まれる管理対象デバイスが 10 台以上のネットワークの場合は、ディストリビューションポイントを使用して管理対象デバイスにアップデートを配信することを推奨します（次の図を参照）。ディストリビューションポイントは管理サーバーの負荷を低減し、管理サーバーと管理対象デバイス間のトラフィックを最適化します。ネットワークに必要なディストリビューションポイントの数と設定を計算できます。

このスキームでは、アップデートは管理サーバーのリポジトリからディストリビューションポイントのリポジトリに自動的にダウンロードされます。ディストリビューションポイントの範囲に含まれる管理対象デバイスは、管理サーバーのリポジトリではなくディストリビューションポイントのリポジトリからアップデートをダウンロードします。



ディストリビューションポイントを使用した、管理サーバーのリポジトリへのアップデートのダウンロードタスクによるアップデート

*管理サーバーのリポジトリへのアップデートのダウンロード*タスクが完了すると、管理サーバーのリポジトリに次のアップデートがダウンロードされます：

- 定義データベースと Kaspersky Security Center のソフトウェアモジュール

  これらのアップデートは自動的にインストールされます。

- 管理対象デバイスのセキュリティ製品用の定義データベースとソフトウェアモジュール

  これらのアップデートは、Kaspersky Endpoint Security for Windows のアップデートタスクを使用してインストールされます。

- 管理サーバー用のアップデート

  これらのアップデートは自動的にインストールされません。管理者が明示的にアップデートのインストールを承認して実行する必要があります。

  > 管理サーバーへのパッチのインストールにはローカル管理者権限が必要です。

- Kaspersky Security Center のコンポーネント用のアップデート

  既定では、これらのアップデートは自動的にインストールされます。ネットワークエージェントポリシーで設定を変更できます。

- セキュリティ製品用のアップデート

  既定では、Kaspersky Endpoint Security for Windows はこれらの承認されたアップデートのみをインストールします（管理コンソールまたは Kaspersky Security Center Web コンソールを使用してアップデートを承認できます）。アップデートは*アップデートタスク*を使用してインストールされ、このタスクのプロパティで設定することができます。

> 仮想管理サーバーでは［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクは利用できません。仮想管理サーバーのリポジトリには、プライマリ管理サーバーにダウンロードされたアップデートが表示されます。

テストデバイスを指定してアップデートの動作とエラーが検証されるように設定できます。検証に成功すると、アップデートが他の管理対象デバイスに配信されます。

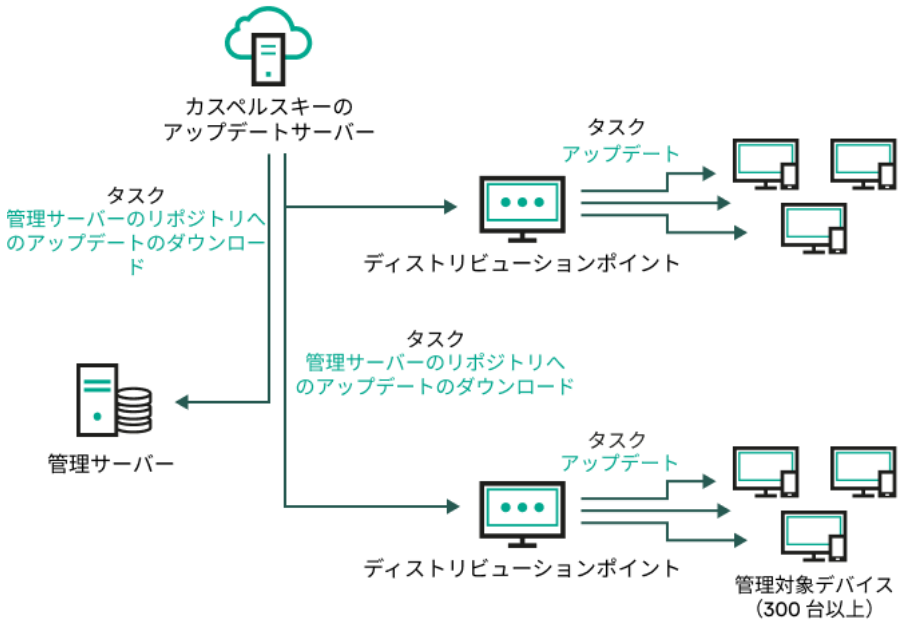
各カスペルスキー製品は、管理サーバーに必要なアップデートを要求します。管理サーバーはこれらの要求を集計した上で、いずれかの製品で要求されたアップデートのみをダウンロードします。これにより、同一のアップデートが複数回ダウンロードされたり、不必要なアップデートがダウンロードされることを防ぐことができます。［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを実行中、関連するバージョンの定義データベースとソフトウェアモジュールを確実にダウンロードする目的で、次の情報が管理サーバーからカスペルスキーのアップデートサーバーに自動的に送信されます：

- 製品 ID およびバージョン
- アプリケーションのインストール ID
- 現在のライセンス ID
- ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの実行 ID

送信される情報には、個人データや機密データは含まれません。カスペルスキーでは、法律で定められた要件に従って情報を保護しています。

2 つのタスク（［管理サーバーのリポジトリへのアップデートのダウンロード］タスクおよび［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスク）の使用

管理サーバーのリポジトリを経由させずに、カスペルスキーのアップデートサーバーからディストリビューションポイントのリポジトリにアップデートを直接ダウンロードして、管理対象デバイスにアップデートを配信できます（次の図を参照）。ディストリビューションポイントのリポジトリへのダウンロードが推奨されるのは、管理サーバーとディストリビューションポイント間の通信の方がディストリビューションポイントとカスペルスキーのアップデートサーバー間の通信よりも費用がかかる場合や、管理サーバーがインターネットにアクセスできない場合などです。



管理サーバーのリポジトリへのアップデートのダウンロードタスクおよびディストリビューションポイントのリポジトリにアップデートをダウンロードタスクによるアップデート

既定では、管理サーバーとディストリビューションポイントは HTTPS プロトコルを使用してカスペルスキーのアップデートサーバーに接続し、アップデートをダウンロードします。必要に応じて、管理サーバー、ディストリビューションポイント、またはその両方で HTTPS プロトコルの代わりに HTTP プロトコルを使用するように設定を編集できます。

このスキームを実装するには、*［管理サーバーのリポジトリへのアップデートのダウンロード］*タスクに加えて*［ディストリビューションポイントのリポジトリにアップデートをダウンロード］*タスクを作成します。その後、ディストリビューションポイントは、管理サーバーのリポジトリではなくカスペルスキーのアップデートサーバーからアップデートをダウンロードします。

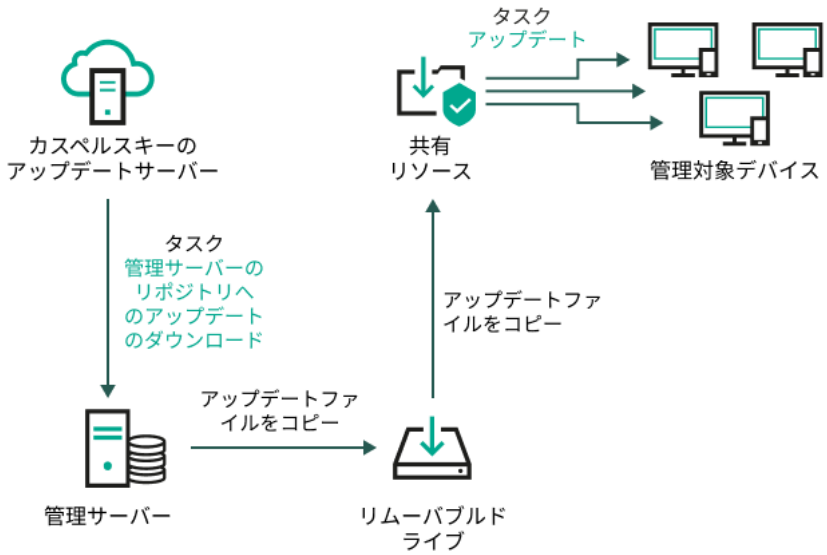
macOS を実行しているディストリビューションポイントデバイスでは、カスペルスキーのアップデートサーバーからアップデートをダウンロードできません。

*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクの対象範囲に macOS を実行しているデバイスが 1 台以上含まれている場合、すべての Windows デバイスでタスクが正常に完了した場合でも、タスクには「*失敗*」ステータスが付与されます。

定義データベースと Kaspersky Security Center のソフトウェアモジュールは*［管理サーバーのリポジトリへのアップデートのダウンロード］*タスクを使用してダウンロードされるため、このスキームでもこのタスクが必要です。

ローカルフォルダー、共有フォルダー、または FTP サーバーを使用して手動で実行

クライアントデバイスが管理サーバーに接続できない場合、ローカルフォルダーまたは共有リソースを使用して定義データベース、ソフトウェアモジュール、カスペルスキー製品をアップデートできます。このスキームでは、管理サーバーのリポジトリからリムーバブルドライブに必要なアップデートをコピーして、Kaspersky Endpoint Security の設定でアップデート元として指定したローカルフォルダーまたは共有リソースにアップデートをコピーする必要があります（次の図を参照）。



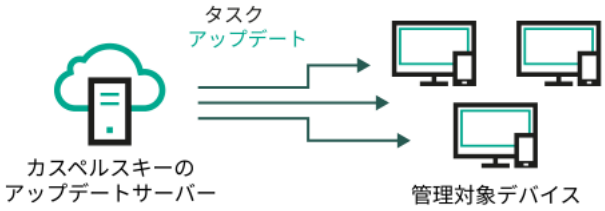
ローカルフォルダー、共有フォルダー、または FTP サーバーを使用したアップデート

Kaspersky Endpoint Security のアップデート元の詳細については、次のヘルプを参照してください：

- Kaspersky Endpoint Security for Windows のヘルプ
- Kaspersky Endpoint Security for Linux のヘルプ

カスペルスキーのアップデートサーバーから管理対象デバイスの Kaspersky Endpoint Security を直接アップデート

管理対象デバイスで、カスペルスキーのアップデートサーバーから直接アップデートを受信するように Kaspersky Endpoint Security を設定できます（次の図を参照）。



カスペルスキーのアップデートサーバーからセキュリティ製品を直接アップデート

このスキームでは、セキュリティ製品は Kaspersky Security Center が提供するリポジトリを使用しません。カスペルスキーのアップデートサーバーからアップデートを直接受信するには、セキュリティ製品のインターフェイスでカスペルスキーのアップデートサーバーをアップデート元として指定します。これらの設定の詳細については、次のヘルプを参照してください：

- Kaspersky Endpoint Security for Windows のヘルプ
- Kaspersky Endpoint Security for Linux のヘルプ

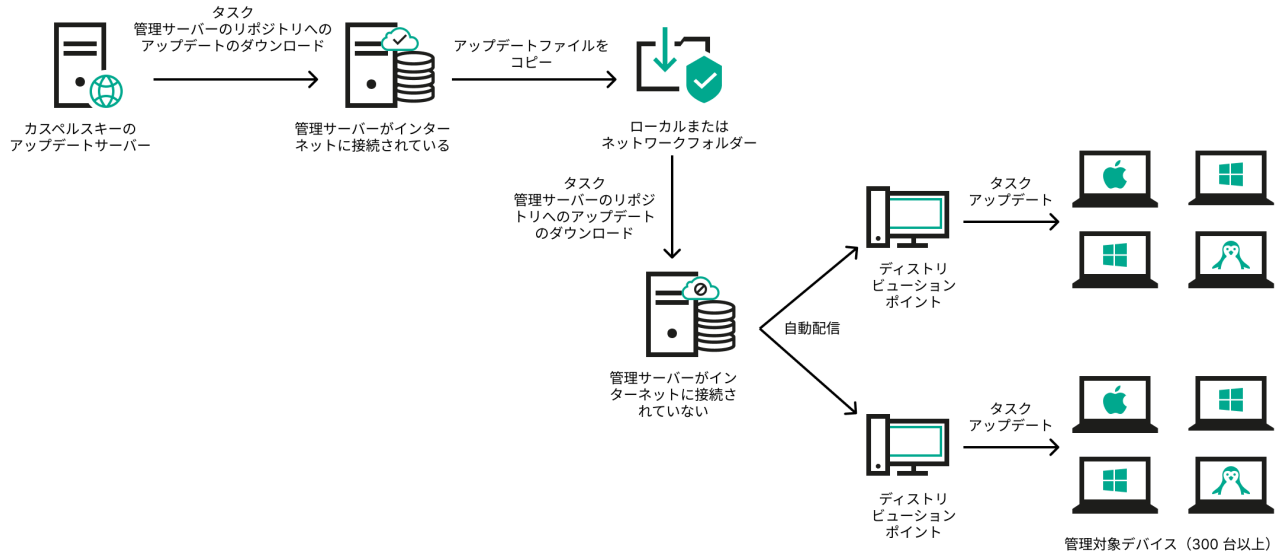
管理サーバーがインターネットに接続されていない場合は、ローカルまたはネットワークフォルダー経由

管理サーバーがインターネットに接続されていない場合は、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを設定して、ローカルまたはネットワークフォルダーからアップデートをダウンロードできます。この場合、指定したフォルダーに必要なアップデートファイルを定期的にコピーする必要があります。たとえば、次のいずれかのソースから、必要なアップデートファイルをコピーできます：

- インターネットに接続されている管理サーバー（下図を参照）

  管理サーバーは、セキュリティ製品が要求したアップデートのみをダウンロードするため、管理サーバーによって管理されるセキュリティ製品のセット（インターネット接続があるものとないもの）が一致している必要があります。

  アップデートのダウンロードに使用する管理サーバーのバージョンが 13.2 以前の場合、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクのプロパティを開き、［**旧スキームを使用してアップデートをダウンロード**］オプションをオンにします。



管理サーバーがインターネットに接続されていない場合のローカルまたはネットワーク フォルダー経由のアップデート

- Kaspersky Update Utility

  このユーティリティは旧スキームを使用してアップデートをダウンロードするため、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクのプロパティを開き、［**旧スキームを使用してアップデートをダウンロード**］オプションをオンにします。

［管理サーバーのリポジトリへのアップデートのダウンロード］タスクの作成

管理サーバーの［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクは、Kaspersky Security Center のクイックスタートウィザードによって自動的に作成されます。［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクは1つのみ作成できます。したがって、*管理サーバーのリポジトリへのアップデートのダウンロード*タスクを作成できるのは、このタスクが管理サーバーのタスクリストから削除された場合のみです。

このタスクは、カスペルスキーのアップデートサーバーから管理サーバーのリポジトリにアップデートをダウンロードするために必要です。アップデートのリストには次の内容が含まれます：

- 管理サーバーの定義データベースおよびソフトウェアモジュールのアップデート
- カスペルスキーのセキュリティ製品の定義データベースおよびソフトウェアモジュールのアップデート
- Kaspersky Security Center コンポーネントのアップデート
- カスペルスキーのセキュリティ製品のアップデート

アップデートのダウンロード後、管理対象デバイスにこれらのアップデートを配信できます。

管理対象デバイスにアップデートを配信する前に、*アップデートの検証*タスクを実行できます。このことにより、管理サーバーが正しいアップデートをインストールし、アップデートによりセキュリティレベルが下がることがないことを確認できます。配信前に検証するには、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの設定で［**アップデートの検証の実行**］オプションをオンにします。

***管理サーバーのリポジトリへのアップデートのダウンロード**タスクを作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。

2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**管理サーバーのリポジトリへのアップデートのダウンロード**］タスク種別を選択します。

4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

5. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

6. ［**作成**］をクリックします。

   タスクが作成され、タスクリストに表示されます。

7. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

8. タスクのプロパティウィンドウの［**アプリケーション設定**］タブで、次の設定を指定します：

   - **アップデート元**

     管理サーバーのアップデート元として、使用できるものは次のとおりです：

     - カスペルスキーのアップデートサーバー

       カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。既定では、管理サーバーは HTTPS プロトコルを使用してカスペルスキーのアップデートサーバーに接続し、アップデートをダウンロードします。必要に応じて、管理サーバーで HTTPS プロトコルの代わりに HTTP プロトコルを使用するように設定を編集できます。

       既定では、この項目が選択されます。

     - プライマリ管理サーバー

       セカンダリ管理サーバーまたは仮想管理サーバーを対象とするタスクに適用されます。

     - ローカルまたはネットワークフォルダー

       最新のアップデートが保存されたローカルフォルダーまたはネットワークフォルダー：ネットワークフォルダーとしては FTP サーバー、HTTP サーバー、または SMB 共有を指定できます。ネットワークフォルダーに認証が必要な場合、SMB プロトコルのみがサポートされています。ローカルフォルダーの選択時には、管理サーバーがインストールされているデバイスのフォルダーを指定する必要があります。

       > アップデート元で使用される FTP/HTTP サーバーまたはネットワークフォルダーは、アップデートを含み、フォルダーの構造がカスペルスキーのアップデートサーバーの使用時に作成された構造と一致する必要があります。

     アップデートが含まれる共有フォルダーがパスワードで保護されている場合は、［**アップデート元の共有フォルダーにアクセスするアカウントを指定する（存在する場合）**］をオンにして、アクセスに必要なアカウント資格情報を入力します。

   - **アップデート保存先フォルダー**

保存したアップデートを保管するためのフォルダーのパス。指定したフォルダーのパスをクリップボードにコピーすることができます。グループタスクに対して指定されたフォルダーのパスを変更することはできません。

- その他の設定：
  - **セカンダリ管理サーバーの強制アップデート**

    このオプションをオンにすると、管理サーバーは、新しいアップデートがダウンロードされるとすぐに、セカンダリ管理サーバーのアップデートタスクを開始します。アップデートタスクは、セカンダリ管理サーバーのタスクプロパティで構成されているアップデートソースを使用して開始されます。

    このオプションをオフにすると、セカンダリ管理サーバーのアップデートタスクは、スケジュールに従って開始されます。

    既定では、このオプションはオフです。

  - **ダウンロード済みのアップデートを追加のフォルダーにコピー**

    管理サーバーがアップデートを受信すると、指定されたフォルダーにコピーします。ネットワークでのアップデートの配信を手動で管理する場合は、このオプションをオンにします。

    このオプションの使用を検討する状況としては、たとえば、組織のネットワークが複数の独立したサブネットワークで構成され、各サブネットワークに属するデバイスは別のサブネットワークへのアクセス権を付与されていない場合があります。ただし、すべてのサブネットワークのデバイスは共通のネットワーク共有へのアクセス権は付与されています。この場合、いずれかのサブネットワークの管理サーバーでカスペルスキーのアップデートサーバーからアップデートをダウンロードするように設定した後、このオプションをオンにし、ネットワーク共有をコピー先に指定します。他の管理サーバーでは、リポジトリへのアップデートのダウンロードタスクのアップデート元として、このネットワーク共有を指定します。

    既定では、このオプションはオフです。

  - **アップデートのコピーが完了していない場合はデバイスおよびセカンダリ管理サーバーを強制アップデートしない**

    クライアントデバイスとセカンダリ管理サーバーでのアップデートのダウンロードタスクは、元のネットワークフォルダーから追加のアップデートフォルダーにアップデートがコピーされるまで開始されません。

    クライアントデバイスとセカンダリ管理サーバーが、追加のネットワークフォルダーからアップデートをダウンロードする場合は、このオプションをオンにする必要があります。

    既定では、このオプションはオフです。

- **アップデートの内容**：
  - **差分ファイルのダウンロード**

    このオプションで差分ファイルのダウンロードを有効にすることができます。

    既定では、このオプションはオフです。

- **旧スキームを使用してアップデートをダウンロード**

Kaspersky Security Center のバージョン 14 から、データベースのアップデートとソフトウェアモジュールのダウンロードには新しいスキームが使用されるようになりました。新しいスキームを使用してアップデートをダウンロードするには、アップデート元に、新しいスキームと互換性のあるメタデータを持つアップデートファイルが含まれている必要があります。アップデート元のアップデートファイルのメタデータが旧スキームのみと互換性がある場合は、［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。オフにした場合、アップデートのダウンロードタスクは失敗します。

たとえば、アップデート元としてローカルまたはネットワークフォルダーが指定されており、そのフォルダー内のアップデートファイルが次のアプリケーションによってダウンロードされた場合にはこのオプションをオンにする必要があります：

- Kaspersky Update Utility

  このユーティリティは旧スキームを使用してアップデートをダウンロードします。

- Kaspersky Security Center 13.2 以前のバージョン

  例えば、管理サーバー 1 はインターネットに接続していないものとします。この場合、インターネットに接続できる管理サーバー 2 を使用してアップデートをダウンロードし、このアップデートを管理サーバー 1 のアップデート元として使用するために、ローカルまたはネットワークフォルダーに保存します。管理サーバー 2 に Kaspersky Security Center のバージョン 13.2 以前のバージョンがインストールされていた場合、管理サーバー 1 向けのタスクでは［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。

既定では、このオプションはオフです。

- **アップデートの検証の実行**

管理サーバーはアップデート元からアップデートをダウンロードし、それらを一時リポジトリに保存して、［**アップデート検証タスク**］で定義されたタスクを実行します。タスクが正常に終了すると、アップデートは一時保管領域から管理サーバーの共有フォルダーにコピーされ、この管理サーバーをアップデート元とするすべてのデバイスに配信されます（［**新しいアップデートがリポジトリにダウンロードされ次第**］のスケジュールが設定されたタスクが開始されます）。アップデートをリポジトリにダウンロードするタスクが完了するのは、*アップデートの検証*タスクの完了後のみです。

既定では、このオプションはオフです。

9. タスクのプロパティウィンドウの［**スケジュール**］タブで、タスクの開始スケジュールを作成します。必要に応じて、次の設定を指定します：

- **タスク開始：**

タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

- **手動**

タスクは、自動的には実行されません。手動でのみ開始できます。

既定では、このオプションがオンです。

- **N 分ごと**

タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

- **N 時間ごと**

  指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

  既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

- **N 日ごと**

  日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

  既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。

  指定した日付が存在しない月には、月の最終日にタスクを実行します。

  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。

  規定では、日付は選択されていません。規定の開始時間は18:00 です。

- **ウイルスアウトブレイク検知次第**

  ［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

  - ワークステーションとファイルサーバー向けアンチウイルス製品
  - 境界防御向けアンチウイルス製品
  - メールサーバー向けアンチウイルス製品

  既定では、すべてのアプリケーション種別がオンです。

  ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

- タスク名で検索するには、検索フィールドにタスク名を入力します。
- 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。
  既定では、タスクはアルファベットの昇順で並べ替えられます。
- フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

  このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

  このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

  このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

  既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内で自動的かつランダムに遅延させる（分）**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

既定では、このオプションはオフです。既定の時間は1分です。

- **次の時間を超える場合はタスクを停止する**

  指定した時間が経過すると、タスクが完了したかどうかに関係なくタスクが自動的に停止します。

  実行に時間がかかり過ぎているタスクを中断したい時に、このオプションを使用します。

  既定では、このオプションはオフです。既定のタスク実行時間は120分です。

10. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。

管理サーバーが［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを実行すると、アップデート元からデータベースとソフトウェアモジュールのアップデートがダウンロードされ、管理サーバーの共有フォルダーに保存されます。管理グループに対してこのタスクを作成すると、指定された管理グループにあるネットワークエージェントにのみ適用されます。

アップデートは管理サーバーの共有フォルダーからクライアントデバイスとセカンダリ管理サーバーに配信されます。

ダウンロードされたアップデートの検証

管理対象デバイスにアップデートをインストールする前に、*アップデート検証*タスクを使用してアップデートの動作およびエラーがないかどうかを検証できます。*アップデート検証*タスクは、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの一部として自動的に実行されます。アップデート元からアップデートがダウンロードされて、一時リポジトリに保存された後、*アップデート検証*タスクが実行されます。タスクが正常に完了すると、一時リポジトリから管理サーバーの共有フォルダーにアップデートがコピーされます。アップデートのコピーは、管理サーバーがアップデート元として指定されているすべてのクライアントデバイスに配信されます。

*アップデート検証*タスクの結果、一時リポジトリにあるアップデートが正しくないことが判明した場合、または*アップデート検証*タスクがエラーで終了した場合、それらのアップデートは共有フォルダーにコピーされません。管理サーバーでは、以前のアップデートが維持されます。また、スケジュール種別として［**新しいアップデートがリポジトリにダウンロードされ次第**］が指定されたタスクも開始されません。新しいアップデートのスキャンが正常に完了した場合、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクの次の開始時に、それらのタスクが実行されます。

少なくとも1台のテストデバイスで次のいずれかの条件が当てはまる場合、アップデートは正しくないと判断されます：

- アップデートタスクエラーが発生した
- セキュリティ製品のリアルタイム保護のステータスがアップデートの適用後に変更された
- オンデマンドスキャンタスクの実行中に、感染したオブジェクトが検知された

- カスペルスキー製品の実行時にエラーが発生した

すべてのテストデバイスの場合に挙げられた条件が当てはまらない場合、そのアップデートは正常とみなされ、*アップデート検証*タスクは正常に終了したと判断されます。

*アップデート検証*タスクを作成する前に、次の前提条件を実行してください：

1. 複数のテストデバイスで管理グループを作成する。このグループはアップデートの検証に必要になります。

   ネットワーク内で、最も信頼性の高い保護が適用されており、最も一般的なアプリケーション設定が行われているデバイスを使用してください。このアプローチにより、スキャン中のウイルス検知の精度が向上し、誤検知のリスクを最小限に抑えます。テストデバイスでウイルスが検知された場合、*アップデート検証*タスクは失敗と判断されます。

2. Kaspersky Endpoint Security for Windows や Kaspersky Security for Windows Server など、Kaspersky Security Center のサポート対象のアプリケーション向けにアップデートおよびマルウェアスキャンタスクを作成します。アップデートおよびマルウェアスキャンタスクの作成時に、テストデバイスの管理グループを指定します。

   *アップデート検証*タスクは、順次テストデバイスでアップデートとマルウェアスキャンタスクを実行し、すべてのアップデートが有効であることを確認します。また、*アップデート検証*タスクの作成中にアップデートおよびマルウェアスキャンタスクを指定する必要があります。

3. ［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクをクリックします。

ダウンロードしたアップデートを、クライアントデバイスに配信する前に Kaspersky Security Center で検証するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**管理サーバーのリポジトリへのアップデートのダウンロード**］タスクをクリックします。
3. タスクのプロパティウィンドウが開いたら、［**アプリケーション設定**］タブに移動し、［**アップデートの検証の実行**］オプションをオンにします。
4. *アップデート検証*タスクがある場合は、［**タスクの選択**］をクリックします。表示されたウィンドウで、テストデバイスの管理グループで*アップデート検証*タスクを選択します。
5. 事前に*アップデート検証*タスクを作成していなかった場合は、次の操作を実行します：

   a. ［**新規タスク**］をクリックします。

   b. タスクの追加ウィザードが表示されるので、事前設定されたタスク名を変更する場合は名前を指定します。

   c. 事前に作成しておいたテストデバイスの管理グループを選択します。

   d. 最初に Kaspersky Security Center がサポートする必要なアプリケーションのアップデートタスクを選択し、次にマルウェアスキャンタスクを選択します。

   その後、次のオプションが表示されます。オプションはオンのままにしておくことを推奨します。

   - **定義データベースのアップデート後にデバイスを再起動する**

     デバイス上で定義データベースをアップデートした後には、デバイスの再起動を推奨します。

     既定では、このオプションはオンです。

- **定義データベースのアップデートとデバイス再起動の後にリアルタイム保護のステータスを確認する**

  このオプションをオンにすると、*アップデート検証*タスクは、管理サーバーのリポジトリにダウンロードされたアップデートが有効であるかどうか、また定義データベースのアップデート後にデバイスが再起動された後に保護レベルが低下することがないかを確認します。

  既定では、このオプションはオンです。

e. *アップデート検証タスク*を実行するアカウントを指定します。自身のアカウントの使用も可能で、［**既定のアカウント**］オプションをオンのままにします。または、必要なアクセス権を持つ別のアカウントを指定してタスクを実行することもできます。この場合は［**アカウントの指定**］をオンにしてそのアカウントの資格情報を入力してください。

6. ［**保存**］をクリックして、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクのプロパティウィンドウを閉じます。

アップデートの自動的な検証が有効になります。これで、［*管理サーバーのリポジトリへのアップデートのダウンロード*］タスクを実行できるようになりました。タスクはアップデートの検証から開始します。

［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの作成

*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクは Windows を実行しているディストリビューションポイントデバイスでのみ使用できます。Linux または macOS を実行しているディストリビューションポイントデバイスでは、カスペルスキーのアップデートサーバーからアップデートをダウンロードできません。タスクの対象範囲に Linux または macOS を実行しているデバイスが 1 台以上含まれている場合、タスクには「*失敗*」ステータスが付与されます。タスクが Windows を実行しているデバイスではすべて正常に実行された場合でも、残りのデバイスに対してエラーが返されます。

*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを管理グループに対して作成できます。このタスクは、指定の管理グループ内のディストリビューションポイントに対して実行されます。

このタスクの使用例としては、管理サーバーとディストリビューションポイント間の通信の方が、ディストリビューションポイントとカスペルスキーのアップデートサーバー間の通信よりも費用がかかる場合や、管理サーバーがインターネットにアクセスできない場合などがあります。

このタスクは、カスペルスキーのアップデートサーバーからディストリビューションポイントのリポジトリにアップデートをダウンロードするために必要です。アップデートのリストには次の内容が含まれます：

- カスペルスキーのセキュリティ製品の定義データベースおよびソフトウェアモジュールのアップデート
- Kaspersky Security Center コンポーネントのアップデート
- カスペルスキーのセキュリティ製品のアップデート

アップデートのダウンロード後、管理対象デバイスにこれらのアップデートを配信できます。

ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを、特定の管理グループに対して作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**タスク種別**］で［**ディストリビューションポイントのリポジトリにアップデートをダウンロード**］を選択します。

4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

5. タスクの適用対象として、管理グループ、デバイスの抽出、または指定したデバイスを選択します。

6. ［**タスク作成の終了**］ステップで、既定のタスク設定を変更する場合、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

7. ［**作成**］をクリックします。

   タスクが作成され、タスクリストに表示されます。

8. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

9. タスクのプロパティウィンドウの［**アプリケーション設定**］タブで、次の設定を指定します：

   - **アップデート元**

     ディストリビューションポイントのアップデート元として、使用できるものは次の通りです：

     - カスペルスキーのアップデートサーバー

       カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。

       既定ではこのオプションが選択されます。

     - プライマリ管理サーバー

       セカンダリ管理サーバーまたは仮想管理サーバーを対象とするタスクに適用されます。

     - ローカルまたはネットワークフォルダー

       最新のアップデートが保存されたローカルフォルダーまたはネットワークフォルダー：ネットワークフォルダーとしては FTP サーバー、HTTP サーバー、または SMB 共有を指定できます。ネットワークフォルダーに認証が必要な場合、SMB プロトコルのみがサポートされています。ローカルフォルダーの選択時には、管理サーバーがインストールされているデバイスのフォルダーを指定する必要があります。

       > アップデート元で使用される FTP/HTTP サーバーまたはネットワークフォルダーは、アップデートを含み、フォルダーの構造がカスペルスキーのアップデートサーバーの使用時に作成された構造と一致する必要があります。

   - **アップデート保存先フォルダー**

     保存したアップデートを保管するためのフォルダーのパス。指定したフォルダーのパスをクリップボードにコピーすることができます。グループタスクに対して指定されたフォルダーのパスを変更することはできません。

- **差分ファイルのダウンロード**

  このオプションで差分ファイルのダウンロードを有効にすることができます。

  既定では、このオプションはオフです。

- **旧スキームを使用してアップデートをダウンロード**

  Kaspersky Security Center のバージョン 14 から、データベースのアップデートとソフトウェアモジュールのダウンロードには新しいスキームが使用されるようになりました。新しいスキームを使用してアップデートをダウンロードするには、アップデート元に、新しいスキームと互換性のあるメタデータを持つアップデートファイルが含まれている必要があります。アップデート元のアップデートファイルのメタデータが旧スキームのみと互換性がある場合は、［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。オフにした場合、アップデートのダウンロードタスクは失敗します。

  たとえば、アップデート元としてローカルまたはネットワークフォルダーが指定されており、そのフォルダー内のアップデートファイルが次のアプリケーションによってダウンロードされた場合にはこのオプションをオンにする必要があります：

  - Kaspersky Update Utility

    このユーティリティは旧スキームを使用してアップデートをダウンロードします。

  - Kaspersky Security Center 13.2 以前のバージョン

    たとえば、ディストリビューションポイントがローカルまたはネットワークフォルダーからアップデートを取得するように設定されているものとします。この場合、インターネットに接続できる管理サーバーを使用してアップデートをダウンロードし、このアップデートをディストリビューションポイントのローカルフォルダーに配置します。管理サーバーに Kaspersky Security Center 13.2 以前のバージョンがインストールされている場合、*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクで［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。

  既定では、このオプションはオフです。

10. タスクの開始スケジュール作成。必要に応じて、次の設定を指定します：

- **タスク開始**

  タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

  - **手動**

    タスクは、自動的には実行されません。手動でのみ開始できます。

    既定では、このオプションがオンです。

  - **N 分ごと**

    タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

    既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

  - **N 時間ごと**

指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

- **N 日ごと**

  日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

  既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。

  指定した日付が存在しない月には、月の最終日にタスクを実行します。

  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。

  規定では、日付は選択されていません。規定の開始時間は18:00 です。

- **ウイルスアウトブレイク検知次第**

  ［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

  - ワークステーションとファイルサーバー向けアンチウイルス製品
  - 境界防御向けアンチウイルス製品
  - メールサーバー向けアンチウイルス製品

  既定では、すべてのアプリケーション種別がオンです。

  ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして*ウイルススキャン*タスクを実行できます。

テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

- タスク名で検索するには、検索フィールドにタスク名を入力します。
- 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。
  既定では、タスクはアルファベットの昇順で並べ替えられます。
- フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

- **未実行のタスクを実行する**

  このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

  このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

  このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

  既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内で自動的かつランダムに遅延させる（分）**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

既定では、このオプションはオフです。既定の時間は1分です。

11. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。

タスクの作成時に指定した設定およびタスクのその他のプロパティは、いつでも変更できます。

*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを実行すると、定義データベースとソフトウェアモジュールのアップデートがアップデート元からダウンロードされ、共有フォルダーに保存されます。指定の管理グループに含まれていて、ディストリビューションポイントタスクが明示的に設定されていないディストリビューションポイントにしか、ダウンロードされたアップデートは使用されません。

Kaspersky Security Center コンポーネントの自動アップデートおよびパッチ適用の有効化と無効化

管理サーバーのアップデートとパッチは、管理者が明示的に承認した後、手動でのみインストールできます。

Kaspersky Security Center コンポーネントのアップデートとパッチの自動インストールは、デバイスにネットワークエージェントをインストールする際に既定値で有効化されます。ネットワークエージェントのインストール中、あるいはインストール後にポリシーを使用して無効化することができます。

ネットワークエージェントをデバイスのローカルにインストール中、Kaspersky Security Center コンポーネントの自動アップデートとパッチを無効にするには：

1. デバイスへのネットワークエージェントのローカルインストールを開始します。
2. **詳細設定**ステップで、［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオフにします。
3. ウィザードの指示に従ってください。

Kaspersky Security Center コンポーネントの自動アップデートとパッチが無効にされたネットワークエージェントが、デバイスにインストールされます。ポリシーを使用して、自動アップデートとパッチを有効にできます。

インストールパッケージを介してネットワークエージェントをデバイスにインストール中に、Kaspersky Security Center コンポーネントの自動アップデートとパッチを無効にするには：

1. メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。
2. **Kaspersky Security Center ネットワークエージェント <バージョン番号>** パッケージをクリックします。

3. プロパティウィンドウで［**設定**］タブを開きます。

4. ［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオフにします。

Kaspersky Security Center コンポーネントの自動アップデートとパッチが無効にされたネットワークエージェントが、このパッケージからインストールされます。ポリシーを使用して、自動アップデートとパッチを有効にできます。

デバイスにネットワークエージェントをインストール中に、このチェックボックスをオンにすると（またはオフにすると）、その後ネットワークエージェントポリシーを使用して自動アップデートを有効（または無効）にできます。

ネットワークエージェントポリシーを使用して、Kaspersky Security Center コンポーネントの自動アップデートとパッチを有効または無効にするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。

2. ネットワークエージェントのポリシーをクリックします。

3. ポリシーのプロパティウィンドウで［**アプリケーション設定**］タブを開きます。

4. ［**パッチとアップデートの管理**］セクションで、［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオンまたはオフにして、自動アップデートとパッチを有効または無効にします。

5. このスイッチの設定に「ロック（🔒）」を設定します。

選択したデバイスにポリシーが適用され、Kaspersky Security Center コンポーネントの自動アップデートとパッチがデバイス上で有効（または無効）になります。

Kaspersky Endpoint Security for Windows のアップデートの自動インストール

クライアントデバイスでの Kaspersky Endpoint Security for Windows の定義データベースとソフトウェアモジュールの自動アップデートを設定できます。

デバイスでの Kaspersky Endpoint Security for Windows のアップデートのダウンロードおよび自動インストールを設定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

2. ［**追加**］をクリックします。

新規タスクウィザードが起動します。ウィザードの指示に従ってください。

3. Kaspersky Endpoint Security for Windows を対象アプリケーションとするタスクから、［**アップデート**］タスク種別を選択します。

4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

5. タスク範囲を選択します。

6. タスクの適用対象として、管理グループ、デバイスの抽出、または指定したデバイスを選択します。

7. ［**タスク作成の終了**］ステップで、既定のタスク設定を変更する場合、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

8. ［**作成**］をクリックします。

   タスクが作成され、タスクリストに表示されます。

9. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

10. タスクのプロパティウィンドウの［**アプリケーション設定**］タブで、アップデートタスクの設定をローカルモードかモバイルモードで指定します：

    - **ローカルモード**：管理サーバーとデバイスの間で接続が確立されている場合。

    - **モバイルモード**：Kaspersky Security Center とデバイスの間で接続が確立されていない場合（たとえば、デバイスがインターネットに接続されていない時）。

11. Kaspersky Endpoint Security for Windows の定義データベースとソフトウェアモジュールのアップデートに使用するアップデート元を有効にします。必要に応じて、［**上へ**］と［**下へ**］を使用して、リスト内のアップデート元の順序を変更できます。複数のアップデート元が有効な場合は、リスト上位のリソースから次々に接続が試行され、最初に使用可能なソースからアップデートパッケージが取得されて、アップデートタスクが実行されます。

12. ［**承認されたソフトウェアモジュールのアップデートのインストール**］をオンにすると、定義データベースとともに、ソフトウェアモジュールのアップデートをダウンロードしてインストールできます。

    このオプションをオンにすると、Kaspersky Endpoint Security for Windows によって適用可能なソフトウェアモジュールのアップデートについてユーザーに通知され、アップデートタスクの実行時に、アップデートパッケージにソフトウェアモジュールのアップデートが追加されます。Kaspersky Endpoint Security for Windows では、*承認*ステータスが付与されたアップデートのみがインストールされます。ローカルへのインストールは、製品インターフェイスまたは Kaspersky Security Center を経由して実行されます。

    ［**ソフトウェアモジュールの重要なアップデートを自動的にインストール**］をオンにすることもできます。ソフトウェアモジュールのアップデートが使用可能な時、Kaspersky Endpoint Security for Windows は「*緊急*」ステータスのアップデートのみを自動的にインストールし、残りのアップデートは承認後にインストールします。

    ソフトウェアモジュールのアップデートで使用許諾契約書とプライバシーポリシーの条項を確認して同意する必要がある場合、カスペルスキー製品では、使用許諾契約書とプライバシーポリシーの条項をユーザーが同意した後にアップデートがインストールされます。

13. フォルダーへダウンロード済みのアップデートを保存するには［**アップデートをフォルダーにコピー**］をオンにし、保存先のフォルダーのパスを指定します。

14. タスクのスケジュールを設定します。確実にタイムリーにアップデートされるようにするため、［**新しいアップデートがリポジトリにダウンロードされ次第**］をオンにすることを推奨します。

15. ［**保存**］をクリックします。

［**アップデート**］タスクの実行時、製品からカスペルスキーのアップデートサーバーにリクエストが送信されます。

アップデートによっては、最新バージョンの管理プラグインをインストールする必要があります。

ソフトウェアアップデートの拒否と承認

アップデートのインストールタスクの設定によっては、インストールするアップデートの承認が必要な場合があります。インストールする必要のあるアップデートを承認し、インストールしないアップデートを拒否します。

たとえば、最初にテスト環境にアップデートをインストールしてデバイスのオペレーティングシステムとの互換性の問題が生じないかを確認してから、クライアントデバイスへのこれらのアップデートのインストールを許可することができます。

1 つ以上のアップデートを承認または拒否するには：

1. メインメニューで、［**操作**］→［**カスペルスキー製品**］→［**シームレスアップデート**］の順に移動します。

   適用可能なアップデートのリストが表示されます。

   管理対象の製品のアップデートには、Kaspersky Security Center の特定の最小バージョンをインストールする必要がある場合があります。この最小バージョンが現在のバージョンよりも新しい場合、これらのアップデートは表示されますが、承認はできません。また、Kaspersky Security Center をアップグレードするまでは、このようなアップデートからインストールパッケージを作成することもできません。Kaspersky Security Center インスタンスを必要な最小バージョンにアップグレードするように要求されます。

2. 承認または拒否するアップデートを選択します。
3. 選択したアップデートを承認する場合は［**承認**］を、拒否する場合は［**承認却下**］を選択します。

   既定値は［*未定義*］です。

   ［*承認*］ステータスを割り当てたアップデートは、インストールを待機するキューに置かれます。

   ［*拒否*］ステータスを割り当てたアップデートは、アップデートをインストール済みのすべてのデバイスからアンインストールされます（可能な場合）。また、今後これらのアップデートは他のデバイスに新規にインストールされません。

カスペルスキー製品の一部のアップデートはアンインストールできません。アンインストールできないカスペルスキー製品のアップデートに［*拒否*］ステータスを設定した場合、これらのアップデートはインストール済みのデバイスからアンインストールされません。しかし、今後これらのアップデートが他のデバイスに新規にインストールされることはありません。

サードパーティ製のソフトウェアアップデートに［*拒否*］ステータスを設定すると、このアップデートは、アップデートのインストールを予定しているがまだ完了していないデバイスにはインストールされません。アップデートをインストール済みのデバイスには、これらのアップデートがそのまま残ります。アップデートを削除する時は、手動でローカル削除できます。

管理サーバーのアップデート

［管理サーバーのアップデートウィザード］を使用することで管理サーバーのアップデートをインストールできます。

管理サーバーのアップデートをインストールするには：

1. メインメニューで、［**操作**］→［**カスペルスキー製品**］→［**シームレスアップデート**］の順に選択します。
2. 次のいずれかの方法で、管理サーバーのアップデートウィザードを実行します：
   - アップデートのリストから管理サーバーのアップデートの名前をクリックし、表示されたウィンドウで［**管理サーバーのアップデートウィザードを実行**］をクリックします。
   - ウィンドウ上部の通知フィールドにある［**管理サーバーのアップデートウィザードを実行**］をクリックします。
3. ［管理サーバーのアップデートウィザード］ウィンドウで、次のいずれかを選択してアップデートのインストール時期を指定します：
   - **今すぐインストール**：アップデートのインストールをすぐにインストールする場合は、このオプションをオンにします。
   - **インストールを延期**：アップデートのインストールをあとでインストールする場合は、このオプションをオンにします。この場合、アップデートに関する通知は表示されます。
   - **アップデートを無視**：アップデートをインストールせず、そのアップデートに関する通知を受け取りたくない場合はこのオプションを選択します。
4. アップデートをインストールする前に管理サーバーのバックアップを作成する場合は［**アップデートをインストールする前に管理サーバーのバックアップコピーを作成する**］を選択します。
5. ［OK］をクリックしてウィザードを完了します。

バックアッププロセスが中断されると、アップデートのプロセスも中断されます。

オフライン方式のアップデートのダウンロードの有効化と無効化

オフライン方式でのアップデートのダウンロードを無効にすることは推奨されません。無効にすると、デバイスにアップデートが提供されません。場合によっては、カスペルスキーのテクニカルサポート担当者が、［**アップデートと定義データベースをあらかじめ管理サーバーからダウンロードする**］をオフにすることを推奨する場合もあります。次に、カスペルスキー製品のアップデートを受信するためのタスクが設定されていることを確認する必要があります。

管理グループでオフライン方式のアップデートのダウンロードを有効または無効にするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. ［**グループ**］をクリックします。
3. 管理グループのリストで、オフライン方式のアップデートのダウンロードを有効化する必要がある管理グループを選択します。

4. ネットワークエージェントのポリシーをクリックします。

   ネットワークエージェントポリシーのプロパティウィンドウが表示されます。

   既定では、子ポリシーの設定は親ポリシーから継承され、変更することもできません。変更したいポリシーが継承されたものである場合、このポリシーを変更するのではなく、最初に目的の管理グループでネットワークエージェントの新規ポリシーを作成する必要があります。新規作成したポリシーでは、親ポリシーで「ロック」状態になっていない設定は変更できます。

5. ［**アプリケーション設定**］タブで、［**パッチとアップデートの管理**］セクションを選択します。

6. ［**アップデートと定義データベースをあらかじめ管理サーバーからダウンロードする（推奨）**］を、オフライン方式のアップデートのダウンロードを有効にする場合はオン、無効にする場合はオフにします。

   既定では、オフライン方式でのアップデートのダウンロードは有効です。

オフライン方式でのアップデートのダウンロードが有効または無効になります。

オフラインデバイスの定義データベースとソフトウェアモジュールのアップデート

管理対象デバイスの定義データベースとソフトウェアモジュールのアップデートは、ウイルスやその他の脅威からデバイスを継続して保護するために重要なタスクです。通常、管理者は管理サーバーのリポジトリまたはディストリビューションポイントのリポジトリを使用するように指定して、定期的なアップデートを設定します。

管理サーバー（プライマリまたはセカンダリ）、ディストリビューションポイント、インターネットのいずれにも接続されていないデバイス（またはデバイスのグループ）のデータベースとソフトウェアモジュールをアップデートする必要がある場合は、FTP サーバーまたはローカルフォルダーなどの代替のアップデート元を使用する必要があります。この場合、フラッシュドライブまたは外付けハードディスクなどの大容量ストレージデバイスを使用して必要なアップデートのファイルを受け渡しする必要があります。

必要なアップデートは次からコピーできます：

- 管理サーバー：

  オフラインデバイスにインストールされているセキュリティ製品に必要なアップデートが管理サーバーのリポジトリに含まれるようにするには、少なくとも1台のオンラインの管理対象デバイスに同じセキュリティ製品がインストールされている必要があります。また、この製品が管理サーバーのリポジトリへのアップデートのダウンロードタスクを使用して管理サーバーのリポジトリからアップデートを受信するように設定されている必要があります。

- 同じセキュリティ製品がインストールされていて、管理サーバーのリポジトリやディストリビューションポイントのリポジトリからアップデートを受信するか、カスペルスキーのアップデートサーバーからアップデートを直接受信するように設定されている任意のデバイス

管理サーバーのリポジトリからアップデートをコピーして、データベースおよびソフトウェアモジュールのアップデートを設定する例を次に示します。

オフラインデバイスの定義データベースとソフトウェアモジュールをアップデートするには：

1. 管理サーバーがインストールされているデバイスにリムーバブルドライブを接続します。

2. アップデートファイルをリムーバブルドライブにコピーします。

既定では、アップデートは「\\<サーバー名>\KLSHARE\Updates」に保存されています。

または、選択したフォルダーにアップデートを定期的にコピーするように Kaspersky Security Center を設定できます。これには、管理サーバーのリポジトリへのアップデートのダウンロードタスクのプロパティにある［**ダウンロード済みのアップデートを追加のフォルダーにコピー**］を使用します。フラッシュドライブまたは外付けハードディスクのフォルダーをこのオプションのターゲットフォルダーに指定した場合、この大容量ストレージデバイスには常にアップデートの最新バージョンが含まれることになります。

3. オフラインデバイスで、ローカルフォルダーまたは FTP サーバーや共有フォルダーなどの共有リソースからアップデートを受信するように、セキュリティ製品（たとえば Kaspersky Endpoint Security for Windows）を設定します。

4. リムーバブルドライブからローカルフォルダーまたはアップデート元として使用する共有リソースにアップデートファイルをコピーします。

5. アップデートのインストールが必要なオフラインデバイスで、Kaspersky Endpoint Security for Windows のアップデートタスクを開始します。

アップデートタスクが完了すると、デバイスの定義データベースとソフトウェアモジュールが最新の状態になります。

Web プラグインのバックアップと復元

Kaspersky Security Center Web コンソールを使用すると、Web プラグインの現在の状態をバックアップして、後から保存した状態を復元できるようになります。たとえば、新しいバージョンへのアップデート前に Web プラグインをバックアップできます。アップデート後、新しいバージョンが要件や期待にそぐわない場合に、バックアップから以前のバージョンの Web プラグインを復元できます。

Web プラグインをバックアップするには：

1. メインメニューで［**設定**］→［**Web プラグイン**］の順に移動します。

2. ［**Web プラグイン**］セクションで、バックアップする Web プラグインを選択して、［**バックアップの作成**］をクリックします。

選択した Web プラグインがバックアップされます。作成したバックアップは、［**バックアップ**］セクションで表示できます。

バックアップから Web プラグインを復元するには：

1. メインメニューで、［**設定**］→［**バックアップ**］の順にクリックします。

2. ［**バックアップ**］セクションで、復元する Web プラグインを選択して、［**バックアップから復元**］をクリックします。

選択したバックアップから Web プラグインが復元されます。

ディストリビューションポイントと接続ゲートウェイの調整

Kaspersky Security Center の管理グループ構造では、次の機能が実行されます：

- ポリシー範囲の設定

  関連する設定をデバイスに適用する別の方法として、*ポリシーのプロファイル*を使用する方法があります。この場合、ポリシーの範囲は、タグ、Active Directory 組織単位内のデバイスの場所、またはActive Directory セキュリティグループの所属で設定します。

- グループタスク範囲の設定

  管理グループの階層に基づいていない、グループタスク範囲の定義方法が存在します。これは、デバイス選択用のタスクと特定のデバイス用のタスクを使用することです。

- デバイス、仮想管理サーバー、およびセカンダリ管理サーバーへのアクセス権限の設定

- ディストリビューションポイントの割り当て

管理グループ構造を構築する際には、ディストリビューションポイントを最適に割り当てるために、組織ネットワークのトポロジーを考慮する必要があります。ディストリビューションポイントを最適に分散配置すると、組織ネットワークのトラフィック量を軽減できます。

組織の組織図とネットワークトポロジーに応じて、管理グループ構造に次の標準設定を適用できます：

- 単一のオフィス

- 複数の小規模なリモートオフィス

ディストリビューションポイントとして動作するデバイスについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

ディストリビューションポイントの標準設定：単一のオフィス

標準の「単一のオフィス」設定では、すべてのデバイスが組織ネットワーク内に置かれているため、お互いを「見る」ことができます。組織ネットワークは、いくつかの部分に区切られ（ネットワークまたはネットワークセグメント）、狭い帯域幅によって連結されるかたちで構成されている場合があります。

管理グループの構造は、次の方法で構築することが可能です：

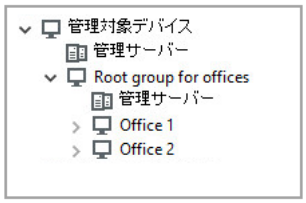
- ネットワークトポロジーを考慮に入れて管理グループの構造を構築します。管理グループの構造が、厳密にネットワークトポロジーを反映していなくても問題ありません。ネットワークが区切られた各部分と特定の管理グループの間に一致があれば十分です。ディストリビューションポイントの自動割り当てを使用するか、または手動で割り当てることができます。

- ネットワークトポロジーを考慮に入れずに管理グループの構造を構築します。この場合は、ディストリビューションポイントの自動割り当てを無効にしてから、ディストリビューションポイントとして動作する1台以上のデバイスをネットワークの区切られた各部分のルート管理グループ（たとえば、**管理対象デバイス**グループ）に対して割り当てる必要があります。ディストリビューションポイントは、すべて同じレベルに置かれ、組織ネットワーク内のすべてのデバイスを包含する同じ範囲を対象とします。この場合、各ネットワークエージェントは最短経路のディストリビューションポイントに接続します。ディストリビューションポイントへの経路は、tracert ユーティリティによって追跡できます。

ディストリビューションポイントの標準設定：複数の小規模なリモートオフィス

この標準設定は、インターネットを介して本社と通信する可能性のある多数の小規模なリモートオフィス向けの設定です。各リモートオフィスは NAT を介するようにその背後に配置されています。つまり、2 つのオフィスはお互いに分離されているため、お互いに接続することはできません。

管理グループ構造内で設定を反映させる必要があります。つまり、各リモートオフィスに対して、個別の管理グループを作成する必要があります（下の図のグループ［**Office 1**］と［**Office 2**］）。



管理グループ構造に含まれているリモートオフィス

1つのオフィスに対応する各管理グループに対して、1つまたは複数個のディストリビューションポイントを割り当てる必要があります。ディストリビューションポイントは、空きディスク容量が十分なリモートオフィスにあるデバイスである必要があります。たとえば、［**Office 1**］グループに導入されているデバイスは、［**Office 1**］管理グループに割り当てられているディストリビューションポイントにアクセスできます。

ノート PC を持ち運んでオフィス間を移動するユーザーが存在する場合は、各リモートオフィスで 2 台以上のデバイス（既存のディストリビューションポイントに加えて）を選択し、それらのデバイスをトップレベルの管理グループ（上の図の［**Root group for offices**］）用のディストリビューションポイントとして動作するように割り当てる必要があります。

例：［**Office 1**］管理グループ内にノート PC を導入しましたが、［**Office 2**］管理グループに対応するオフィスにマシンを持って移動するとします。ノート PC を移動させると、ネットワークエージェントは［**Office 1**］グループに割り当てられているネットワークエージェントへのアクセスを試行しますが、これらのディストリビューションポイントは使用不可の状態です。次に、ネットワークエージェントは、［**Root group for offices**］に割り当てられているディストリビューションポイントへのアクセスの試行を開始します。リモートオフィスはお互いに分離されているため、［**Root group for offices**］管理グループに割り当てられているディストリビューションポイントへのアクセスの試行は、ネットワークエージェントが［**Office 2**］グループ内にあるディストリビューションポイントへのアクセスを試行した際にのみ正常に実行されます。つまり、ノート PC は最初のオフィスに対応する管理グループ内に残りますが、ディストリビューションポイントについては移動後のオフィスに存在するディストリビューションポイントを使用します。

ディストリビューションポイントの割り当ての概要

管理対象デバイスをディストリビューションポイントとして、手動または自動で割り当てることができます。

管理対象デバイスをディストリビューションポイントとして手動で割り当てる場合は、ネットワーク内の任意のデバイスを選択できます。

ディストリビューションポイントを自動的に割り当てる場合、Kaspersky Security Center は、次の条件を満たす管理対象デバイスのみを選択できます：

- デバイスに少なくとも 50 GB のディスク空き容量がある。
- 管理対象デバイスが Kaspersky Security Center に直接接続されている(ゲートウェイを中継しない）。
- 管理対象デバイスがノート PC ではない。

指定された条件を満たすデバイスがネットワークにない場合、Kaspersky Security Center はデバイスをディストリビューションポイントとして自動的に割り当てません。

ディストリビューションポイントの自動的な割り当て

ディストリビューションポイント用デバイスは、自動的に割り当てることを推奨します。自動的に割り当てる場合、ディストリビューションポイントに指定するデバイスを Kaspersky Security Center が選択します。

ディストリビューションポイントを自動的に割り当てるには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
3. ［**ディストリビューションポイントを自動的に割り当て**］をオンにします。

   ディストリビューションポイントとしてのデバイスの自動割り当てが有効な場合、手動でディストリビューションポイントを設定したりディストリビューションポイントのリストを編集したりすることはできません。

4. ［**保存**］をクリックします。

管理サーバーが自動的にディストリビューションポイントを割り当てて設定します。

ディストリビューションポイントの手動での割り当て

Kaspersky Security Center で、ディストリビューションポイントとして動作するデバイスを手動で指定できます。

ディストリビューションポイント用デバイスは、自動的に割り当てることを推奨します。自動的に割り当てる場合、ディストリビューションポイントに指定するデバイスを Kaspersky Security Center が選択します。何らかの理由（たとえば、この用途専用で割り当てられたサーバーを使用する、など）により自動割り当てが選択できない場合、ディストリビューションポイント数の計算と設定を行った後に、手動でディストリビューションポイントを割り当てることができます。

ディストリビューションポイントとして動作するデバイスについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

ディストリビューションポイントとして動作するデバイスを手動で指定するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
3. ［**ディストリビューションポイントを手動で割り当て**］をオンにします。

4. ［**割り当て**］をクリックします。

5. ディストリビューションポイントとして動作させるデバイスを選択します。

   デバイスを選択する際は、ディストリビューションポイントの動作とディストリビューションポイントとして動作するデバイスの要件を確認してください。

6. 選択したディストリビューションポイントの受け持ち範囲に含める管理グループを選択します。

7. ［OK］をクリックします。

   追加されたディストリビューションポイントが、［**ディストリビューションポイント**］セクションのディストリビューションポイントのリストに表示されます。

8. 新しく追加したディストリビューションポイントをリストからクリックし、プロパティウィンドウを開きます。

9. プロパティウィンドウでディストリビューションポイントを設定します。

   - ［**全般**］セクションには、ディストリビューションポイントとクライアントデバイス間の対話の設定があります。

     - **SSL ポート**

       SSL を使用したクライアントデバイスとディストリビューションポイントの間の暗号化接続で使用する SSL ポートの番号。

       既定では、ポート 13000 が使用されます。

     - **マルチキャストを使用する**

       このオプションをオンにすると、グループ内にあるクライアントデバイスへのインストールパッケージの自動配布に IP マルチキャストが使用されます。

       IP マルチキャストを使用すると、インストールパッケージからクライアントデバイスのグループに製品をインストールするのに必要な時間が短縮されます。一方で、1 台のクライアントデバイスに製品をインストールする場合は、インストールの時間は長くなります。

     - **マルチキャスト IP アドレス**

       マルチキャストで使用される IP アドレス。224.0.0.0 ～ 239.255.255.255 の範囲で IP アドレスを定義できます。

       既定では、Kaspersky Security Center は定められた範囲内で一意の IP マルチキャストアドレスを自動的に割り当てます。

     - **IP マルチキャストポート番号**

       IP マルチキャストのポート番号。

       既定では、ポート番号は 15001 です。管理サーバーがインストールされたデバイスがディストリビューションポイントとして指定された場合、既定では SSL 接続でポート 13001 が使用されます。

     - **リモートデバイスのディストリビューションポイントアドレス**

リモートデバイスがディストリビューションポイントに接続するために使用する IPv4 アドレス。

- **アップデートの配信**

  アップデートは、次のアップデート元から管理対象デバイスに配布されます：

  - このオプションがオンの場合は、このディストリビューションポイントです。
  - このオプションがオフの場合は、管理サーバーやカスペルスキーのアップデートサーバーなどその他のディストリビューションポイントです。

  アップデートの配信にディストリビューションポイントを使用している場合は、ダウンロード数を減らすため、トラフィックを節約できます。また、管理サーバーの負荷を軽減し、ディストリビューションポイント間の負荷を移動することもできます。ネットワークのディストリビューションポイントの数を計算して、トラフィックと負荷を最適化できます。

  このオプションをオフにすると、アップデートのダウンロード数が増えて管理サーバーの負荷が増加する可能性があります。既定では、このオプションはオンです。

- **インストールパッケージの配布**

  インストールパッケージは、次の配布元から管理対象デバイスに配布されます：

  - このオプションがオンの場合は、このディストリビューションポイントです。
  - このオプションがオフの場合は、管理サーバーやカスペルスキーのアップデートサーバーなどその他のディストリビューションポイントです。

  インストールパッケージの配信にディストリビューションポイントを使用すると、ダウンロード数を減らすため、トラフィックを節約できます。また、管理サーバーの負荷を軽減し、ディストリビューションポイント間の負荷を移動することもできます。ネットワークのディストリビューションポイントの数を計算して、トラフィックと負荷を最適化できます。

  このオプションをオフにすると、アップデートのダウンロード数が増えて管理サーバーの負荷が増加する可能性があります。既定では、このオプションはオンです。

- **プッシュサーバーを実行**

  Kaspersky Security Center で、ディストリビューションポイントをモバイルプロトコルを使用して管理されているデバイスおよび Network Agent により管理されているデバイスのプッシュサーバーとして動作させることができます。たとえば、KasperskyOS デバイスと管理サーバー間の強制同期を実行可能にする時に、プッシュサーバーを有効にする必要があります。プッシュサーバーの管理デバイスの範囲は、プッシュサーバーを有効にするディストリビューションポイントの範囲と同じです。同一の管理グループに複数のディストリビューションポイントを割り当てている場合は、各ディストリビューションポイントに対してプッシュサーバーを有効に設定できます。この場合、管理サーバーはディストリビューション間の負荷を分散します。

- **プッシュサーバーのポート**

  プッシュサーバー用のポート番号です。使用されていないポートの番号を入力できます。

- ［**範囲**］セクションで、ディストリビューションポイントがアップデートを配信する範囲を指定します（管理グループまたはネットワークロケーション）。

Windows オペレーティングシステムが実行されているデバイスのみが、ネットワークロケーションを判別できます。他のオペレーティングシステムが実行されているデバイスのネットワークロケーションを判別することはできません。

- ディストリビューションポイントが管理サーバー以外のマシンで動作する場合、［**アップデート元**］セクションで、ディストリビューションポイントの更新のソースを選択できます。

  - **アップデート元**

    ディストリビューションポイントのアップデート元を選択します：

    - ディストリビューションポイントが管理サーバーからアップデートを取得できるようにするには、［**管理サーバーから取得**］をオンにします。
    - タスクを使用してディストリビューションポイントがアップデートを受信できるようにするには、［**アップデートのダウンロードタスクを使用**］をオンにして、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを指定します：
      - そのようなタスクが既にデバイスにある場合は、リストからタスクを選択します。
      - タスクがデバイスに存在しない場合、［**タスクの作成**］をクリックし、タスクを作成します。新規タスクウィザードが起動します。ウィザードの指示に従ってください。

  - **差分ファイルのダウンロード**

    このオプションで差分ファイルのダウンロードを有効にすることができます。

    既定では、このオプションはオンです。

- ［**インターネット接続設定**］サブセクションでは、インターネットアクセスを設定できます。

  - **プロキシサーバーを使用する**

    このチェックボックスをオンにすると、入力フィールドでプロキシサーバー接続を設定できます。
    既定では、このチェックボックスはオフです。

  - **プロキシサーバーアドレス**

    プロキシサーバーのアドレス。

  - **ポート番号**

    接続に使用されるポート番号。

  - **ローカルアドレスにプロキシサーバーを使用しない**

このオプションをオンにすると、ローカルネットワークのデバイスへの接続にプロキシサーバーが使用されません。

既定では、このオプションはオフです。

- **プロキシサーバー認証**

  このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。

  既定では、このチェックボックスはオフです。

- **ユーザー名**

  プロキシサーバーへの接続の確立に使用されるユーザーアカウント。

- **パスワード**

  タスクが実行されるアカウントのパスワード。

- ［**KSN プロキシ**］セクションでは、ディストリビューションポイントを使用して管理対象デバイスからの KSN リクエストを転送するようにアプリケーションを設定できます：

  - **ディストリビューションポイントで KSN プロキシを有効にする**

    ディストリビューションポイントとして使用しているデバイス上で KSN プロキシサービスが実行されます。この機能を使用することで、ネットワーク上でトラフィックを分配しなおし、最適化できます。

    ディストリビューションポイントは、Kaspersky Security Network に関する声明に記載されている KSN の統計情報をカスペルスキーに送信します。既定では、KSN 声明は「%ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula」にあります。

    既定では、このオプションはオフです。管理サーバーのプロパティウィンドウで、［**管理サーバーをプロキシサーバーとして使用する**］と［**Kaspersky Security Network への参加に同意する**］がオンになっている場合にのみ使用できます。

    アクティブ / パッシブモードのクラスターのノードをディストリビューションポイントに割り当て、ノード上で KSN プロキシサーバーを有効にできます。

  - **KSN リクエストを管理サーバーに転送する**

    ディストリビューションポイントは管理対象デバイスからの KSN リクエストを管理サーバーに転送します。

    既定では、このオプションはオンです。

  - **インターネット経由で直接 KSN クラウド / KPSN にアクセスする**

ディストリビューションポイントは管理対象デバイスからの KSN リクエストを KSN クラウドまたは KPSN に転送します。ディストリビューションポイント自体で生成された KSN リクエストも、KSN クラウドまたは KPSN に直接送信されます。

バージョン 11 以前のネットワークエージェントをインストールしているディストリビューションポイントでは、KPSN に直接アクセスできません。これらのディストリビューションポイントで KPSN リクエストを KPSN に送信するように設定を編集するには、各ディストリビューションポイントで［**KSN リクエストを管理サーバーに転送する**］をオンにします。

バージョン 12 以降のネットワークエージェントをインストールしているディストリビューションポイントでは、KPSN に直接アクセスできません。

- **KPSN への接続時に プロキシサーバーの設定を無視する**

  ディストリビューションポイントのプロパティまたはネットワークエージェントのポリシーでプロキシサーバー設定が構成済みであるにも関わらず、ネットワークアーキテクチャで KPSN を直接使用する必要がある場合は、このオプションをオンにします。このオプションをオンにしないと、管理対象アプリケーションからのリクエストが KPSN に到達できません。

  このオプションは［**インターネット経由で直接 KSN クラウド / KPSN にアクセスする**］をオンにした場合に使用できます。

- **ポート**

  管理対象デバイスが KSN プロキシサーバーへの接続に使用する TCP ポートの番号。既定のポート番号は 13111 です。

- **UDP ポートを使用**

  UDP ポートを経由して KSN プロキシサーバーと管理対象デバイスを接続する場合は、［**UDP ポートを使用**］をオンにして、UDP ポート番号を指定します。既定では、このオプションはオンです。

- **UDP ポート**

  管理対象デバイスが KSN プロキシサーバーへの接続に使用する UDP ポートの番号。KSN プロキシサーバーに接続する既定の UDP ポートは 15111 です。

- ディストリビューションポイントが管理サーバー以外のマシンで動作する場合、［**接続ゲートウェイ**］セクションで、ネットワークエージェントインスタンスと管理サーバー間の接続のゲートウェイとして機能するようにディストリビューションポイントを構成できます。

  - **接続ゲートウェイ**

    ネットワークの構成が原因で、管理サーバーとネットワークエージェント間の直接接続を確立できない場合は、ディストリビューションポイントを使用して、管理サーバーとネットワークエージェント間の接続ゲートウェイとして機能させることができます。

    ディストリビューションポイントがネットワークエージェントと管理サーバー間の接続ゲートウェイとして機能する必要がある場合は、このオプションをオンにします。既定では、このオプションはオフです。

  - **管理サーバー側からゲートウェイ接続を確立する（ゲートウェイが DMZ 内にある場合）**

管理サーバーがローカル エリア ネットワーク上の非武装地帯（DMZ）の外にある場合、リモートデバイスにインストールされたネットワークエージェントは管理サーバーに接続できません。ディストリビューションポイントをリバース接続の接続ゲートウェイとして使用できます（管理サーバーがディストリビューションポイントへの接続を確立します）。

管理サーバーを DMZ の接続ゲートウェイに接続する必要がある場合は、このオプションをオンにします。

- **Kaspersky Security Center Web コンソール用にローカルポートを開く**

  DMZ 内またはインターネット上にある Web コンソールのポートを開くために DMZ 内の接続ゲートウェイが必要な場合は、このオプションをオンにします。Web コンソールからディストリビューションポイントへの接続に使用するポート番号を指定します。既定のポート番号は 13299 です。

  このオプションは、［**管理サーバー側からゲートウェイ接続を確立する（ゲートウェイが DMZ 内にある場合）**］をオンにした場合に使用できます。

接続ゲートウェイとして機能するディストリビューションポイントを介してモバイルデバイスを管理サーバーに接続する場合、次のオプションを有効にできます。

- **モバイルデバイス用にポートを開く(管理サーバーの SSL 認証のみ)**

  接続ゲートウェイでモバイル デバイス用のポートを開き、モバイルデバイスがディストリビューションポイントへの接続に使用するポート番号を指定する必要がある場合は、このオプションをオンにします。既定のポート番号は 13292 です。モバイルデバイスは管理サーバー証明書を確認します。接続を確立するときは、管理サーバーのみが認証されます。

- **モバイルデバイス用にポートを開く（SSL 相互認証）**

  管理サーバーとモバイル デバイスの双方向認証に使用されるポートを開くために接続ゲートウェイが必要な場合は、このオプションをオンにします。モバイルデバイスは管理サーバー証明書をチェックし、管理サーバーはモバイルデバイスの証明書をチェックします。次のパラメータを指定します：

  - モバイル デバイスがディストリビューションポイントへの接続に使用するポート番号。既定のポート番号は 13293 です。
  - モバイル デバイスで使用される接続ゲートウェイの DNS ドメイン名。ドメイン名はコンマで区切ります。指定したドメイン名は、ディストリビューションポイント証明書に含まれます。モバイル デバイスが使用するドメイン名がディストリビューションポイント証明書の共通名と一致しない場合、モバイル デバイスはディストリビューションポイントに接続しません。

    デフォルトの DNS ドメイン名は、接続ゲートウェイの FQDN 名です。

どちらの場合も、証明書はディストリビューションポイントでの TLS セッションの確立時にのみチェックされます。証明書は管理サーバーによるチェックのために転送されません。モバイルデバイスとの TLS セッションが確立されると、ディストリビューションポイントは管理サーバー証明書を使用して、モバイルデバイスと管理サーバー間の同期用のトンネルを作成します。双方向 SSL 認証用にポートを開く場合、モバイルデバイス証明書を配布する唯一の方法は、インストールパッケージを使用することです。

- ディストリビューションポイントによる、Windows ドメイン、Active Directory、および IP アドレス範囲のポーリングを設定します：

- **Windows ドメイン**

  Windows ドメインに対するデバイスの検索を有効にし、スケジュールを設定できます。

- **ドメインコントローラー**

  Active Directory に対するネットワークのポーリングを有効にし、ポーリングのスケジュールを設定できます。

  Windows ディストリビューションポイントを使用する場合は、次のオプションのいずれかをオンにできます：

  - **現在の Active Directory ドメインのポーリング**
  - **Active Directory ドメインフォレストのポーリング**
  - **指定した Active Directory ドメインのみポーリング**：このオプションを選択した場合、1 つ以上の Active Directory ドメインをリストに追加してください

  ネットワークエージェント 15 がインストールされた Linux ディストリビューションポイントを使用する場合は、アドレスとユーザー資格情報を指定した Active Directory ドメインのみをポーリングできます。現在の Active Directory ドメインと Active Directory ドメインフォレストのポーリングは使用できません。

  ドメインコントローラーのデバイス検出を有効にできます。

  ［**ドメインコントローラーのポーリングを有効にする**］をオンにすると、ポーリングの対象となるドメインコントローラーを選択し、それらのポーリングスケジュールを指定することもできます。

  Linux ディストリビューションポイントを使用する場合は、［**指定したドメインのポーリング**］セクションで［**追加**］をクリックし、ドメインコントローラーのアドレスとユーザー資格情報を指定します。

  Windows ディストリビューションポイントを使用する場合は、次のオプションのいずれかをオンにできます：

  - **現在のドメインのポーリング**
  - **ドメインフォレスト全体のポーリング**
  - **指定したドメインのポーリング**

- **IP アドレス範囲**

デバイスの検索は IPv4 範囲および IPv6 ネットワークで有効にできます。

［**IP アドレス範囲のポーリングを有効にする**］をオンにすると、対象範囲を追加して実行スケジュールを設定できます。スキャン対象範囲のリストに IP アドレス範囲を追加できます。

［**Zeroconf を使用して IPv6 ネットワークのポーリングを実行する**］をオンにすると、ディストリビューションポイントは自動的にゼロコンフィギュレーションネットワーキング（「*Zeroconf*」とも表記）を使用して IPv6 ネットワークのポーリングを行います。この場合、ディストリビューションポイントはネットワーク全体を検索するため、指定した IP 範囲は無視されます。ディストリビューションポイントが Linux を実行している場合は、［**Zeroconf を使用して IPv6 ネットワークのポーリングを実行する**］を使用できます。Zeroconf IPv6 ポーリングを使用するには、ディストリビューションポイントで avahi-browse ユーティリティをインストールする必要があります。

- ［**詳細**］セクションで、配信されたデータの格納用にディストリビューションポイントが使用するフォルダーを指定します：
  - **既定のフォルダーを使用する**

    このオプションをオンにすると、ディストリビューションポイント上でネットワークエージェントがインストールされているフォルダーが使用されます。

  - **指定したフォルダーを使用する**

    このオプションをオンにすると、この下のフィールドで、フォルダーのパスを指定できます。ディストリビューションポイントのローカルフォルダーまたは組織ネットワーク内の任意のデバイス上にあるフォルダーを指定できます。

    ネットワークエージェントの実行時にディストリビューションポイントで使用されるユーザーアカウントには、指定したフォルダーへの読み取りおよび書き込みアクセス権限が必要です。

10. ［**OK**］をクリックします。

選択されたデバイスがディストリビューションポイントとして使用されます。

管理グループに割り当てられたディストリビューションポイントのリストの編集

特定の管理グループに割り当てられたディストリビューションポイントのリストを表示し、ディストリビューションポイントを追加または削除してこのリストを編集できます。

管理グループに割り当てられたディストリビューションポイントのリストの表示と編集を行うには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. 管理対象デバイスのリストの上にある［**現在のパス**］フィールドで、パスリンクをクリックします。
3. 表示される左側のペインで、割り当てられたディストリビューションポイントを表示する管理グループを選択します。

   これにより、［**ディストリビューションポイント**］メニュー項目をオンにします。

4. メインメニューで、［**アセット（デバイス）**］→［**ディストリビューションポイント**］の順に選択します。

5. 管理グループに新しいディストリビューションポイントを追加するには、管理対象デバイスのリストの上にある［**割り当て**］をクリックし、開いたペインからデバイスを選択します。

6. 割り当てられたディストリビューションポイントを削除するには、リストからデバイスを選択し、［**割り当て解除**］をクリックします。

変更内容に応じて、新しいディストリビューションポイントがリストに追加されるか、既存のディストリビューションポイントがリストから削除されます。

強制同期

Kaspersky Security Center は管理対象デバイスのステータス、設定、タスクおよびポリシーを自動的に同期しますが、特定のデバイスに対して強制的に同期を実行したいという場合があります。このような場合、次のデバイスに対して強制的に同期を実行することができます：

- ネットワークエージェントが実行されているデバイス
- KasperskyOS を実行しているデバイス

  KasperskyOS デバイスに対して強制的に同期を実行する前に、デバイスがディストリビューションポイントの範囲に含まれていることと、ディストリビューションポイントでプッシュサーバーが有効になっていることを確認してください。
- iOS デバイス
- Android デバイス

  Android デバイスに対して強制同期を実行する前に、Firebase Cloud Messaging を設定しておく必要があります。

単一デバイスの同期

管理サーバーと管理対象デバイスの同期を強制的に実行するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
2. 管理サーバーと同期させるデバイスの名前をクリックします。

   プロパティウィンドウの［**全般**］セクションが表示されます。
3. ［**強制同期**］をクリックします。

指定したデバイスと管理サーバーの同期が実行されます。

複数デバイスの同期

管理サーバーと複数の管理対象デバイスの同期を強制的に実行するには：

1. 管理グループまたはデバイスの抽出からデバイスリストを開きます：

- メインメニューで［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動し、管理対象デバイスのリストの上にある［**現在のパス**］フィールドのパスリンクをクリックして、同期するデバイスを含む管理グループを選択します。
- デバイスの抽出を実行してデバイスリストを表示します。

2. 管理サーバーと同期するデバイスに隣接するチェックボックスをオンにします。
3. 管理対象デバイスのリストの上にある省略記号ボタン（...）、［**強制同期**］をクリックします。
   指定したデバイスと管理サーバーの同期が実行されます。
4. デバイスリストで、指定したデバイスでの前回の管理サーバーへの接続の時間が現在の時間に変更されていることが確認できます。時間が変更されていない場合は、［**更新**］をクリックしてページの内容を更新します。

選択したデバイスのデータが管理サーバーと同期します。

ポリシーの配信時間の表示

管理サーバーでカスペルスキー製品のポリシーを変更した後、変更後のポリシーが特定の管理対象デバイスに配信されたかどうかを管理者は確認できます。ポリシーは、定期的な同期または強制的な同期によって配信されます。

管理対象デバイスに製品ポリシーが配信された日時を表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
2. 管理サーバーと同期させるデバイスの名前をクリックします。
   プロパティウィンドウの［**全般**］セクションが表示されます。
3. ［**アプリケーション**］タブを選択します。
4. ポリシーを同期した日時を表示する製品を選択します。
   製品ポリシーのプロパティウィンドウの［**全般**］セクションが表示され、ポリシーの配信日時を確認できます。

プッシュサーバーの有効化

Kaspersky Security Center で、ディストリビューションポイントをモバイルプロトコルを使用して管理されているデバイスおよび Network Agent により管理されているデバイスのプッシュサーバーとして動作させることができます。たとえば、KasperskyOS デバイスと管理サーバー間の強制同期を実行可能にする時に、プッシュサーバーを有効にする必要があります。プッシュサーバーの管理デバイスの範囲は、プッシュサーバーを有効にするディストリビューションポイントの範囲と同じです。同一の管理グループに複数のディストリビューションポイントを割り当てている場合は、各ディストリビューションポイントに対してプッシュサーバーを有効に設定できます。この場合、管理サーバーはディストリビューション間の負荷を分散します。

ディストリビューションポイントをプッシュサーバーとして使用して、管理対象デバイスと管理サーバー間の継続的な接続を確認できます。ローカルタスクの実行と停止、管理対象アプリケーションの統計の受信、トンネルの作成など、一部の操作には継続的な接続が必要です。ディストリビューションポイントをプッシュサーバーとして使用する場合は、管理対象デバイスで［**管理サーバーから切断しない**］をオンにしたり、ネットワークエージェントの UDP ポートにパケットを送信したりする必要はありません。

プッシュサーバーは、最大 50,000 件の同時接続の負荷をサポートします。

ディストリビューションポイントでプッシュサーバーを有効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
3. プッシュサーバーを有効にするディストリビューションポイントの名前をクリックします。
   ディストリビューションポイントのプロパティウィンドウが開きます。
4. ［**全般**］セクションで、［**プッシュサーバーを実行**］をオンにします。
5. ［**プッシュサーバーのポート**］フィールドで、ポート番号を入力します。使用されていないポートの番号を入力できます。
6. ［**リモートホストのアドレス**］フィールドで、ディストリビューションポイントデバイスの IP アドレスまたは名前を指定します。
7. ［**OK**］をクリックします。

選択したディストリビューションポイントでプッシュサーバーが有効になります。

クライアントデバイス上のサードパーティ製品の管理

このセクションでは、クライアントデバイスにインストールされているサードパーティ製ソフトウェアの管理に関わる Kaspersky Security Center の機能について説明します。

サードパーティ製品について

Kaspersky Security Center を使用してクライアントデバイスにインストールされたサードパーティ製のソフトウェアをアップデートしたり脆弱性を修正したりできます。Kaspersky Security Center はサードパーティ製ソフトウェアを最新バージョンにのみアップデートします。以下のリストに、Kaspersky Security Center を使用してアップデートできるサードパーティ製ソフトウェアを記載します。

サードパーティ製ソフトウェアのリストはアップデートまたは新しい製品で拡張されることがあります。ユーザーのデバイスにインストールされたサードパーティ製ソフトウェアを Kaspersky Security Center でアップデートできるかどうかは Kaspersky Security Center Web コンソールで使用可能なアップデートのリストで確認できます。

- 7-Zip Developers：7-Zip
- Adobe Systems：
  - Adobe Acrobat DC

    - Adobe Acrobat Reader DC
    - Adobe Acrobat
    - Adobe Reader
    - Adobe Shockwave Player
- AIMPDevTeam：AIMP
- ALTAP：Altap Salamander
- Apache Software Foundation：Apache Tomcat
- Apple：
    - Apple iTunes
    - Apple QuickTime
- Armory Technologies, Inc.：Armory
- Cerulean Studios：Trillian Basic
- Ciphrex Corporation：mSIGNA
- Cisco：Cisco Jabber
- Code Sector：TeraCopy
- Codec Guide：
    - K-Lite Codec Pack Basic
    - K-Lite Codec Pack Full
    - K-Lite Codec Pack Mega
    - K-Lite Codec Pack Standard
- DbVis Software AB：DbVisualizer
- Decho Corp.：
    - Mozy Enterprise
    - Mozy Home
    - Mozy Pro
- Dominik Reichl：KeePass Password Safe
- Don HO don.h@free.fr：Notepad++
- DoubleGIS：2GIS

- Dropbox, Inc.：Dropbox
- EaseUs：EaseUS Todo Backup Free
- Electrum Technologies GmbH：Electrum
- Enter Srl：Iperius Backup
- Eric Lawrence：Fiddler
- EverNote：EverNote
- Exodus Movement Inc：Exodus
- EZB Systems：UltraISO
- Famatech:
  - Radmin
  - Remote Administrator
- Far Manager：FAR Manager
- FastStone Soft：FastStone Image Viewer
- FileZilla Project：FileZilla
- Firebird Developers：Firebird
- Foxit Corporation：
  - Foxit Reader
  - Foxit Reader Enterprise
- Free Download Manager.ORG：Free Download Manager
- GIMP project：GIMP
- GlavSoft LLC.：TightVNC
- GNU Project：Gpg4win
- Google：
  - Google Earth
  - Google Chrome
  - Google Chrome Enterprise
  - Google Earth Pro
- Inkscape Project：Inkscape

- IrfanView：IrfanView
- iterate GmbH：Cyberduck
- Logitech：SetPoint
- LogMeIn, Inc.：
  - LogMeIn
  - Hamachi
  - LogMeIn Rescue Technician Console
- Martin Prikryl：WinSCP
- Microsoft: SQL Server Management Studio
- Mozilla Foundation：
  - Mozilla Firefox
  - Mozilla Firefox ESR
  - Mozilla SeaMonkey
  - Mozilla Thunderbird
- New Cloud Technologies Ltd：MyOffice Standard.Home Edition
- OpenOffice.org: OpenOffice
- Oracle Corporation：
  - Oracle Java JRE
  - Oracle VirtualBox
- PDF44：PDF24 MSI / EXE
- Piriform：
  - CCleaner
  - Defraggler
  - Recuva
  - Speccy
- Postgresql：PostgreSQL
- RealNetworks：RealPlayer Cloud
- RealVNC：

    - RealVNC Server
    - RealVNC Viewer
- Right Hemisphere Inc.：SAP Visual Enterprise Viewer (Complete/Minimum)
- Simon Tatham：PuTTY
- Skype Technologies：Skype for Windows
- Sober Lemur S.a.s.：
    - PDFsam Basic
    - PDFsam Visual
- Softland：FBackup
- Splashtop Inc.：Splashtop Streamer
- Stefan Haglund, Fredrik Haglund, Florian Schmitz：CDBurnerXP
- Sublime HQ Pty Ltd：Sublime Text
- TeamViewer GmbH：
    - TeamViewer Host
    - TeamViewer
- Telegram Messenger LLP：Telegram Desktop
- The Document Foundation：
    - LibreOffice
    - LibreOffice HelpPack
- The Git Development Community：
    - Git for Windows
    - Git LFS
- The Pidgin developer community：Pidgin
- TortoiseSVN Developers：TortoiseSVN
- VideoLAN：VLC media player
- VMware：
    - VMware Player
    - VMware Workstation

- WinRAR Developers：WinRAR
- WinZip：WinZip
- Wireshark Foundation：Wireshark
- Wrike：Wrike
- Zimbra：Zimbra Desktop

サードパーティ製ソフトウェアのアップデートのインストール

Kaspersky Security Center では、管理対象デバイスにインストールされたサードパーティ製ソフトウェアのアップデートを管理し、Microsoft 製アプリケーションや他のソフトウェア会社の製品に含まれる脆弱性を、必要なアップデートをインストールすることで修正できます。

Kaspersky Security Center は、*脆弱性とアプリケーションのアップデートの検索*タスクでアップデートを検索します。タスクが完了すると、管理サーバーはタスクのプロパティで指定したデバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。適用可能なアップデートの情報を確認した後、アップデートをデバイスにインストールできます。

Kaspersky Security Center はいくつかのアプリケーションについて、古いバージョンを削除して新しいバージョンをインストールして更新します。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

セキュリティ上の理由から、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートすべてに対して、カスペルスキーの技術によるマルウェアのスキャンが自動的に実行されます。この技術は自動的なファイルのチェックに使用され、ウイルススキャン、Sandbox 環境における静的分析、動的分析、ふるまい分析、機械学習が含まれます。

カスペルスキーは、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートを手動で分析することはありません。さらに、カスペルスキーの専門家は脆弱性（既知または未知）や文書化されていないアップデートの機能について確認したり、上記で指定されているもの以外のアップデートの分析を行ったりすることはありません。

サードパーティ製ソフトウェアのアップデートのインストールタスク

サードパーティ製ソフトウェアのアップデートのメタデータがリポジトリにダウンロードされると、以下のタスクを使用してクライアントデバイスにアップデートをインストールできます：

- *アップデートのインストールと脆弱性の修正*タスク

  *アップデートのインストールと脆弱性の修正*タスクは、Windows Update サービス経由で提供される場合も含めた Microsoft アプリケーションのアップデートとその他の製造元の製品のアップデートのインストールに使用されます。このタスクは、脆弱性とパッチ管理機能を利用できるライセンスを使用している場合にのみ作成できます。

このタスクが完了すると、管理対象デバイスにアップデートが自動的にインストールされます。新しいアップデートのメタデータが管理サーバーのリポジトリにダウンロードされると、Kaspersky Security Center はそのアップデートがアップデートルールで指定されている条件を満たすかどうかをチェックします。条件を満たす新しいアップデートはすべて、次回のタスク実行時に自動的にダウンロードされてインストールされます。

- *Windows Update 更新プログラムのインストール*タスク

  ［*Windows Update 更新プログラムのインストール*］タスクを使用するために、特別なライセンスは必要ありません。ただし、インストールできるのは Windows Update の更新プログラムのみです。

  このタスクが完了すると、タスクのプロパティで指定したアップデートのみがインストールされます。タスクの作成後、管理サーバーのリポジトリにダウンロードされた新しいアップデートをインストールする場合は、既存のタスクに目的のアップデートを追加するか、新たに Windows Update 更新プログラムのインストールタスクを作成する必要があります。

管理サーバーの WSUS サーバーとしての使用

Microsoft Windows の使用可能な更新プログラムの情報は、Windows Update サービスによって提供されます。管理サーバーは Windows Server Update Service（WSUS）サーバーとして使用できます。管理サーバーを WSUS サーバーとして使用するには、Windows Update の同期の実行タスクを作成し、ネットワークエージェントのポリシーで［**管理サーバーを WSUS サーバーとして使用する**］をオンにする必要があります。Windows Update とのデータの同期の設定が終わると、管理サーバーは一元管理モードで、また設定された頻度で、デバイス上の Windows Update サービスにアップデートを提供します。

シナリオ：サードパーティ製ソフトウェアのアップデート

このセクションでは、クライアントデバイスにインストールされているサードパーティ製ソフトウェアをアップデートするシナリオについて説明します。「サードパーティ製ソフトウェア」とは、Microsoft およびその他の製造元が提供しているアプリケーションを指します。Microsoft 製品のアップデートの情報は、Windows Update サービスによって提供されます。

必須条件

Microsoft 製品以外のサードパーティ製ソフトウェアのアップデートをインストールするには、管理サーバーはインターネットに接続している必要があります。

既定では、管理サーバーが管理対象デバイスに Microsoft 製品のアップデートをインストールするためにインターネット接続は必要ありません。たとえば、管理対象デバイスは、Microsoft Update サーバーから直接、または組織のネットワークに展開されている Microsoft Windows Server Update Services（WSUS）を使用して WindowsServer から、Microsoft ソフトウェアのアップデートをダウンロードできます。管理サーバーを WSUS サーバーとして使用する場合は、管理サーバーがインターネットに接続されている必要があります。

実行するステップ

サードパーティ製ソフトウェアのアップデートは段階的に進行します：

1. **必要なアップデートの検索**

管理対象デバイスに必要なサードパーティ製ソフトウェアのアップデートを検索するには、［*脆弱性とアプリケーションのアップデートの検索*］タスクを実行します。タスクが完了すると、Kaspersky Security Center はタスクのプロパティで指定したデバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。

［*脆弱性とアプリケーションのアップデートの検索*］タスクは、管理サーバークイックスタートウィザードによって自動的に作成されます。ウィザードを実行していない場合は、次の手順に進む前にタスクを手動で作成するか、クイックスタートウィザードを実行してください。

実行手順の説明：

- 管理コンソール：アプリケーションの脆弱性スキャン、脆弱性とアプリケーションのアップデートの検索タスクのスケジュール設定
- Kaspersky Security Center Web コンソール：脆弱性とアプリケーションのアップデートの検索タスクの作成、脆弱性とアプリケーションのアップデートの検索タスクの設定

2 検出されたアップデートのリストの分析

［**ソフトウェアのアップデート**］リストを確認して、どのアップデートをインストールするかを決定します。それぞれのアップデートの詳細情報を確認するには、リスト内のアップデートの名前をクリックします。リスト内のそれぞれのアップデートについて、クライアントデバイスへのアップデートのインストールに関する統計情報を表示することもできます。

実行手順の説明：

- 管理コンソール：適用可能なアップデートに関する情報の表示
- Kaspersky Security Center Web コンソール：サードパーティ製品の使用可能なアップデートに関する情報の表示

3 アップデートのインストールの設定

Kaspersky Security Center でサードパーティ製ソフトウェアのアップデートのリストの取得が完了すると、*アップデートのインストールと脆弱性の修正タスク*または *Windows Update 更新プログラムのインストール*タスクを使用して、クライアントデバイスにアップデートをインストールできます。いずれかのタスクを作成してください。［**タスク**］タブまたは［**ソフトウェアのアップデート**］リストを使用してこれらのタスクを作成できます。

*アップデートのインストールと脆弱性の修正*タスクは、Windows Update サービス経由で提供される場合も含めた Microsoft アプリケーションのアップデートとその他の製造元の製品のアップデートのインストールに使用されます。このタスクは、脆弱性とパッチ管理機能を使用できるライセンスを使用している場合にのみ作成できます。

［*Windows Update 更新プログラムのインストール*］タスクを使用するために、特別なライセンスは必要ありません。ただし、インストールできるのは Windows Update の更新プログラムのみです。

一部のソフトウェアのアップデートのインストールでは、インストールするために使用許諾契約書に同意する必要があります。使用許諾契約書に同意しない場合、アップデートはインストールされません。

アップデートのインストールタスクをスケジュールを指定して開始できます。タスクのスケジュールを指定する場合は、［*脆弱性とアプリケーションのアップデートの検索*］タスクが完了してからアップデートのインストールタスクが開始されるようにしてください。

実行手順の説明：

- 管理コンソール：アプリケーションの脆弱性の修正、適用可能なアップデートに関する情報の表示
- Kaspersky Security Center Web コンソール：の作成アップデートのインストールと脆弱性の修正タスク、Windows Update 更新プログラムのインストールタスクの作成、サードパーティ製品の使用可能なアップデートに関する情報の表示

4 タスクのスケジュール設定

アップデートのリストを最新の状態に維持するため、［*脆弱性とアプリケーションのアップデートの検索*］タスクが定期的に自動で実行されるようにスケジュールを指定してください。既定では、*脆弱性とアプリケーションのアップデートの検索*タスクは手動で開始するように設定されています。

*アップデートのインストールと脆弱性の修正*タスクを作成している場合は、実行頻度が*脆弱性とアプリケーションのアップデートの検索*タスクの実行頻度以下となるようにスケジュールを設定します。*Windows Update 更新プログラムのインストール*タスクのスケジュールを設定する場合は、タスクを実行する前に毎回、インストールするアップデートのリストを指定する必要があることに注意してください。

タスクのスケジュールを指定する場合は、*脆弱性とアプリケーションのアップデートの検索*タスクが完了してからアップデートのインストールタスクが開始されるようにしてください。

5. **ソフトウェアアップデートの拒否と承認（必要に応じて実施）**

アップデートのインストールと脆弱性の修正タスクを作成している場合は、タスクのプロパティでアップデートのインストールルールを指定できます。Windows Update 更新プログラムのインストールタスクを作成している場合は、この手順はスキップしてください。

それぞれのルールで、アップデートの次のようなステータスに応じて、インストールするアップデートを指定できます：*未定義*、*承認*、*拒否*。たとえば、サーバー向けのタスクとして、「*承認*」ステータスの Windows Update 更新プログラムのインストールのみを許可するようにルールを設定したタスクを設定するなどの使用方法が考えられます。この場合、インストールするアップデートに手動で「*承認*」ステータスを設定します。このように設定すると、Windows Update 更新プログラムでもステータスが「*未定義*」または「*拒否*」のアップデートは、タスクでインストール先に指定したサーバーにインストールされません。

アップデートのインストールを管理するための「*承認*」ステータスの使用は、アップデート量が少ない場合に効率的です。複数のアップデートをインストールするには、［*アップデートのインストールと脆弱性の修正*］タスクで構成できるルールを使用します。ルールで指定された基準を満たさない特定のアップデートに対してのみ、「*承認*」ステータスを設定することを推奨します。大量のアップデートを手動で承認すると、管理サーバーのパフォーマンスが低下し、サーバーが過負荷状態になる場合があります。

既定では、ダウンロードされたソフトウェアアップデートのステータスは「*未定義*」です。［**ソフトウェアのアップデート**］リストで、アップデートのステータスを「*承認*」または「*拒否*」に変更できます（［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動して操作）。

実行手順の説明：

- 管理コンソール：ソフトウェアアップデートの拒否と承認
- Kaspersky Security Center Web コンソール：サードパーティ製ソフトウェアのアップデートの拒否と承認

6. **管理サーバーが Windows Server Update Service（WSUS）サーバーとして動作するように設定（省略可能）**

既定では、Windows Update 更新プログラムは Microsoft のサーバーから管理対象デバイスにダウンロードされます。この設定を変更して、管理サーバーを WSUS サーバーとして使用するように設定できます。この場合、管理サーバーは指定した頻度で、Windows Update サービスとアップデートに関するデータの同期を実行し、ネットワークデバイスに一元的に Windows Update の更新プログラムを提供します。

管理サーバーを WSUS サーバーとして使用するには、Windows Update の同期の実行タスクを作成し、ネットワークエージェントのポリシーで［**管理サーバーを WSUS サーバーとして使用する**］をオンにする必要があります。

実行手順の説明：

- 管理コンソール：Windows Update の更新プログラムと管理サーバーとの同期、ネットワークエージェントポリシーでの Windows アップデートの設定
- Kaspersky Security Center Web コンソール：Windows Update の同期の実行タスクの作成

7. **アップデートのインストールタスクの実行**

アップデートのインストールと脆弱性の修正タスクまたは *Windows Update 更新プログラムのインストール* タスクを開始します。これらのタスクを開始すると、管理対象デバイスにアップデートがダウンロードされインストールされます。タスクが完了したら、タスクリストでのタスクのステータスが［*正常終了*］になっていることを確認します。

8. **サードパーティ製ソフトウェアのアップデートのインストール結果のレポートの作成（省略可能）**

   アップデートのインストールに関する詳細な統計情報を確認するには、［**サードパーティ製ソフトウェアのアップデートのインストール結果に関するレポート**］を作成します。

   実行手順の説明：

   - 管理コンソール：レポートの作成と表示
   - Kaspersky Security Center Web コンソール：レポートの生成と表示

結果

*アップデートのインストールと脆弱性の修正*タスクを作成し設定した場合は、管理対象デバイスにアップデートが自動的にインストールされます。新しいアップデートが管理サーバーのリポジトリにダウンロードされると、Kaspersky Security Center はそのアップデートがアップデートルールで指定されている条件を満たすかどうかをチェックします。条件を満たす新しいアップデートはすべて、次回のタスク実行時に自動的にインストールされます。

*Windows Update 更新プログラムのインストール*タスクを作成した場合は、*Windows Update 更新プログラムのインストール*タスクのプロパティで指定したアップデートのみがインストールされます。タスクの作成後、管理サーバーのリポジトリにダウンロードされた新しいアップデートをインストールする場合は、既存のタスクに目的のアップデートを追加するか、新たに *Windows Update 更新プログラムのインストール*タスクを作成する必要があります。

サードパーティ製ソフトウェアのアップデートのインストール

以下のタスクのいずれかを作成し実行して、管理対象デバイスにサードパーティ製ソフトウェアのアップデートをインストールできます：

- *アップデートのインストールと脆弱性の修正*

  ［*アップデートのインストールと脆弱性の修正*］タスクは、脆弱性とパッチ管理機能のライセンスをお持ちの場合にのみ作成できます。このタスクを使用して、Microsoft が提供する Windows Update 更新プログラムと他の製造元による製品のアップデートの両方をインストールできます。

- *Windows Update 更新プログラムのインストール*

  *Windows Update 更新プログラムのインストール*タスクを使用して Windows Update 更新プログラムのみをインストールできます。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

オプションとして、次の方法で必要なアップデートをインストールするタスクを作成できます：

- アップデートリストを開き、インストールするアップデートを指定する。

その結果、選択したアップデートをインストールする新しいタスクが作成されます。オプションとして、選択したアップデートを既存のタスクに追加できます。

- アップデートのインストールウィザードを実行する。

  アップデートのインストールウィザードの機能は、脆弱性とパッチ管理ライセンスがある場合にのみ使用できます。

  このウィザードを使用すると、アップデートのインストールタスクの作成と設定手順が簡略化され、インストールするのと同じアップデートで構成される冗長なタスクを作成せずに済みます。

アップデートリストを使用してサードパーティ製ソフトウェアのアップデートをインストールする

アップデートのリストを使用して、サードパーティ製ソフトウェアのアップデートをインストールするには：

1. アップデートのリストの1つを開きます：

   - 一般的なアップデートのリストを開くには、メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動します。
   - 管理対象デバイスのアップデートのリストを開くには、メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］→［<デバイス名>］→［**詳細**］→［**適用可能なアップデート**］の順に移動します。
   - 特定のアプリケーションのアップデートのリストを開くには、メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］→［<製品名>］→［**適用可能なアップデート**］の順に移動します。

   適用可能なアップデートのリストが表示されます。

2. インストールするアップデートに隣接するチェックボックスをオンにします。

3. ［**アップデートのインストール**］をクリックします。

   インストールするソフトウェアのアップデートによっては、使用許諾契約書に同意する必要があります。使用許諾契約書に同意しない場合、ソフトウェアのアップデートはインストールされません。

4. 次のいずれかのオプションをオンにします：

   - **新規タスク**

     新規タスクウィザードが起動します。脆弱性とパッチ管理 ライセンスをお持ちの場合は、［*アップデートのインストールと脆弱性の修正*］タスクが事前選択されています。ライセンスをお持ちでない場合は、［*Windows Update 更新プログラムのインストール*］タスクが事前選択されています。ウィザードの手順に従って、タスクの作成を完了します。

   - **アップデートのインストール（指定したタスクにルールを追加）**

     選択したアップデートを追加するタスクを選択します。脆弱性とパッチ管理 ライセンスをお持ちの場合は、［*アップデートのインストールと脆弱性の修正*］タスクを選択します。選択したアップデートをインストールするための新しいルールが、選択したタスクに自動的に追加されます。ライセンスをお持ちでない場合は、*Windows Update 更新プログラムのインストール*タスクを選択します。選択したアップデートがタスクのプロパティに追加されます。

     タスクのプロパティウィンドウが開きます。［**保存**］をクリックして変更を保存します。

タスクの作成を選択した場合は、タスクが作成され、タスクリスト（［**アセット（デバイス）**］→［**タスク**］）に表示されます。既存のタスクにアップデートを追加することを選択した場合、アップデートはタスクのプロパティに保存されます。

サードパーティ製ソフトウェアのアップデートをインストールするには、［*アップデートのインストールと脆弱性の修正*］タスク、または［*Windows Update 更新プログラムのインストール*］タスクを開始します。これらのタスクは手動によって、または開始するタスクのプロパティでスケジュール設定を指定することによって開始できます。タスクのスケジュールを指定する場合は、［*脆弱性とアプリケーションのアップデートの検索*］タスクが完了してからアップデートのインストールタスクが開始されるようにしてください。

アップデートのインストールウィザードを使用してサードパーティ製ソフトウェアのアップデートをインストールする

アップデートのインストールウィザードの機能は、脆弱性とパッチ管理ライセンスがある場合にのみ使用できます。

アップデートのインストールウィザードを使用して、サードパーティ製ソフトウェアのアップデートをインストールするタスクを作成するには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動します。
   適用可能なアップデートのリストが表示されます。
2. インストールするアップデートに隣接するチェックボックスをオンにします。
3. ［**アップデートのインストールウィザードを実行**］をクリックします。
   アップデートのインストールウィザードが起動します。［**アップデートのインストールタスクを選択する**］ページには、次の種別の既存の全タスクのリストが表示されます。
   - *アップデートのインストールと脆弱性の修正*
   - *Windows Update 更新プログラムのインストール*
   - *脆弱性の修正*

   最後の 2 つの種別のタスクを変更して新しいアップデートをインストールすることはできません。新しいアップデートをインストールする際に使用できるのは、［*アップデートのインストールと脆弱性の修正*］タスクのみです。
4. 選択したアップデートをインストールするタスクのみをウィザードに表示するには、［**このアップデートをインストールするタスクのリストを表示**］をオンにします。
5. 目的の対象を追加します：
   - タスクを開始するには、タスク名の横にあるチェックボックスをオンにして、［**開始**］をクリックします。
   - 既存のタスクに新しいルールを追加するには：
     a. タスク名に隣接するチェックボックスをオンにし、［**ルールの追加**］をクリックします。
     b. 開いたページで、新しいルールを構成します：
     - **この重要度レベルのアップデートのインストールルール**

ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

既定では、このオプションはオフです。

- **MSRC に基づく重要度レベルのアップデートのインストールルール**

  ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

  このオプションをオンにすると（Windows Update 更新プログラムでのみ使用可能）、MSRC（Microsoft Security Response Center）が設定する重要度レベルが、リストで選択した値（**低**、**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみがアップデートによって修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

  このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

  既定では、このオプションはオフです。

- **この製造元によるアップデートのインストールルール**

  このオプションは、サードパーティ製アプリケーションのアップデートにのみ使用可能です。Kaspersky Security Centerは、選択したアップデートと同じベンダーによって作成されたアプリケーションに関連するアップデートのみをインストールします。拒否された更新および他のベンダーが作成したアプリケーションの更新はインストールされません。

  既定では、このオプションはオフです。

- **種別「」のアップデートのインストールルール**
- **選択したアップデートのインストールルール**
- **選択したアップデートを承認**

  選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

  既定では、このオプションはオフです。

- **選択したアップデートのインストールに必要な以前のアップデートをすべて自動的にインストールする**

選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、このオプションをオンのままにします。

このオプションをオフにすると、選択したバージョンのアプリケーションのみがインストールされます。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、このオプションをオフにします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

たとえば、デバイスにアプリケーションのバージョン 3 がインストールされていて、バージョン 5 にアップデートしたいが、バージョン 5 はバージョン 4 経由のみでしかインストールできない状況を想定します。このオプションをオンにすると、先にバージョン 4 をインストールし、続いてバージョン 5 をインストールします。このオプションをオフにすると、アプリケーションのアップデートは失敗します。

既定では、このオプションはオンです。

c. ［**追加**］をクリックします。

- タスクを作成するには：

  a. ［**新規タスク**］をクリックします。

  b. 開いたページで、新しいルールを構成します：

  - **この重要度レベルのアップデートのインストールルール**

    ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

    このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

    このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

    既定では、このオプションはオフです。

  - **MSRC に基づく重要度レベルのアップデートのインストールルール**

    ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

    このオプションをオンにすると（Windows Update 更新プログラムでのみ使用可能）、MSRC（Microsoft Security Response Center）が設定する重要度レベルが、リストで選択した値（**低**、**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみがアップデートによって修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

    このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

    既定では、このオプションはオフです。

  - **この製造元によるアップデートのインストールルール**

このオプションは、サードパーティ製アプリケーションのアップデートにのみ使用可能です。Kaspersky Security Centerは、選択したアップデートと同じベンダーによって作成されたアプリケーションに関連するアップデートのみをインストールします。拒否された更新および他のベンダーが作成したアプリケーションの更新はインストールされません。

既定では、このオプションはオフです。

- **種別「」のアップデートのインストールルール**
- **選択したアップデートのインストールルール**
- **選択したアップデートを承認**

  選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

  既定では、このオプションはオフです。

- **選択したアップデートのインストールに必要な以前のアップデートをすべて自動的にインストールする**

  選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、このオプションをオンのままにします。

  このオプションをオフにすると、選択したバージョンのアプリケーションのみがインストールされます。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、このオプションをオフにします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

  たとえば、デバイスにアプリケーションのバージョン 3 がインストールされていて、バージョン 5 にアップデートしたいが、バージョン 5 はバージョン 4 経由のみでしかインストールできない状況を想定します。このオプションをオンにすると、先にバージョン 4 をインストールし、続いてバージョン 5 をインストールします。このオプションをオフにすると、アプリケーションのアップデートは失敗します。

  既定では、このオプションはオンです。

c. ［**追加**］をクリックします。

タスクの開始を選択した場合は、ウィザードを閉じることができます。タスクはバックグラウンドモードで完了します。追加の操作は必要ありません。

ルールを既存のタスクに追加することを選択した場合は、タスクのプロパティウィンドウが開きます。新しいルールは既にタスクのプロパティに追加されています。ルールまたはその他のタスク設定を表示あるいは変更できます。［**保存**］をクリックして変更を保存します。

タスクの作成を選択した場合は、新規タスクウィザードで引き続きタスクを作成します。アップデートのインストールウィザードで追加した新しいルールが、新規タスクウィザードに表示されます。タスク追加ウィザードを完了すると、［*アップデートのインストールと脆弱性の修正*］タスクがタスクリストに追加されます。

［脆弱性とアプリケーションのアップデートの検索］タスクの作成

［脆弱性とアプリケーションのアップデートの検索］タスクを使用して、Kaspersky Security Center は管理対象デバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。

［脆弱性とアプリケーションのアップデートの検索］タスクは、クイックスタートウィザードの実行時に自動作成されます。ウィザードを実行していない場合も、手動でタスクを作成できます。

［脆弱性とアプリケーションのアップデートの検索］タスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**脆弱性とアプリケーションのアップデートの検索**］タスク種別を選択します。
4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクを割り当てるデバイスを選択します。
6. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
7. ［**作成**］をクリックします。

   タスクが作成され、タスクリストに表示されます。
8. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。
9. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。
10. ［**アプリケーション設定**］タブで、次の設定を指定します：

    - **Microsoft による脆弱性とアップデートのリストを検索する**

      脆弱性とアップデートの検索時に、Kaspersky Security Center は、現時点で適用可能な Microsoft Update のアップデート元からの該当する Microsoft Update の情報を使用します。

      Microsoft Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

      既定では、このオプションはオンです。

    - **アップデートサーバーに接続してアップデートを取得**

管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元として指定した場所に接続します。以下のサーバーを Microsoft Update のアップデート元として動作させることができます：

- Kaspersky Security Center 管理サーバー（詳細は、「ネットワークエージェントのポリシーの設定」を参照してください）
- 組織ネットワーク内で Microsoft Windows Server Update Services（WSUS）として機能している Windows Server
- Microsoft Update サーバー

このオプションをオンにすると、管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元に接続して、該当する Microsoft Windows Update の情報を最新にします。

このオプションをオフにすると、管理対象デバイス上の Windows Update エージェントは Microsoft アップデートプログラムのソースから以前に受信した、該当する Microsoft Windows アップデートプログラムに関する情報を使用します。

Microsoft Update のアップデート元への接続は、多くのリソースを消費します。別のタスクまたはセクション［**ソフトウェアのアップデートと脆弱性**］のネットワークエージェントのポリシーのプロパティで、アップデート元へ定期的に接続するように設定している場合は、このオプションをオフにすることを検討してください。このオプションをオフにしない場合は、サーバーの負荷を下げるために、タスクの開始を 360 分以内でランダムに遅延させるようにタスクのスケジュールを設定できます。

既定では、このオプションはオンです。

ネットワークエージェントのポリシーの設定の各オプションの組み合わせに応じて、以下のようにアップデートの取得方法が異なります：

- 管理対象デバイス上の Windows Update エージェントがアップデートサーバーに接続してアップデートを取得するのは、［*脆弱性とアプリケーションのアップデートの検索*］タスクのプロパティでアップデートサーバーに［**アップデートサーバーに接続してアップデートを取得**］が有効になっており、ネットワークエージェントポリシーの設定で［**Windows Update 検索モード**］が［**アクティブ**］に設定されている場合のみです。
- *脆弱性スキャン*タスクを実行する時に、ネットワークエージェントが Microsoft Windows アップデート元への接続を開始して更新をダウンロードする必要がない場合は、［**Windows Update 検索モード**］を［**パッシブ**］に設定できますが、［**アップデートサーバーに接続してアップデートを取得**］は有効のままにする必要があります。これにより、リソースを節約し、以前に受信した Windows アップデートプログラムを使用して脆弱性をスキャンできるようになります。
  Microsoft Windows アップデートプログラムの受信を別の方法で構成する場合は、パッシブモードを使用できます。Microsoft Windows アップデートプログラムの受信が別の方法で構成されていない場合は、**Windows Update 検索モード**オプションを**[パッシブ]** に設定しないでください。この場合、アップデートプログラムに関する情報は受信されません。
- ［**アップデートサーバーに接続してアップデートを取得**］の状態（オンまたはオフ）に関係なく、［**Windows Update 検索モード**］が［**無効**］に設定されている場合、Kaspersky Security Center はアップデートプログラムに関する情報を要求しません。

- **カスペルスキーによるサードパーティ製品の脆弱性とアップデートのリストを検索する**

このオプションをオンにすると、Kaspersky Security Center は Windows のレジストリおよび［**ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**］で指定したフォルダーに存在するサードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）の脆弱性とアップデートを検索します。サポート対象のサードパーティ製品の全リストはカスペルスキーが管理しています。

このオプションをオフにすると、サードパーティ製品の脆弱性とアップデートの検索は行われません。Microsoft Windows Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

既定では、このオプションはオンです。

- **ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**

  Kaspersky Security Center が脆弱性の修正とアップデートのインストールが必要なアプリケーションを検索する時に対象とするフォルダーです。システム変数を使用できます。

  アプリケーションがインストールされているフォルダーを指定します。既定では、ほとんどのアプリケーションのインストール先となっているシステムフォルダーがリストに含まれます。

- **詳細な診断を有効にする**

  このオプションをオンにすると、Kaspersky Security Center リモート診断ユーティリティでネットワークエージェントによるトレースがオフになっていても、ネットワークエージェントがトレースを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

  このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center リモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

  タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

  既定では、このオプションはオフです。

- **詳細な診断ファイルの最大サイズ（MB）**

  既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

11. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。

タスクの結果に 0x80240033「Windows Update Agent error 80240033（「License terms could not be downloaded.」）」エラーが含まれている場合、Windows レジストリを使用してこの問題を解決することができます。

脆弱性とアプリケーションのアップデートの検索タスクの設定

［*脆弱性とアプリケーションのアップデートの検索*］タスクは、クイックスタートウィザードの実行時に自動作成されます。ウィザードを実行していない場合も、手動でタスクを作成できます。

全般的なタスクの設定以外に、［*脆弱性とアプリケーションのアップデートの検索*］タスクでは、タスクの作成時または作成後に、作成したタスクのプロパティを編集する時に次の設定を指定できます：

- **Microsoft による脆弱性とアップデートのリストを検索する**

  脆弱性とアップデートの検索時に、Kaspersky Security Center は、現時点で適用可能な Microsoft Update のアップデート元からの該当する Microsoft Update の情報を使用します。

  Microsoft Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

  既定では、このオプションはオンです。

- **アップデートサーバーに接続してアップデートを取得**

管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元として指定した場所に接続します。以下のサーバーを Microsoft Update のアップデート元として動作させることができます：

- Kaspersky Security Center 管理サーバー（詳細は、「ネットワークエージェントのポリシーの設定」を参照してください）
- 組織ネットワーク内で Microsoft Windows Server Update Services（WSUS）として機能している Windows Server
- Microsoft Update サーバー

このオプションをオンにすると、管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元に接続して、該当する Microsoft Windows Update の情報を最新にします。

このオプションをオフにすると、管理対象デバイス上の Windows Update エージェントは Microsoft アップデートプログラムのソースから以前に受信した、該当する Microsoft Windows アップデートプログラムに関する情報を使用します。

Microsoft Update のアップデート元への接続は、多くのリソースを消費します。別のタスクまたはセクション［**ソフトウェアのアップデートと脆弱性**］のネットワークエージェントのポリシーのプロパティで、アップデート元へ定期的に接続するように設定している場合は、このオプションをオフにすることを検討してください。このオプションをオフにしない場合は、サーバーの負荷を下げるために、タスクの開始を 360 分以内でランダムに遅延させるようにタスクのスケジュールを設定できます。

既定では、このオプションはオンです。

ネットワークエージェントのポリシーの設定の各オプションの組み合わせに応じて、以下のようにアップデートの取得方法が異なります：

- 管理対象デバイス上の Windows Update エージェントがアップデートサーバーに接続してアップデートを取得するのは、［*脆弱性とアプリケーションのアップデートの検索*］タスクのプロパティでアップデートサーバーに［**アップデートサーバーに接続してアップデートを取得**］が有効になっており、ネットワークエージェントポリシーの設定で［**Windows Update 検索モード**］が［**アクティブ**］に設定されている場合のみです。
- *脆弱性スキャン*タスクを実行する時に、ネットワークエージェントが Microsoft Windows アップデート元への接続を開始して更新をダウンロードする必要がない場合は、［**Windows Update 検索モード**］を［**パッシブ**］に設定できますが、［**アップデートサーバーに接続してアップデートを取得**］は有効のままにする必要があります。これにより、リソースを節約し、以前に受信した Windows アップデートプログラムを使用して脆弱性をスキャンできるようになります。Microsoft Windows アップデートプログラムの受信を別の方法で構成する場合は、パッシブモードを使用できます。Microsoft Windows アップデートプログラムの受信が別の方法で構成されていない場合は、**Windows Update 検索モード**オプションを[**パッシブ**] に設定しないでください。この場合、アップデートプログラムに関する情報は受信されません。
- ［**アップデートサーバーに接続してアップデートを取得**］の状態（オンまたはオフ）に関係なく、［**Windows Update 検索モード**］が［**無効**］に設定されている場合、Kaspersky Security Center はアップデートプログラムに関する情報を要求しません。

- **カスペルスキーによるサードパーティ製品の脆弱性とアップデートのリストを検索する**

このオプションをオンにすると、Kaspersky Security Center は Windows のレジストリおよび［**ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**］で指定したフォルダーに存在するサードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）の脆弱性とアップデートを検索します。サポート対象のサードパーティ製品の全リストはカスペルスキーが管理しています。

このオプションをオフにすると、サードパーティ製品の脆弱性とアップデートの検索は行われません。Microsoft Windows Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

既定では、このオプションはオンです。

- **ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**

  Kaspersky Security Center が脆弱性の修正とアップデートのインストールが必要なアプリケーションを検索する時に対象とするフォルダーです。システム変数を使用できます。

  アプリケーションがインストールされているフォルダーを指定します。既定では、ほとんどのアプリケーションのインストール先となっているシステムフォルダーがリストに含まれます。

- **詳細な診断を有効にする**

  このオプションをオンにすると、Kaspersky Security Center リモート診断ユーティリティでネットワークエージェントによるトレースがオフになっていても、ネットワークエージェントがトレースを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

  このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center リモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

  タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

  既定では、このオプションはオフです。

- **詳細な診断ファイルの最大サイズ（MB）**

  既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

タスクのスケジュールに関する推奨事項

［*脆弱性とアプリケーションのアップデートの検索*］タスクのスケジュールを設定する場合は、［**未実行のタスクを実行する**］と［**タスクの開始を自動的かつランダムに遅延させる**］の 2 つのオプションがオンになっていることを確認してください。

既定では、［*脆弱性とアプリケーションのアップデートの検索*］タスクは手動で開始するように設定されています。組織で採用されている規則などによりこの時刻にすべてのデバイスをシャットダウンするように定められている場合は、デバイスが再度電源オンになる時刻、つまり翌日の朝に、*脆弱性とアプリケーションのアップデートの検索*タスクが実行されます。脆弱性スキャン時にはCPUとディスクサブシステムの負荷が増大するため、このように業務時間中に処理が実行されてしまうことが問題となる可能性があります。組織で採用されている職場のルールに基づいて、このタスクに対する最も効率的なスケジュールをセットアップする必要があります。

［アップデートのインストールと脆弱性の修正］タスクの作成

［*アップデートのインストールと脆弱性の修正*］タスクは、脆弱性とパッチ管理 ライセンスがある場合にのみ使用できます。

［*アップデートのインストールと脆弱性の修正*］タスクは、管理対象デバイス上でMicrosoft製品やその他のサードパーティ製ソフトウェアの脆弱性をアップデートによって修正するために使用します。このタスクを使用することで、一定のルールに従って複数のアップデートをインストールしたり、複数の脆弱性を修正したりすることができます。

［*アップデートのインストールと脆弱性の修正*］タスクを使用してアップデートのインストールまたは脆弱性の修正を実行するには、次のうち1つの操作を実行します：

- アップデートのインストールウィザードまたは脆弱性修正ウィザードを実行します。
- ［*アップデートのインストールと脆弱性の修正*］タスクを作成します。
- 既存の［*アップデートのインストールと脆弱性の修正*］タスクにアップデートのインストールに関するルールを追加します。

［アップデートのインストールと脆弱性の修正］タスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. Kaspersky Security Centerを対象アプリケーションとするタスクから、［**アップデートのインストールと脆弱性の修正**］タスク種別を選択します。
   タスクが表示されない場合は、［**システム管理**：**脆弱性とパッチ管理**］機能領域の**読み取り**、**変更**、および**実行**権限がアカウントに付与されていることを確認してください。これらのアクセス権がない場合、*アップデートのインストールと脆弱性の修正*タスクを作成および設定することはできません。
4. 作成中のタスク名を入力します。タスク名は100文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクを割り当てるデバイスを選択します。
6. アップデートインストールのルールを指定してから、次の設定を指定します：
   - **デバイスの再起動時またはシャットダウン時にインストールを開始する**

このオプションをオンにすると、デバイスの再起動時またはシャットダウン時にアップデートがインストールされます。オプションがオフの場合、アップデートのインストールはスケジュールに従って実行されます。

アップデートのインストールによりデバイスのパフォーマンスに影響を与える可能性がある場合は、このオプションを使用します。

既定では、このオプションはオフです。

- **必要なシステムコンポーネントをインストールする**

  このオプションをオンにすると、アップデートのインストール前にインストールが必要な一般システムコンポーネントをすべて自動的にインストールします。インストールが必要な対象とは、たとえばオペレーティングシステムのアップデートなどです。

  このオプションをオフにすると、必須コンポーネントを手動でインストールすることが必要となる場合があります。

  既定では、このオプションはオフです。

- **アップデート中に新しい製品のバージョンのインストールを許可する**

  このオプションをオンにすると、製品の新しいバージョンをインストールするアップデートを許可できます。

  このオプションをオフにすると、製品はアップグレードされません。製品の新しいバージョンは手動でインストールするか、別のタスクを通してインストールできます。この設定は、所属企業のインフラストラクチャでソフトウェアの新しいバージョンがサポートされていなかったり、アップグレードをテスト環境で確認したい場合に使用します。

  既定では、このオプションはオンです。

  製品をアップデートすることにより、クライアントデバイスにインストールされた対象製品に依存するアプリケーションが正しく動作しなくなることがあります。

- **デバイスにアップデートをダウンロードするがインストールしない**

  このオプションをオンにすると、アップデートをデバイスにダウンロードしますが、自動ではインストールしません。ダウンロードされたアップデートを手動でインストールできます。

  Microsoft 製品のアップデートは、システム Windows フォルダーにダウンロードされます。サードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートは、［**アップデートのダウンロード先**］で指定したフォルダーにダウンロードされます。

  このオプションをオフにすると、アップデートはデバイスに自動的にインストールされません。

  既定では、このオプションはオフです。

- **アップデートのダウンロード先**

  このフォルダーはサードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートのダウンロードに使用されます。

- **詳細な診断を有効にする**

このオプションをオンにすると、Kaspersky Security Center リモート診断ユーティリティでネットワークエージェントによるトレースがオフになっていても、ネットワークエージェントがトレースを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center リモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

既定では、このオプションはオフです。

- **詳細な診断ファイルの最大サイズ（MB）**

  既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

7. OS の再起動設定を指定します。

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

- **通知の繰り返し間隔（分）**

このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

- **再起動するまでの時間（分）**

  ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

  既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了するまで待機する時間（分）**

  ユーザーのデバイスがロックされた場合にアプリケーションが強制終了されます（指定した非アクティブの時間が経過した後に自動で、または手動で）。

  このオプションを有効にすると、入力フィールドに指定した時間を過ぎた時に、ロックされたデバイスでアプリケーションが強制的に終了します。

  このオプションをオフにすると、ロックされたデバイスでアプリケーションは終了しません。

  既定では、このオプションはオフです。

8. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

9. ［**終了**］をクリックします。

   タスクが作成され、タスクリストに表示されます。

10. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

11. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。

12. ［**保存**］をクリックします。

    タスクが指定した設定で作成されます。

タスクの結果に 0x80240033「Windows Update Agent error 80240033（「License terms could not be downloaded.」）」エラーが含まれている場合、Windows レジストリを使用してこの問題を解決することができます。

アップデートインストールのルールの追加

この機能は、脆弱性とパッチ管理 ライセンスでのみ使用できます。

［*アップデートのインストールと脆弱性の修正*］タスクを使用してソフトウェアのアップデートをインストールする、またはソフトウェアの脆弱性を修正する場合は、アップデートインストールのルールを指定する必要があります。これらのルールにより、インストールするアップデートと修正する脆弱性が決定されます。

厳密な設定内容は、追加するルールがすべてのアップデート、Windows Update 更新プログラム、サードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートのいずれを対象とするのかによって異なります。Windows Update 更新プログラムまたはサードパーティ製品のアップデートのいずれかを対象にルールを追加する場合は、アップデートをインストールする特定のアプリケーションとバージョンを選択できます。すべてのアップデートのルールを追加する場合は、インストールする特定のアップデートおよびアップデートをインストールすることで修正する脆弱性を選択できます。

次の方法で、アップデートのインストールのルールを追加できます：

- 新規のアップデートのインストールと脆弱性の修正タスクの作成中にルールを追加する。
- 既存の［*アップデートのインストールと脆弱性の修正*］タスクの［**Application Settings**］タブでルールを追加する。
- アップデートのインストールウィザードまたは脆弱性修正ウィザード。

すべてのアップデートを対象とするルールを追加するには：

1. ［**追加**］をクリックします。
   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
2. ［**ルール種別**］ページで、［**すべてのアップデートのルール**］を選択します。
3. ［**全般基準**］ウィンドウで、ドロップダウンリストを使用して次の設定を指定します。

- **インストールするアップデートの設定**

  クライアントデバイスにインストールする必要がある更新を選択します。
  - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
  - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
  - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。

- **次のレベル以上の深刻度の脆弱性を修正する**

  ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

  このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

  このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

  既定では、このオプションはオフです。

4. ［**アップデート**］ウィンドウで、インストールするアップデートを選択します：

- **すべての適用可能なアップデートをインストールする**

  ウィザードの［**全般基準**］ウィンドウで指定した基準に合致するソフトウェアアップデートをすべてインストールします。既定では、この項目が選択されます。

- **リストのアップデートのみをインストールする**

  手動で選択したリストのソフトウェアアップデートのみをインストールします。追加できるアップデートには、使用可能なすべてのソフトウェアアップデートが含まれます。

  特定のアップデートを選択する状況としてはたとえば、テスト環境でのインストールの確認、重要なアプリケーションのみのアップデート、特定のアプリケーションのみのアップデートなどが考えられます。

  - **選択したアップデートのインストールに必要な以前のアップデートをすべて自動的にインストールする**

    選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、このオプションをオンのままにします。

    このオプションをオフにすると、選択したバージョンのアプリケーションのみがインストールされます。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、このオプションをオフにします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

    たとえば、デバイスにアプリケーションのバージョン 3 がインストールされていて、バージョン 5 にアップデートしたいが、バージョン 5 はバージョン 4 経由のみでしかインストールできない状況を想定します。このオプションをオンにすると、先にバージョン 4 をインストールし、続いてバージョン 5 をインストールします。このオプションをオフにすると、アプリケーションのアップデートは失敗します。

    既定では、このオプションはオンです。

5. ［**脆弱性**］ウィンドウで、選択したアップデートのインストールで修正する脆弱性を選択します：

- **他の基準に一致するすべての脆弱性を修正する**

  ウィザードの［**全般基準**］ウィンドウで指定した基準に合致する脆弱性をすべて修正します。既定では、この項目が選択されます。

- **リストの脆弱性のみを修正する**

  手動で選択したリストの脆弱性のみをインストールします。追加できるアップデートには、検知されたすべての脆弱性が含まれます。

  特定の脆弱性を選択する状況としてはたとえば、テスト環境での脆弱性の修正の確認、重要なアプリケーションのみでの脆弱性の修正、特定のアプリケーションのみでの脆弱性の修正などが考えられます。

6. ［**名前**］ページで、追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**設定**］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが追加され、新規タスクウィザードまたはタスクのプロパティに表示されます。

Windows Update 更新プログラムを対象とする新しいルールを追加するには：

1. ［**追加**］をクリックします。
   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
2. ［**ルール種別**］ページで、［**Windows Update のルール**］を選択します。
3. ［**全般基準**］ウィンドウで、次の設定を指定します：
   - **インストールするアップデートの設定**

     クライアントデバイスにインストールする必要がある更新を選択します。
     - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
     - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
     - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。
   - **次のレベル以上の深刻度の脆弱性を修正する**

     ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

     このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

     このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

     既定では、このオプションはオフです。
   - **次のレベル以上の MSRC 深刻度の脆弱性を修正する**

     ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

     このオプションをオンにすると、MSRC（Microsoft Security Response Center）が設定する重要度レベルが、リストで選択した値（**低**、**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

     このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

     既定では、このオプションはオフです。
4. ［**アプリケーション**］ウィンドウで、アップデートをインストールするアプリケーションとアプリケーションのバージョンを選択します。既定では、すべてのアプリケーションがオンです。

5. ［**アップデートのカテゴリ**］ウィンドウで、インストールするアップデートのカテゴリを選択します。これらのカテゴリは Microsoft Update カタログで使用されているのと同じカテゴリです。既定では、すべてのカテゴリがオンです。

6. ［**名前**］ページで、追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**設定**］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが追加され、新規タスクウィザードまたはタスクのプロパティに表示されます。

サードパーティ製品のアップデートを対象とする新しいルールを追加するには：

1. ［**追加**］をクリックします。
ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

2. ［**ルール種別**］ページで、［**サードパーティ製品のアップデートのルール**］を選択します。

3. ［**全般基準**］ウィンドウで、次の設定を指定します：

- **インストールするアップデートの設定**

  クライアントデバイスにインストールする必要がある更新を選択します。
  - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
  - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
  - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。

- **次のレベル以上の深刻度の脆弱性を修正する**

  ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

  このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

  このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

  既定では、このオプションはオフです。

4. ［**アプリケーション**］ウィンドウで、アップデートをインストールするアプリケーションとアプリケーションのバージョンを選択します。既定では、すべてのアプリケーションがオンです。

5. ［**名前**］ページで、追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［設定］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが追加され、新規タスクウィザードまたはタスクのプロパティに表示されます。

［Windows Update 更新プログラムのインストール］タスクの作成

［*Windows Update 更新プログラムのインストール*］タスクを使用することで、Windows Update サービス経由で提供されるソフトウェアのアップデートを管理対象デバイスにインストールできます。

Vulnerability and Patch Managementライセンスをお持ちでない場合、*Windows Update 更新プログラムのインストール*の種別の新しいタスクを作成できません。新しいアップデートをインストールするには、既存の［*Windows Update 更新プログラムのインストール*］タスクに新しいアップデートを追加します。*アップデートのインストールと脆弱性の修正*タスクを、［*Windows Update 更新プログラムのインストール*］の代わりに使用することを推奨します。［*アップデートのインストールと脆弱性の修正*］タスクを使用すると、定義したルールに従って、複数の更新をインストールし、複数の脆弱性を自動的に修正できます。また、このタスクを使用すると、Microsoft 以外のソフトウェア開発元からのアップデートをインストールできます。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。開いてたとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

［Windows Update 更新プログラムのインストール］タスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**Windows Update 更新プログラムのインストール**］タスク種別を選択します。
4. 作成中のタスク名を入力します。
   タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクを割り当てるデバイスを選択します。
6. ［**追加**］をクリックします。
   アップデートのリストが表示されます。
7. インストールする Windows Update 更新プログラムを選択し、［**OK**］をクリックします。
8. OS の再起動設定を指定します。

   - **デバイスを再起動しない**

     操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

   - **デバイスを再起動する**

インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

既定では、このオプションがオンです。

- **通知の繰り返し間隔（分）**

このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

既定では、このオプションはオンです。既定の間隔は 5 分です。1分から1,440 分までの値を指定できます。

このオプションをオフにすると、確認メッセージは1回だけ表示されます。

- **再起動するまでの時間（分）**

ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

既定では、このオプションはオンです。既定の間隔は 30 分です。1分から1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

既定では、このオプションはオフです。

9. 次のようにアカウントの設定を指定します。

- **既定のアカウント**

タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。

既定では、このオプションがオンです。

- **アカウントの指定**

  ［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

- **アカウント**

  タスクを実行するアカウント。

- **パスワード**

  タスクが実行されるアカウントのパスワード。

10. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

11. ［**終了**］をクリックします。

    タスクが作成され、タスクリストに表示されます。

12. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

13. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。

14. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。

サードパーティ製品の使用可能なアップデートに関する情報の表示

クライアントデバイスにインストールされた Microsoft 製品やその他のサードパーティ製ソフトウェアに対して適用可能なアップデートのリストを表示できます。

クライアントデバイスにインストールされたサードパーティ製ソフトウェアに対して適用可能なアップデートのリストを表示するには、

メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動します。

適用可能なアップデートのリストが表示されます。

ソフトウェアアップデートのリストの表示では、フィルターを指定できます。ソフトウェアアップデートのリストの右上にある**フィルター**アイコン（）をクリックして、フィルターを指定してください。ソフトウェアの脆弱性リストの上の［**設定済みのフィルター**］ドロップダウンリストから、いずれかの設定済みのフィルターを選択することもできます。

アップデートのプロパティを表示するには：

1. 目的のソフトウェアのアップデートの名前をクリックします。

2. アップデートのプロパティウィンドウが開き、次のタブごとにまとめられた情報が表示されます：

- **全般**

  このタブには、選択したアップデートの一般的な詳細が表示されます。

  - 承認ステータスのアップデート（ドロップダウンリストの新しいステータスをオンにすると、手動で変更できます）
  - アップデートが属する Windows Server Update Services（WSUS）カテゴリ
  - アップデートが登録された日時
  - アップデートが作成された日時
  - アップデートの重要度
  - アップデートによって適用されるインストール要件
  - アップデートが属するアプリケーションファミリー
  - アップデートが適用されるアプリケーション
  - アップデートのリビジョン番号

- **属性**

  このタブには、選択したアップデートに関する詳細情報の取得に使用できる一連の属性が表示されます。表示される属性は、アップデートの公開元が Microsoft かサードパーティかによって異なります。

  このタブには、Microsoft のアップデートに関する次の情報が表示されます：

  - Microsoft Security Response Center（MSRC）によって定義されたアップデートの重要度
  - アップデートについて説明しているマイクロソフトサポート技術情報の記事へのリンク
  - アップデートについて説明しているマイクロソフトセキュリティ情報の記事へのリンク
  - アップデートの識別子（ID）

  このタブには、サードパーティの更新プログラムに関する次の情報が表示されます：

  - アップデートがパッチか、または配布パッケージか
  - アップデートのローカリゼーション言語
  - アップデートが自動インストールか手動インストールか
  - 適用後にアップデートが取り消されたかどうか
  - アップデートをダウンロードするためのリンク

- **デバイス**

このタブには、選択したアップデートがインストールされているデバイスのリストが表示されます。

- **修正済みの脆弱性**

  このタブには、選択したアップデートで修正できる脆弱性のリストが表示されます。

- **アップデートの重複**

  このタブには、同じアプリケーションに対して公開された複数のアップデート間で起こり得るクロスオーバーが表示されます。つまり、選択したアップデートが他のアップデートより優先されるか、逆に他のアップデートが優先されるかを表示します（Microsoft のアップデートでのみ使用可能）。

- **このアップデートをインストールするタスク**

  このタブには、選択したアップデートのインストールをスコープに含むタスクのリストが表示されます。このタブでは、アップデート用の新しいリモートインストールタスクを作成することもできます。

アップデートのインストールの統計情報を表示するには：

1. 目的のソフトウェアのアップデートに隣接するチェックボックスをオンにします。
2. ［**アップデートのインストールステータスの統計**］をクリックします。

アップデートのインストールステータスを示した図表が表示されます。それぞれのステータスをクリックすると、選択したステータスのアップデートが存在するデバイスのリストが表示されます。

Windows を使用している選択した管理対象デバイスにインストールされた Microsoft 製品やその他のサードパーティ製ソフトウェアに対して適用可能なアップデートのリストを表示できます。

選択した管理対象デバイスにインストールされているサードパーティ製ソフトウェアに対して適用可能なアップデートのリストを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、サードパーティ製ソフトウェアのアップデートを表示するデバイスの名前のリンクをクリックします。
   選択したデバイスのプロパティウィンドウが表示されます。
3. 選択したデバイスのプロパティウィンドウで、［**詳細**］タブを選択します。
4. 左側のペインで、［**適用可能なアップデート**］セクションを選択します。インストール済みのアップデートのみを表示する場合は、［**インストールされたアップデートの表示**］をオンにします。

選択したデバイス上で適用可能なサードパーティ製ソフトウェアのアップデートのリストが表示されます。

使用可能なソフトウェアアップデートのリストのファイルへのエクスポート

Microsoft 製品やその他のサードパーティ製ソフトウェアに対するアップデートとして表示されているアップデートのリストを、CSV ファイルまたは TXT ファイルにエクスポートできます。エクスポートしたファイルは、情報セキュリティ部門に共有したり、統計情報を取得するために保存するなどの用途に使用できます。

管理対象デバイスにインストールされているサードパーティ製ソフトウェアに対して適用可能なすべてのアップデートのリストをファイルにエクスポートするには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動します。

   管理対象デバイスにインストールされているサードパーティ製ソフトウェアに対して適用可能なすべてのアップデートのリストが表示されます。

2. エクスポートするファイルの形式に応じて、［**TXT へエクスポート**］または［**CSV へエクスポート**］をクリックします。

   操作に使用しているデバイスに、Microsoft 製品やその他のサードパーティ製ソフトウェアに対して適用可能なアップデートのリストをエクスポートしたファイルがダウンロードされます。

選択した管理対象デバイスにインストールされているサードパーティ製ソフトウェアに対して適用可能なアップデートのリストをファイルにエクスポートするには：

1. 選択した管理対象デバイスに対して適用可能なサードパーティ製ソフトウェアのアップデートのリストが表示されます。

2. エクスポートするソフトウェアアップデート項目を選択します。

   ソフトウェアアップデートのリストをそのままエクスポートする場合は、この手順をスキップします。

   ただし、ソフトウェアアップデートのリストをそのままエクスポートする場合でも、エクスポートできるのはウィンドウで現在表示されているアップデート項目のみです。

   インストール済みのアップデートのみをエクスポートする場合、［**インストールされたアップデートの表示**］をオンにします。

3. エクスポートするファイルの形式に応じて、［**TXT へエクスポート**］または［**CSV へエクスポート**］をクリックします。

   操作に使用しているデバイスに、選択した管理対象デバイスにインストールされている Microsoft 製品やその他のサードパーティ製ソフトウェアに対して適用可能なアップデートのリストをエクスポートしたファイルがダウンロードされます。

サードパーティ製ソフトウェアのアップデートの拒否と承認

*アップデートのインストールと脆弱性の修正*タスクを設定する際には、アップデートに特定のステータスが割り当てられていることをインストールの要件とするルールを作成できます。たとえば、次のようなステータスのアップデートのインストールのみを許可するようにルールを設定できます：

- 承認済みのアップデートのみ
- 承認済みのアップデートとステータスが未定義のアップデートのみ

- すべてのアップデート（ステータスを考慮しない）

インストールする必要のあるアップデートを承認し、インストールしないアップデートを拒否します。

アップデートのインストールを管理するための「*承認*」ステータスの使用は、アップデート量が少ない場合に効率的です。複数のアップデートをインストールするには、*アップデートのインストールと脆弱性の修正*タスクで設定できるルールを使用します。ルールで指定された基準を満たさない特定のアップデートに対してのみ、「*承認*」ステータスを設定することを推奨します。大量のアップデートを手動で承認すると、管理サーバーのパフォーマンスが低下し、サーバーが過負荷状態になる場合があります。

1 つ以上のアップデートを承認または拒否するには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動します。
   適用可能なアップデートのリストが表示されます。
2. 承認または拒否するアップデートを選択します。
3. 選択したアップデートを承認する場合は［**承認**］を、拒否する場合は［**承認却下**］を選択します。
   既定値は［*未定義*］です。

   選択したアップデートのステータスが、指定したステータスに変更されます。

オプションとして、特定のアップデートのプロパティで承認ステータスを変更できます。

プロパティでアップデートを承認または拒否するには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動します。
   適用可能なアップデートのリストが表示されます。
2. 承認または拒否するアップデートの名前をクリックします。
   アップデートのプロパティウィンドウが開きます。
3. ［**全般**］セクションで、［**アップデート承認の状況**］を変更してアップデートのステータスを選択します。［*承認*］、［*承認却下*］、または［*未定義*］のいずれかのステータスを選択できます。
4. ［**保存**］をクリックして変更を保存します。

   選択したアップデートのステータスが、指定したステータスに変更されます。

サードパーティ製のソフトウェアアップデートに［**拒否**］ステータスを設定すると、このアップデートは、アップデートのインストールを予定しているがまだ完了していないデバイスにはインストールされません。アップデートをインストール済みのデバイスには、これらのアップデートがそのまま残ります。アップデートを削除する時は、手動でローカル削除できます。

［Windows Update の同期の実行］タスクが作成されます

［*Windows Update の同期の実行*］タスクは、脆弱性とパッチ管理ライセンスがある場合にのみ使用できます。

管理サーバーを WSUS サーバーとして使用する場合は、［*Windows Update の同期の実行*］タスクが必要です。この場合、管理サーバーは Windows の更新プログラムをデータベースにダウンロードし、ネットワークエージェントを介して集中モードでクライアントデバイス上の Windows Update に更新プログラムを渡します。ネットワークで WSUS サーバーが使用されていない場合は、個々のクライアントデバイスが外部のサーバーから Microsoft のアップデートを個別にダウンロードします。

*Windows Update の同期の実行*タスクは、メタデータのみを Microsoft のサーバーからダウンロードします。アップデートインストールタスクを実行すると、Kaspersky Security Center は更新プログラムをダウンロードします。その際、インストール用に選択した更新プログラムのみをダウンロードします。

Windows Update の同期の実行タスクの実行時に、本製品は Microsoft Update サーバーから現行のアップデート一覧を受信します。その後、本製品は古くなったアップデートの一覧を作成します。次に**脆弱性とアプリケーションのアップデートの検索**タスクを開始する時に、本製品はすべての古くなったアップデートにフラグを付け、削除までの時間を設定します。次に **Windows Update の同期の実行**タスクを開始する時に、30 日前に削除フラグが付けられたアップデートはすべて削除されます。また、フラグを付けてから 181 日以上経過しているアップデートの有無を確認し、あれば削除します。

Windows Update の同期の実行タスクが完了し、古くなったアップデートが削除されても、削除されたアップデートのファイルに属するハッシュコードがデータベース上に残っていることがあります。同様に、%AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles にある対応するファイルもデータベース上に残っていることがあります（それ以前にダウンロードされていた場合）。［**管理サーバーのメンテナンス**］タスクを実行して、定義データベースと対応するファイルからこれらの古いレコードを削除できます。

Windows Update の同期の実行タスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**Windows Update の同期の実行**］タスク種別を選択します。
4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクの実行時に高速アップデートファイルをダウンロードする場合は、［**高速インストールファイルをダウンロード**］をオンにします。

   Kaspersky Security Center が Microsoft Windows Update Server のアップデートと同期すると、全ファイルに関する情報が管理サーバーのデータベースに保存されます。Windows Update エージェントとのやり取りの間、アップデートに必要なファイルもすべてドライブにダウンロードされます。具体的には、Kaspersky Security Center によって、高速インストールファイルに関する情報がデータベースに保存され、必要な時にこれらのファイルがダウンロードされます。高速インストールファイルをダウンロードすると、ドライブの空き容量が減少します。

   ディスクの空き容量の減少を避け、トラフィックを減らすには、［**高速インストールファイルをダウンロード**］をオフにします。
6. アップデートをダウンロードするアプリケーションを選択します。

   ［**全製品**］をオンにすると、すべての既存のアプリケーション、および今後リリースされる可能性のあるすべてのアプリケーションのアップデートがダウンロードされます。
7. 管理サーバーにダウンロードするアップデートのカテゴリを選択します。

   ［**全カテゴリ**］をオンにすると、すべての既存のアップデートカテゴリ、および今後生じる可能性のあるすべてのカテゴリのアップデートがダウンロードされます。

8. 管理サーバーにダウンロードするアップデートのローカリゼーション言語を選択します。次のいずれかのオプションをオンにします：

   - **新しい言語を含むすべての言語をダウンロード**

     このオプションをオンにすると、使用可能なすべての言語のアップデートを管理サーバーにダウンロードできます。既定では、このオプションがオンです。

   - **特定の言語をダウンロード**

     このオプションをオンにすると、管理サーバーにダウンロードするアップデートの言語をリストから選択できます。

9. タスクの実行時に使用するアカウントを指定します。次のいずれかのオプションをオンにします：

   - **既定のアカウント**

     タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。
     既定では、このオプションがオンです。

   - **アカウントの指定**

     ［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

10. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

11. ［**終了**］をクリックします。
    タスクが作成され、タスクリストに表示されます。

12. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

13. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。

14. ［**保存**］をクリックします。

    タスクが指定した設定で作成されます。

サードパーティ製品の自動アップデート

一部のサードパーティ製品は自動的にアップデートできます。アプリケーションの製造元は、アプリケーションが自動アップデート機能をサポートするかどうかを定義します。管理対象デバイスにインストールされているサードパーティ製品が自動アップデートをサポートしている場合は、アプリケーションのプロパティで自動アップデートの設定を指定できます。自動アップデート設定の変更後、ネットワークエージェントは、アプリケーションがインストールされている各管理対象デバイスにその新しい設定を適用します。

自動アップデートの設定は、脆弱性とパッチ管理機能の他のオブジェクトと設定から独立しています。たとえば、この設定はアップデート承認の状況や、［*アップデートのインストールと脆弱性の修正*］、［*Windows Update 更新プログラムのインストール*］、［*脆弱性の修正*］などのアップデートのインストールタスクには依存しません。

サードパーティ製品の自動アップデート設定を行うには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。
2. 自動アップデート設定を変更するアプリケーションの名前をクリックします。
   検索を簡略化するには、［**自動アップデートのステータス**］列でリストをフィルタリングできます。
   アプリケーションプロパティのウィンドウが開きます。
3. ［**全般**］セクションで、次の設定の値を選択します：
   自動アップデートのステータス

   次のいずれかのオプションをオンにします：

   - **未定義**
     自動アップデート機能は無効になっています。Kaspersky Security Center は、［*アップデートのインストールと脆弱性の修正*］、［*Windows Update 更新プログラムのインストール*］、［*脆弱性の修正*］の各タスクを使用して、サードパーティ製品のアップデートをインストールします。
   - **許可**
     製造元がアプリケーションのアップデートをリリースすると、このアップデートは管理対象デバイスに自動的にインストールされます。追加の操作は必要ありません。
   - **ブロック**
     アプリケーションのアップデートは自動的にインストールされません。Kaspersky Security Center は、［*アップデートのインストールと脆弱性の修正*］、［*Windows Update 更新プログラムのインストール*］、［*脆弱性の修正*］の各タスクを使用して、サードパーティ製品のアップデートをインストールします。
4. ［**保存**］をクリックして変更を保存します。

選択したアプリケーションに自動アップデートの設定が適用されます。

サードパーティ製ソフトウェアの脆弱性の修正

このセクションでは、管理対象デバイスにインストールされているソフトウェアの脆弱性の修正に関連する Kaspersky Security Center の機能について説明します。

シナリオ：サードパーティ製ソフトウェアの脆弱性の検知と修正

このセクションでは Windows オペレーティングシステムを使用しているデバイスで、脆弱性を検知し修正する方法について説明しています。オペレーティングシステムとサードパーティ製ソフトウェア（Microsoft 製品を含む）の脆弱性の検知と修正を実行できます。

必須条件

- 組織内に Kaspersky Security Center が導入されている。
- 組織内に Windows を使用している管理対象デバイスが存在する。
- 管理サーバーで次のタスクを実行する場合は、インターネット接続が必要になります。
  - Microsoft ソフトウェアの脆弱性に対して推奨される修正のリストを作成する。このリストは、カスペルスキーのスペシャリストにより作成され、定期的に更新されます。
  - Microsoft ソフトウェア以外のサードパーティ製ソフトウェアで脆弱性を修正する。

実行するステップ

ソフトウェアの脆弱性の検知と修正は、次の手順で進みます：

1. **管理対象デバイスにインストールされているソフトウェアの脆弱性のスキャン**

   管理対象デバイスにインストールされているソフトウェアの脆弱性を検知するには、［*脆弱性とアプリケーションのアップデートの検索*］タスクを実行します。タスクが完了すると、Kaspersky Security Center はタスクのプロパティで指定したデバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。

   *脆弱性とアプリケーションのアップデートの検索*タスクは、Kaspersky Security Center のクイックスタートウィザードによって自動的に作成されます。ウィザードを実行していない場合は、次の手順に進む前にウィザードを実行するか手動でタスクを作成してください。

   実行手順の説明：

   - 管理コンソール：アプリケーションの脆弱性スキャン、脆弱性とアプリケーションのアップデートの検索タスクのスケジュール設定
   - Kaspersky Security Center Web コンソール：脆弱性とアプリケーションのアップデートの検索タスクの作成、脆弱性とアプリケーションのアップデートの検索タスクの設定

2. **検知されたソフトウェアの脆弱性の分析**

   ［**ソフトウェアの脆弱性**］リストを確認して、どの脆弱性を修正するかを決定します。それぞれの脆弱性の詳細情報を確認するには、リスト内の脆弱性の名前をクリックします。リスト内のそれぞれの脆弱性について、管理対象デバイス上の脆弱性に関する統計情報を表示することもできます。

   実行手順の説明：

   - 管理コンソール：ソフトウェアの脆弱性に関する情報の表示、管理対象デバイス上の脆弱性に関する統計情報の表示
   - Kaspersky Security Center Web コンソール：ソフトウェアの脆弱性に関する情報の表示、管理対象デバイス上の脆弱性に関する統計情報の表示

3. **脆弱性の修正の設定**

   管理対象デバイス上でソフトウェアの脆弱性が検知された場合、［*アップデートのインストールと脆弱性の修正*］タスクまたは［*脆弱性の修正*］タスクを使用して、ソフトウェア脆弱性を修正できます。

［*アップデートのインストールと脆弱性の修正*］タスクは、管理対象デバイス上で Microsoft 製品やその他のサードパーティ製ソフトウェアの脆弱性をアップデートによって修正するために使用します。このタスクを使用することで、一定のルールに従って複数のアップデートをインストールしたり、複数の脆弱性を修正したりすることができます。このタスクは、脆弱性とパッチ管理機能を利用できるライセンスを使用している場合にのみ作成できます。ソフトウェア脆弱性を修正するために、*アップデートのインストールと脆弱性の修正*タスクは推奨されるソフトウェアアップデートを使用します。

*脆弱性の修正*タスクは、脆弱性とパッチ管理機能を使用できるライセンスがなくても使用できます。このタスクを使用するには、タスクの設定で、サードパーティ製ソフトウェアの脆弱性を修正するために使用するユーザー修正を手動で指定する必要があります。*脆弱性の修正*タスクでは、Microsoft 製品に対しては推奨される修正を、その他のサードパーティ製ソフトウェアに対してはユーザー修正をインストールして脆弱性を修正します。

脆弱性修正ウィザードを起動すると、これらのタスクのいずれかを自動的に作成できます。または、手動でタスクを作成することもできます。

実行手順の説明：

- 管理コンソール：サードパーティ製ソフトウェアの脆弱性へのユーザー修正の選択、アプリケーションの脆弱性の修正
- Kaspersky Security Center Web コンソール：サードパーティ製ソフトウェアの脆弱性へのユーザー修正の選択、サードパーティ製ソフトウェアの脆弱性の修正、アップデートのインストールと脆弱性の修正タスクの作成

4 タスクのスケジュール設定

脆弱性のリストを最新の状態に維持するため、［*脆弱性とアプリケーションのアップデートの検索*］タスクが定期的に自動で実行されるようにスケジュールを指定してください。推奨される平均的なタスクの実行頻度は週に 1 回です。

［*アップデートのインストールと脆弱性の修正*］タスクを作成している場合は、実行頻度を［*脆弱性とアプリケーションのアップデートの検索*］と同じかそれよりも少なくします。*脆弱性の修正*タスクのスケジュールを設定する場合は、タスクを開始する前に、毎回 Microsoft 製品の修正を選択するか、サードパーティ製ソフトウェアのユーザー修正を指定する必要があることに注意してください。

タスクのスケジュールを指定する場合は、［*脆弱性とアプリケーションのアップデートの検索*］タスクが完了してからこれらのタスクが開始するようにしてください。

5 検知されたソフトウェアの脆弱性への非対応の判断（必要に応じて実施）

必要に応じて、すべてのデバイス上または選択した特定のデバイス上で、ソフトウェアの脆弱性を無視できます。

実行手順の説明：

- 管理コンソール：検知されたソフトウェアの脆弱性への非対応の判断
- Kaspersky Security Center Web コンソール：検知されたソフトウェアの脆弱性への非対応の判断

6 脆弱性の修正タスクの実行

*アップデートのインストールと脆弱性の修正*タスクまたは*脆弱性の修正*タスクを開始します。タスクが完了したら、タスクリストでのタスクのステータスが［*正常終了*］になっていることを確認します。

7 ソフトウェアの脆弱性の修正結果のレポートの作成（省略可能）

脆弱性の修正に関する詳細な統計情報を確認するには、脆弱性レポートを生成します。レポートには、修正されなかったソフトウェアの脆弱性に関する情報が表示されます。これにより、組織内での Microsoft 製品やその他のサードパーティ製ソフトウェアの脆弱性の検知と修正の状況を把握することができます。

実行手順の説明：

- 管理コンソール：レポートの作成と表示

- Kaspersky Security Center Web コンソール：レポートの生成と表示

8. **サードパーティ製ソフトウェアの脆弱性の検知と修正に関する設定の確認**

   次の手順がすべて完了していることを確認してください：

   - 管理対象デバイス上のソフトウェアの脆弱性のリストを作成して内容を確認した
   - 必要に応じて、修正対応しないソフトウェアの脆弱性を選定した
   - 脆弱性を修正するタスクを設定した
   - タスクの実行順序として、ソフトウェアの脆弱性を検知するタスクが実行された後に脆弱性を修正するタスクが実行されるようにスケジュールを指定した
   - ソフトウェアの脆弱性を修正するタスクが実行されたことを確認した

結果

［*アップデートのインストールと脆弱性の修正*］タスクを作成した場合、管理対象デバイス上の脆弱性が自動的に修正されます。タスクの実行時に、適用可能なソフトウェアアップデートのリストとタスクの設定で指定されたルールとが照合されます。ルールの条件に一致するすべてのソフトウェアアップデートが管理サーバーのリポジトリにダウンロードされ、ソフトウェアの脆弱性を修正するためにインストールされます。

［*脆弱性の修正*］タスクを作成した場合、Microsoft 製品のソフトウェア脆弱性のみが修正されます。

ソフトウェアの脆弱性の検知と修正

Kaspersky Security Center では、Microsoft Windows オペレーティングシステムを実行している管理対象デバイスのソフトウェア脆弱性を検知して修正することができます。オペレーティングシステムとサードパーティ製ソフトウェア（Microsoft 製品を含む）の脆弱性が検知されます。

> アップデート機能（ウイルス対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

ソフトウェア脆弱性の検知

ソフトウェア脆弱性の検知では、Kaspersky Security Center は既知の脆弱性のデータベースに記録されている情報を使用します。このデータベースは、カスペルスキーのスペシャリストによって作成されています。データベースには、脆弱性の説明、脆弱性の検知日、脆弱性の深刻度などの情報が含まれています。アプリケーションの脆弱性に関する詳細情報は、カスペルスキーの Web サイトにあります。

Kaspersky Security Center は*脆弱性とアプリケーションのアップデートの検索*タスクを使用してソフトウェア脆弱性を検知します。

場合によっては、Microsoft Windows オペレーティングシステムで検知された脆弱性は、次のいずれかの方法を使用して修正できます：

- OS のアップデートをインストールしています。

- OS を新しいバージョンにアップグレードする（たとえば、Windows 10 から Windows 11 へ）。

このシナリオでは、KSC は同じ脆弱性に対して 2 つのエントリを表示します。

ソフトウェア脆弱性の修正

ソフトウェア脆弱性の修正では、Kaspersky Security Center はソフトウェアの製造元から提供されているソフトウェアのアップデートを使用します。次のタスクを実行すると、ソフトウェアアップデートのメタデータが管理サーバーのリポジトリにダウンロードされます：

- *管理サーバーのリポジトリへのアップデートのダウンロード*：このタスクは、カスペルスキー製品とサードパーティ製ソフトウェアのアップデートのメタデータをダウンロードするためのタスクです。このタスクは、Kaspersky Security Center のクイックスタートウィザードによって自動的に作成されます。管理サーバーのリポジトリへのアップデートのダウンロードタスクを手動で作成することもできます。

- *Windows Update の同期の実行*：このタスクは、Microsoft 製品のアップデートのメタデータをダウンロードするためのタスクです。

脆弱性を修正するためのソフトウェアのアップデートは、配布パッケージまたはパッチの形式で提供されます。ソフトウェアの脆弱性を修正するソフトウェアのアップデートは、「*修正*」という名称で呼ばれます。*推奨される修正*は、カスペルスキーのスペシャリストがインストールを推奨する修正です。*ユーザー修正*は、インストールするようにユーザーが手動で指定する修正です。ユーザー修正をインストールするには、修正を含むインストールパッケージを事前に作成する必要があります。

脆弱性とパッチ管理機能を使用できる Kaspersky Security Center ライセンスを使用している場合、ソフトウェア脆弱性の修正に*アップデートのインストールと脆弱性の修正*タスクを使用できます。このタスクでは、推奨される修正をインストールして、検知された複数の脆弱性を自動的に修正します。このタスクを使用する場合、脆弱性を修正するためのルールを手動で指定できます。

脆弱性とパッチ管理機能を使用できる Kaspersky Security Center ライセンスを使用していない場合、ソフトウェア脆弱性の修正に*脆弱性の修正*タスクを使用できます。このタスクを使用すると、Microsoft 製品に対して推奨される修正とその他のサードパーティ製ソフトウェアに対するユーザー修正をインストールして脆弱性を修正できます。

セキュリティ上の理由から、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートすべてに対して、カスペルスキーの技術によるマルウェアのスキャンが自動的に実行されます。この技術は自動的なファイルのチェックに使用され、ウイルススキャン、Sandbox 環境における静的分析、動的分析、ふるまい分析、機械学習が含まれます。

カスペルスキーは、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートを手動で分析することはありません。さらに、カスペルスキーの専門家は脆弱性（既知または未知）や文書化されていないアップデートの機能について確認したり、上記で指定されているもの以外のアップデートの分析を行ったりすることはありません。

> 管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

一部のソフトウェアに関する脆弱性の修正では、ソフトウェアのインストールについて使用許諾契約書（EULA）への同意を要求された場合、EULA に同意する必要があります。使用許諾契約書に同意しない場合、脆弱性は修正されません。

サードパーティ製ソフトウェアの脆弱性の修正

ソフトウェアの脆弱性のリストの取得が完了すると、Windows オペレーティングシステムを使用している管理対象デバイスでソフトウェアの脆弱性を修正できます。Microsoft 製品を含めて、オペレーティングシステムとサードパーティ製ソフトウェアの脆弱性を修正するには、［*脆弱性の修正*］タスクまたは［*アップデートのインストールと脆弱性の修正*］タスクを作成して実行します。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

オプションとして、次の方法でソフトウェアの脆弱性を修正するタスクを作成できます：

- 脆弱性リストを開き、修正する脆弱性を指定する。

  その結果、ソフトウェアの脆弱性を修正する新しいタスクが作成されます。オプションとして、選択した脆弱性を既存のタスクに追加できます。

- 脆弱性修正ウィザードを実行する。

  脆弱性修正ウィザードは、脆弱性とパッチ管理が使用可能なライセンスがある場合にのみ使用できます。

  このウィザードを使用すると、脆弱性の修正タスクの作成と設定手順が簡略化され、インストールするのと同じアップデートで構成される冗長なタスクを作成せずに済みます。

脆弱性リストを使用してソフトウェアの脆弱性を修正する

ソフトウェアの脆弱性を修正するには：

1. 脆弱性のリストの1つを開きます：

   - 一般的な脆弱性のリストを開くには、メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアの脆弱性**］の順に移動します。
   - 管理対象デバイスの脆弱性のリストを開くには、メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］→［<デバイス名>］→［**詳細**］→［**ソフトウェアの脆弱性**］の順に移動します。
   - 特定のアプリケーションの脆弱性のリストを開くには、メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］→［<製品名>］→［**脆弱性**］の順に移動します。

   サードパーティ製ソフトウェアの脆弱性のリストを掲載したページが表示されます。

2. リストから1つ以上の脆弱性を選択して、［**脆弱性の修正**］をクリックします。

   選択した脆弱性の一部について推奨されるソフトウェアアップデートが存在しない場合、通知メッセージが表示されます。

   一部のソフトウェアに関する脆弱性の修正では、ソフトウェアのインストールについて使用許諾契約書への同意を要求された場合、使用許諾契約書に同意する必要があります。使用許諾契約書に同意しない場合、脆弱性は修正されません。

3. 次のいずれかのオプションをオンにします：

- **新規タスク**

  新規タスクウィザードが起動します。脆弱性とパッチ管理 ライセンスをお持ちの場合は、［*アップデートのインストールと脆弱性の修正*］タスクが事前選択されています。ライセンスをお持ちでない場合は、［*脆弱性の修正*］タスクが事前選択されています。ウィザードの手順に従って、タスクの作成を完了します。

- **脆弱性の修正（指定したタスクにルールを追加）**

  選択した脆弱性を追加するタスクを選択します。脆弱性とパッチ管理 ライセンスをお持ちの場合は、［*アップデートのインストールと脆弱性の修正*］タスクを選択します。選択した脆弱性を修正するための新しいルールが、選択したタスクに自動的に追加されます。ライセンスをお持ちでない場合は、*脆弱性の修正*タスクを選択します。選択した脆弱性がタスクのプロパティに追加されます。

  タスクのプロパティウィンドウが開きます。［**保存**］をクリックして変更を保存します。

タスクの作成を選択した場合は、タスクが作成され、タスクリスト（［**アセット（デバイス）**］→［**タスク**］）に表示されます。脆弱性を既存のタスクに追加することを選択した場合、脆弱性はタスクのプロパティに保存されます。

サードパーティ製ソフトウェアの脆弱性を修正するには、［*アップデートのインストールと脆弱性の修正*］タスク、または［*脆弱性の修正*］タスクを開始します。作成したタスクが［*脆弱性の修正*］タスクである場合は、タスクの設定リストに含まれているソフトウェアの脆弱性を修正するためのソフトウェアアップデートを手動で指定する必要があります。

脆弱性修正ウィザードを使用してソフトウェアの脆弱性を修正する

脆弱性修正ウィザードは、脆弱性とパッチ管理が使用可能なライセンスがある場合にのみ使用できます。

脆弱性修正ウィザードを使用してソフトウェアの脆弱性を修正するには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアの脆弱性**］の順に移動します。

   管理対象デバイスにインストールされているサードパーティ製ソフトウェアの脆弱性のリストを掲載したページが表示されます。

2. 修正する脆弱性に隣接するチェックボックスをオンにします。

3. ［**脆弱性修正ウィザードを実行**］をクリックします。

   脆弱性修正ウィザードが起動します。［**脆弱性を修正するタスクを選択**］ページには、次の種別の既存の全タスクのリストが表示されます。

   - *アップデートのインストールと脆弱性の修正*
   - *Windows Update 更新プログラムのインストール*
   - *脆弱性の修正*

   最後の 2 つの種別のタスクを変更して新しいアップデートをインストールすることはできません。新しいアップデートをインストールする際に使用できるのは、［*アップデートのインストールと脆弱性の修正*］タスクのみです。

4. 選択した脆弱性を修正するタスクのみをウィザードに表示する場合は、［**この脆弱性を修正するタスクのみ表示**］をオンにします。

5. 目的の対象を追加します：

- タスクを開始するには、タスク名の横にあるチェックボックスをオンにして、［**開始**］をクリックします。
- 既存のタスクに新しいルールを追加するには：

  a. タスク名に隣接するチェックボックスをオンにし、［**ルールの追加**］をクリックします。

  b. 開いたページで、新しいルールを構成します：

  - **この深刻度の脆弱性すべてを修正するルール**

    ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

    このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

    このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

    既定では、このオプションはオフです。

  - **選択した脆弱性に対して推奨されるものとして定義されているアップデートと同じタイプのアップデートによって脆弱性を修正するためのルール**（Microsoftソフトウェアの脆弱性でのみ適用可能）
  - **選択した製造元のアプリケーションの脆弱性を修正するルール**（サードパーティ製ソフトウェアの脆弱性に対してのみ使用可能）
  - **選択したアプリケーションのすべてのバージョンの脆弱性を修正するルール**（サードパーティ製ソフトウェアの脆弱性に対してのみ使用可能）
  - **選択した脆弱性を修正するルール**
  - **この脆弱性を修正するアップデートを承認する**

    選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

    既定では、このオプションはオフです。

  c. ［**追加**］をクリックします。

- タスクを作成するには：

  a. ［**新規タスク**］をクリックします。

  b. 開いたページで、新しいルールを構成します：

  - **この深刻度の脆弱性すべてを修正するルール**

ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

既定では、このオプションはオフです。

- **選択した脆弱性に対して推奨されるものとして定義されているアップデートと同じタイプのアップデートによって脆弱性を修正するためのルール**（Microsoftソフトウェアの脆弱性でのみ適用可能）
- **選択した製造元のアプリケーションの脆弱性を修正するルール**（サードパーティ製ソフトウェアの脆弱性に対してのみ使用可能）
- **選択したアプリケーションのすべてのバージョンの脆弱性を修正するルール**（サードパーティ製ソフトウェアの脆弱性に対してのみ使用可能）
- **選択した脆弱性を修正するルール**
- **この脆弱性を修正するアップデートを承認する**

  選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

  既定では、このオプションはオフです。

c. ［**追加**］をクリックします。

タスクの開始を選択した場合は、ウィザードを閉じることができます。タスクはバックグラウンドモードで完了します。追加の操作は必要ありません。

ルールを既存のタスクに追加することを選択した場合は、タスクのプロパティウィンドウが開きます。新しいルールは既にタスクのプロパティに追加されています。ルールまたはその他のタスク設定を表示あるいは変更できます。［**保存**］をクリックして変更を保存します。

タスクの作成を選択した場合は、新規タスクウィザードで引き続きタスクを作成します。脆弱性修正ウィザードで追加した新しいルールは、新規タスクウィザードに表示されます。ウィザードを完了すると、［*アップデートのインストールと脆弱性の修正*］タスクがタスクリストに追加されます。

脆弱性の修正タスクの作成

*脆弱性の修正*タスクを使用すると、Windows を実行している管理対象デバイスのソフトウェアの脆弱性を修正できます。Microsoft 製品を含めて、サードパーティ製ソフトウェアの脆弱性を修正できます。

脆弱性とパッチ管理機能を利用できるライセンスをお持ちでない場合、［*脆弱性の修正*］の種別の新しいタスクは作成できません。新しい脆弱性を修正するには、それらの脆弱性を既存の［*脆弱性の修正*］タスクに追加します。［*アップデートのインストールと脆弱性の修正*］タスクを、［*脆弱性の修正*］の代わりに使用することを推奨します。［*アップデートのインストールと脆弱性の修正*］タスクを使用すると、定義したルールに従って、複数の更新をインストールし、複数の脆弱性を自動的に修正できます。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが開いている場合、終了するように指示される場合があります。

脆弱性の修正タスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**脆弱性の修正**］タスク種別を選択します。
4. 作成中のタスク名を入力します。
   タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクを割り当てるデバイスを選択します。
6. ［**追加**］をクリックします。
   脆弱性のリストが表示されます。
7. 修正する脆弱性を選択し、［**OK**］をクリックします。
   Microsoft ソフトウェアの脆弱性には通常、推奨される修正が用意されています。その他の操作は必要ありません。他の製造元のソフトウェアの脆弱性については、まず修正する脆弱性ごとにユーザー修正を指定する必要があります。その後、それらの脆弱性を*脆弱性の修正*タスクに追加できるようになります。
8. OS の再起動設定を指定します。

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

既定では、このオプションがオンです。

- **通知の繰り返し間隔（分）**

このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

- **再起動するまでの時間（分）**

ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

既定では、このオプションはオフです。

9. 次のようにアカウントの設定を指定します。

- **既定のアカウント**

タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。

既定では、このオプションがオンです。

- **アカウントの指定**

［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

- **アカウント**

タスクを実行するアカウント。

- **パスワード**

  タスクが実行されるアカウントのパスワード。

10. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

11. ［**終了**］をクリックします。
    タスクが作成され、タスクリストに表示されます。

12. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

13. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。

14. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。

［アップデートのインストールと脆弱性の修正］タスクの作成

［*アップデートのインストールと脆弱性の修正*］タスクは、脆弱性とパッチ管理 ライセンスがある場合にのみ使用できます。

［*アップデートのインストールと脆弱性の修正*］タスクは、管理対象デバイス上で Microsoft 製品やその他のサードパーティ製ソフトウェアの脆弱性をアップデートによって修正するために使用します。このタスクを使用することで、一定のルールに従って複数のアップデートをインストールしたり、複数の脆弱性を修正したりすることができます。

［*アップデートのインストールと脆弱性の修正*］タスクを使用してアップデートのインストールまたは脆弱性の修正を実行するには、次のうち 1 つの操作を実行します：

- アップデートのインストールウィザードまたは脆弱性修正ウィザードを実行します。
- ［*アップデートのインストールと脆弱性の修正*］タスクを作成します。
- 既存の［*アップデートのインストールと脆弱性の修正*］タスクにアップデートのインストールに関するルールを追加します。

［アップデートのインストールと脆弱性の修正］タスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。

2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

3. Kaspersky Security Center を対象アプリケーションとするタスクから、［**アップデートのインストールと脆弱性の修正**］タスク種別を選択します。

   タスクが表示されない場合は、［**システム管理**：**脆弱性とパッチ管理**］機能領域の**読み取り**、**変更**、および**実行**権限がアカウントに付与されていることを確認してください。これらのアクセス権がない場合、*アップデートのインストールと脆弱性の修正*タスクを作成および設定することはできません。

4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。

5. タスクを割り当てるデバイスを選択します。

6. アップデートインストールのルールを指定してから、次の設定を指定します：

   - **デバイスの再起動時またはシャットダウン時にインストールを開始する**

     このオプションをオンにすると、デバイスの再起動時またはシャットダウン時にアップデートがインストールされます。オプションがオフの場合、アップデートのインストールはスケジュールに従って実行されます。

     アップデートのインストールによりデバイスのパフォーマンスに影響を与える可能性がある場合は、このオプションを使用します。

     既定では、このオプションはオフです。

   - **必要なシステムコンポーネントをインストールする**

     このオプションをオンにすると、アップデートのインストール前にインストールが必要な一般システムコンポーネントをすべて自動的にインストールします。インストールが必要な対象とは、たとえばオペレーティングシステムのアップデートなどです。

     このオプションをオフにすると、必須コンポーネントを手動でインストールすることが必要となる場合があります。

     既定では、このオプションはオフです。

   - **アップデート中に新しい製品のバージョンのインストールを許可する**

     このオプションをオンにすると、製品の新しいバージョンをインストールするアップデートを許可できます。

     このオプションをオフにすると、製品はアップグレードされません。製品の新しいバージョンは手動でインストールするか、別のタスクを通してインストールできます。この設定は、所属企業のインフラストラクチャでソフトウェアの新しいバージョンがサポートされていなかったり、アップグレードをテスト環境で確認したい場合に使用します。

     既定では、このオプションはオンです。

     製品をアップデートすることにより、クライアントデバイスにインストールされた対象製品に依存するアプリケーションが正しく動作しなくなることがあります。

   - **デバイスにアップデートをダウンロードするがインストールしない**

このオプションをオンにすると、アップデートをデバイスにダウンロードしますが、自動ではインストールしません。ダウンロードされたアップデートを手動でインストールできます。

Microsoft 製品のアップデートは、システム Windows フォルダーにダウンロードされます。サードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートは、［**アップデートのダウンロード先**］で指定したフォルダーにダウンロードされます。

このオプションをオフにすると、アップデートはデバイスに自動的にインストールされません。

既定では、このオプションはオフです。

- **アップデートのダウンロード先**

このフォルダーはサードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートのダウンロードに使用されます。

- **詳細な診断を有効にする**

このオプションをオンにすると、Kaspersky Security Center リモート診断ユーティリティでネットワークエージェントによるトレースがオフになっていても、ネットワークエージェントがトレースを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center リモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

既定では、このオプションはオフです。

- **詳細な診断ファイルの最大サイズ（MB）**

既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

7. OS の再起動設定を指定します。

- **デバイスを再起動しない**

操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

- **通知の繰り返し間隔（分）**

  このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

  既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

  このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

- **再起動するまでの時間（分）**

  ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

  既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了するまで待機する時間（分）**

  ユーザーのデバイスがロックされた場合にアプリケーションが強制終了されます（指定した非アクティブの時間が経過した後に自動で、または手動で）。

  このオプションを有効にすると、入力フィールドに指定した時間を過ぎた時に、ロックされたデバイスでアプリケーションが強制的に終了します。

  このオプションをオフにすると、ロックされたデバイスでアプリケーションは終了しません。

  既定では、このオプションはオフです。

8. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

9. ［**終了**］をクリックします。

   タスクが作成され、タスクリストに表示されます。

10. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

11. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。

12. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。

タスクの結果に 0x80240033「Windows Update Agent error 80240033（「License terms could not be downloaded.」）」エラーが含まれている場合、Windows レジストリを使用してこの問題を解決することができます。

アップデートインストールのルールの追加

この機能は、脆弱性とパッチ管理 ライセンスでのみ使用できます。

［*アップデートのインストールと脆弱性の修正*］タスクを使用してソフトウェアのアップデートをインストールする、またはソフトウェアの脆弱性を修正する場合は、アップデートインストールのルールを指定する必要があります。これらのルールにより、インストールするアップデートと修正する脆弱性が決定されます。

厳密な設定内容は、追加するルールがすべてのアップデート、Windows Update 更新プログラム、サードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートのいずれを対象とするのかによって異なります。Windows Update 更新プログラムまたはサードパーティ製品のアップデートのいずれかを対象にルールを追加する場合は、アップデートをインストールする特定のアプリケーションとバージョンを選択できます。すべてのアップデートのルールを追加する場合は、インストールする特定のアップデートおよびアップデートをインストールすることで修正する脆弱性を選択できます。

次の方法で、アップデートのインストールのルールを追加できます：

- 新規のアップデートのインストールと脆弱性の修正タスクの作成中にルールを追加する。
- 既存の［*アップデートのインストールと脆弱性の修正*］タスクの［**Application Settings**］タブでルールを追加する。
- アップデートのインストールウィザードまたは脆弱性修正ウィザード。

すべてのアップデートを対象とするルールを追加するには：

1. ［**追加**］をクリックします。

   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

2. ［**ルール種別**］ページで、［**すべてのアップデートのルール**］を選択します。

3. ［**全般基準**］ウィンドウで、ドロップダウンリストを使用して次の設定を指定します。

   - **インストールするアップデートの設定**

クライアントデバイスにインストールする必要がある更新を選択します。

- **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
- **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
- **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。

- **次のレベル以上の深刻度の脆弱性を修正する**

ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

既定では、このオプションはオフです。

4. ［**アップデート**］ウィンドウで、インストールするアップデートを選択します：

- **すべての適用可能なアップデートをインストールする**

ウィザードの［**全般基準**］ウィンドウで指定した基準に合致するソフトウェアアップデートをすべてインストールします。既定では、この項目が選択されます。

- **リストのアップデートのみをインストールする**

手動で選択したリストのソフトウェアアップデートのみをインストールします。追加できるアップデートには、使用可能なすべてのソフトウェアアップデートが含まれます。

特定のアップデートを選択する状況としてはたとえば、テスト環境でのインストールの確認、重要なアプリケーションのみのアップデート、特定のアプリケーションのみのアップデートなどが考えられます。

- **選択したアップデートのインストールに必要な以前のアップデートをすべて自動的にインストールする**

選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、このオプションをオンのままにします。

このオプションをオフにすると、選択したバージョンのアプリケーションのみがインストールされます。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、このオプションをオフにします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

たとえば、デバイスにアプリケーションのバージョン 3 がインストールされていて、バージョン 5 にアップデートしたいが、バージョン 5 はバージョン 4 経由のみでしかインストールできない状況を想定します。このオプションをオンにすると、先にバージョン 4 をインストールし、続いてバージョン 5 をインストールします。このオプションをオフにすると、アプリケーションのアップデートは失敗します。

既定では、このオプションはオンです。

5. ［**脆弱性**］ウィンドウで、選択したアップデートのインストールで修正する脆弱性を選択します：

   - **他の基準に一致するすべての脆弱性を修正する**

     ウィザードの［**全般基準**］ウィンドウで指定した基準に合致する脆弱性をすべて修正します。既定では、この項目が選択されます。

   - **リストの脆弱性のみを修正する**

     手動で選択したリストの脆弱性のみをインストールします。追加できるアップデートには、検知されたすべての脆弱性が含まれます。

     特定の脆弱性を選択する状況としてはたとえば、テスト環境での脆弱性の修正の確認、重要なアプリケーションのみでの脆弱性の修正、特定のアプリケーションのみでの脆弱性の修正などが考えられます。

6. ［**名前**］ページで、追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**設定**］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが追加され、新規タスクウィザードまたはタスクのプロパティに表示されます。

Windows Update 更新プログラムを対象とする新しいルールを追加するには：

1. ［**追加**］をクリックします。
   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
2. ［**ルール種別**］ページで、［**Windows Update のルール**］を選択します。
3. ［**全般基準**］ウィンドウで、次の設定を指定します：

   - **インストールするアップデートの設定**

クライアントデバイスにインストールする必要がある更新を選択します。

- **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
- **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
- **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。

- **次のレベル以上の深刻度の脆弱性を修正する**

ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

既定では、このオプションはオフです。

- **次のレベル以上の MSRC 深刻度の脆弱性を修正する**

ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

このオプションをオンにすると、MSRC（Microsoft Security Response Center）が設定する重要度レベルが、リストで選択した値（**低**、**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

既定では、このオプションはオフです。

4. ［**アプリケーション**］ウィンドウで、アップデートをインストールするアプリケーションとアプリケーションのバージョンを選択します。既定では、すべてのアプリケーションがオンです。

5. ［**アップデートのカテゴリ**］ウィンドウで、インストールするアップデートのカテゴリを選択します。これらのカテゴリは Microsoft Update カタログで使用されているのと同じカテゴリです。既定では、すべてのカテゴリがオンです。

6. ［**名前**］ページで、追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**設定**］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが追加され、新規タスクウィザードまたはタスクのプロパティに表示されます。

サードパーティ製品のアップデートを対象とする新しいルールを追加するには：

1. ［**追加**］をクリックします。
   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
2. ［**ルール種別**］ページで、［**サードパーティ製品のアップデートのルール**］を選択します。
3. ［**全般基準**］ウィンドウで、次の設定を指定します：

   - **インストールするアップデートの設定**

     クライアントデバイスにインストールする必要がある更新を選択します。
     - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
     - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
     - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。

   - **次のレベル以上の深刻度の脆弱性を修正する**

     ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

     このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

     このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

     既定では、このオプションはオフです。
4. ［**アプリケーション**］ウィンドウで、アップデートをインストールするアプリケーションとアプリケーションのバージョンを選択します。既定では、すべてのアプリケーションがオンです。
5. ［**名前**］ページで、追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［設定］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが追加され、新規タスクウィザードまたはタスクのプロパティに表示されます。

サードパーティ製ソフトウェアの脆弱性へのユーザー修正の選択

［*脆弱性の修正*］タスクを使用するには、タスクの設定で、サードパーティ製ソフトウェアの脆弱性を修正するソフトウェアアップデートを手動で指定する必要があります。［*脆弱性の修正*］タスクでは、Microsoft 製品に対しては推奨される修正を、その他のサードパーティ製ソフトウェアに対してはユーザー修正をインストールして脆弱性を修正します。*ユーザー修正*は、脆弱性を修正するためにインストールするように管理者が手動で指定するソフトウェアアップデートです。

サードパーティ製ソフトウェアの脆弱性へのユーザー修正を選択するには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアの脆弱性**］の順に移動します。
   クライアントデバイスで検知されたソフトウェア脆弱性のリストが表示されます。
2. ソフトウェア脆弱性のリストで、ユーザー修正を適用するように指定する脆弱性の名前のリンクをクリックします。
   脆弱性のプロパティウィンドウが表示されます。
3. 左側のペインで、［**ユーザーによる修正とその他の修正**］セクションを選択します。
   選択したソフトウェア脆弱性に対するユーザー修正のリストが表示されます。
4. ［**追加**］をクリックします。
   利用可能なインストールパッケージのリストが表示されます。ここで表示されるインストールパッケージのリストは、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］リストの順に移動して表示されるリストと同じものです。選択している脆弱性に対するユーザー修正を含んだインストールパッケージを作成していない場合、新規パッケージウィザードを起動してパッケージを作成できます。
5. サードパーティ製ソフトウェアの脆弱性に対するユーザー修正を含んだインストールパッケージを1つ以上選択します。
6. ［**保存**］をクリックします。

ソフトウェア脆弱性に対するユーザー修正を含んだインストールパッケージが指定されます。*脆弱性の修正*タスクが実行されると、インストールパッケージがインストールされてソフトウェア脆弱性が修正されます。

管理対象デバイスで検知されたすべてのソフトウェア脆弱性に関する情報の表示

管理対象デバイスでのソフトウェア脆弱性のスキャンが完了すると、管理対象デバイスで検知されたすべてのソフトウェア脆弱性を表示できます。管理サーバーの階層に対してタスクを実行すると、選択した管理サーバーに対してのみ、脆弱性が検知された管理対象デバイスのリストを表示できます。

管理対象デバイスで検知されたすべてのソフトウェア脆弱性のリストを表示するには：

メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアの脆弱性**］の順に移動します。

クライアントデバイスで検知されたソフトウェア脆弱性のリストが表示されます。

また、脆弱性レポートの生成と表示も実行できます。

ソフトウェア脆弱性のリストの表示では、フィルターを指定できます。ソフトウェア脆弱性のリストの右上にある**フィルター**アイコン（  ）をクリックして、フィルターを指定してください。ソフトウェアの脆弱性リストの上の［**設定済みのフィルター**］ドロップダウンリストから、いずれかの設定済みのフィルターを選択することもできます。

リスト内の任意の脆弱性に関する詳細情報を取得できます。

ソフトウェア脆弱性に関する情報を取得するには：

ソフトウェア脆弱性のリストで、脆弱性の名前のリンクをクリックします。

ソフトウェアの脆弱性のプロパティウィンドウが開きます。

指定した管理対象デバイスで検知されたソフトウェア脆弱性に関する情報の表示

指定した管理対象の Windows デバイスで検知されたソフトウェア脆弱性に関する情報を表示できます。

指定した管理対象デバイスで検知されたソフトウェア脆弱性のリストをエクスポートするには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、検知されたソフトウェア脆弱性を表示するデバイスの名前のリンクをクリックします。
   選択したデバイスのプロパティウィンドウが表示されます。
3. 選択したデバイスのプロパティウィンドウで、［**詳細**］タブを選択します。
4. 左側のペインで、［**ソフトウェアの脆弱性**］セクションを選択します。
   選択した管理対象デバイスで検知された脆弱性のリストが表示されます。

選択したソフトウェア脆弱性のプロパティを表示するには：

ソフトウェア脆弱性のリストで、脆弱性の名前のリンクをクリックします。

選択したソフトウェア脆弱性のプロパティウィンドウが表示されます。

管理対象デバイス上の脆弱性に関する統計情報の表示

管理対象デバイス上でのそれぞれのソフトウェア脆弱性に関する統計情報を表示できます。統計情報は図表として表示されます。図表には、次のステータスごとに該当するデバイス数が表示されます：

- *無視：<デバイス数>*：脆弱性のプロパティでその脆弱性を無視するように手動で設定した場合に、このステータスが割り当てられます。
- *修正済み：<デバイス数>*：脆弱性を修正するためのタスクが正常に完了した場合に、このステータスが割り当てられます。
- *修正をスケジュール済み：<デバイス数>*：脆弱性を修正するためのタスクを作成済みだが、タスクがまだ実行されていない場合に、このステータスが割り当てられます。
- *パッチが適用済み：<デバイス数>*：脆弱性の修正をするためのソフトウェアのアップデートを手動で選択したが、そのソフトウェアのアップデートでは脆弱性が修正されていない場合に、このステータスが割り当てられます。

- *修正が必要：<デバイス数>*：脆弱性が一部の管理対象デバイスでのみ修正されており、さらに多くの管理対象デバイスで脆弱性を修正する必要がある場合に、このステータスが割り当てられます。

管理対象デバイス上の脆弱性に関する統計情報を表示するには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアの脆弱性**］の順に移動します。
   管理対象デバイスで検知されたソフトウェア脆弱性のリストが表示されます。
2. 目的の脆弱性に隣接するチェックボックスをオンにします。
3. ［**デバイスの脆弱性の統計**］をクリックします。

脆弱性のステータスを示した図表が表示されます。それぞれのステータスをクリックすると、選択したステータスの脆弱性が存在するデバイスのリストが表示されます。

ソフトウェア脆弱性のリストのファイルへのエクスポート

表示されている脆弱性のリストを CSV ファイルまたは TXT ファイルにエクスポートできます。エクスポートしたファイルは、情報セキュリティ部門に共有したり、統計情報を取得するために保存するなどの用途に使用できます。

管理対象デバイスで検知されたすべてのソフトウェア脆弱性のリストをファイルにエクスポートするには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアの脆弱性**］の順に移動します。
   管理対象デバイスで検知されたソフトウェア脆弱性のリストが表示されます。
2. エクスポートするファイルの形式に応じて、［**TXT へエクスポート**］または［**CSV へエクスポート**］をクリックします。

操作に使用しているデバイスに、ソフトウェア脆弱性のリストをエクスポートしたファイルがダウンロードされます。

選択した管理対象デバイスで検知されたソフトウェア脆弱性のリストをファイルにエクスポートするには：

1. 選択した管理対象デバイスで検知されたソフトウェア脆弱性のリストを表示します。
2. エクスポートするソフトウェア脆弱性項目を選択します。
   選択した管理対象デバイスで検知されたソフトウェア脆弱性のリストをそのままエクスポートする場合は、この手順をスキップします。
   ただし、選択した管理対象デバイスで検知されたソフトウェア脆弱性のリストをそのままエクスポートする場合でも、エクスポートできるのはウィンドウで現在表示されている脆弱性項目のみです。
3. エクスポートするファイルの形式に応じて、［**TXT へエクスポート**］または［**CSV へエクスポート**］をクリックします。

操作に使用しているデバイスに、選択した管理対象デバイスで検知されたソフトウェア脆弱性のリストをエクスポートしたファイルがダウンロードされます。

検知されたソフトウェアの脆弱性への非対応の判断

必要に応じて、検知されたソフトウェア脆弱性を無視することもできます。ソフトウェア脆弱性に対応しない理由として、次が考えられます：

- 管理者として、該当するソフトウェアの脆弱性が組織内で緊急なものではないと判断した場合。
- 脆弱性の修正を適用すると、該当するソフトウェアでデータの破損などが生じる可能性があることが判明した場合。
- 管理者として、管理対象デバイスを保護する別の対策を使用しているため、ソフトウェア脆弱性が組織ネットワークにとって危険ではないと判断した場合。

すべてのデバイス上または選択した特定のデバイス上で、ソフトウェア脆弱性を無視できます。

すべての管理対象デバイスで、特定のソフトウェア脆弱性に対応せずに無視するには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアの脆弱性**］の順に移動します。
   管理対象デバイスで検知されたソフトウェア脆弱性のリストが表示されます。
2. ソフトウェア脆弱性のリストで、対応せずに無視する脆弱性の名前のリンクをクリックします。
   ソフトウェア脆弱性のプロパティウィンドウが開きます。
3. ［**全般**］タブで、［**脆弱性を無視**］をオンにします。
4. ［**保存**］をクリックします。
   ソフトウェア脆弱性のプロパティウィンドウが閉じます。

すべての管理対象デバイスで、対象のソフトウェア脆弱性が無視されます。

選択した管理対象デバイスで、特定のソフトウェア脆弱性に対応せずに無視するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、特定のソフトウェア脆弱性を無視するデバイスの名前のリンクをクリックします。
   デバイスのプロパティウィンドウが表示されます。
3. デバイスのプロパティウィンドウで［**詳細**］タブを選択します。
4. 左側のペインで、［**ソフトウェアの脆弱性**］セクションを選択します。
   デバイスで検知された脆弱性のリストが表示されます。
5. ソフトウェア脆弱性のリストで、選択しているデバイス上で対応せずに無視する脆弱性を選択します。
   ソフトウェア脆弱性のプロパティウィンドウが開きます。
6. ソフトウェア脆弱性のプロパティウィンドウの［**全般**］タブで、［**脆弱性を無視**］をオンにします。
7. ［**保存**］をクリックします。
   ソフトウェア脆弱性のプロパティウィンドウが閉じます。
8. デバイスのプロパティウィンドウを閉じます。

選択したデバイスで、対象のソフトウェア脆弱性が無視されます。

無視することを選択したソフトウェアの脆弱性は、［*脆弱性の修正*］タスクまたは［*アップデートのインストールと脆弱性の修正*］タスクが完了しても修正されません。脆弱性のリストで、無視することを選択した脆弱性をフィルターを使用して表示から除外することができます。

クライアントデバイス上で実行されるアプリケーションの管理

このセクションでは、クライアントデバイス上で実行されるアプリケーションの管理と関連する Kaspersky Security Center の機能について説明します。

アプリケーションコントロールを使用して実行ファイルを管理する

アプリケーションコントロールコンポーネントを使用すると、ユーザーデバイス上の実行ファイルの起動を許可またはブロックできます。アプリケーションコントロールコンポーネントは、Windows ベースおよび Linux ベースのオペレーティングシステムをサポートします。

Linux ベースのオペレーティングシステムの場合、Application Control コンポーネントは Kaspersky Endpoint Security 11.2 for Linux 以降から使用できます。

必須条件

- 組織内に Kaspersky Security Center が導入されている。
- Kaspersky Endpoint Security for Windows または Kaspersky Endpoint Security for Linux のポリシーが作成され、有効になっている。

実行するステップ

アプリケーションコントロールのユーザーシナリオは次のステップに分かれています：

1. **クライアントデバイス上の実行ファイルのリストの作成と表示**

   このステップでは、管理対象デバイスでどのような実行ファイルが検知されたかを把握できます。実行ファイルのリストを表示して、許可対象の実行ファイルと禁止対象の実行ファイルのリストと照合してください。組織の情報セキュリティポリシーに関連した制限が実行ファイルに対して必要になる場合もあります。

   実行手順の説明：

   - 管理コンソール：実行ファイルのインベントリ
   - Kaspersky Security Center Web コンソール：クライアントデバイスにある実行ファイルのリストの取得と表示

2. **組織内で使用される実行ファイルのカテゴリを作成する**

   管理対象デバイスに保管されている実行ファイルのリストを分析します。分析に基づいて、実行ファイルのカテゴリを作成します。組織で使用される標準的な実行ファイル群をカバーする「作業用アプリケーション」カテゴリを作成することを推奨します。異なるセキュリティグループがそれぞれの業務で実行ファイルセットを使用する場合、セキュリティグループごとに別のカテゴリを作成することができます。

   実行手順の説明：

- 管理コンソール：コンテンツが手動で追加されるアプリケーションカテゴリの作成、選択したデバイス上の実行ファイルが含まれるアプリケーションカテゴリの作成、特定のフォルダーの実行ファイルが含まれるアプリケーションカテゴリの作成。

- Kaspersky Security Center Web コンソール：コンテンツが手動で追加されるアプリケーションカテゴリの作成、選択したデバイス上の実行ファイルが含まれるアプリケーションカテゴリの作成、特定のフォルダーの実行ファイルが含まれるアプリケーションカテゴリの作成。

3. **Kaspersky Endpoint Security ポリシーでのアプリケーションコントロール機能の設定**

   上述したステップで作成したカテゴリを使用して、Kaspersky Endpoint Security ポリシー内でアプリケーションコントロール機能を設定します。

   実行手順の説明：

   - 管理コンソール：クライアントデバイスでのアプリケーション起動コントロールの設定

   - Kaspersky Security Center Web コンソール：Kaspersky Endpoint Security ポリシーでのアプリケーションコントロールの設定

4. **アプリケーションコントロール機能のテストモードでの有効化**

   アプリケーションコントロールルールが業務で必要な実行ファイルをブロックしないことを確認するため、新規ルールの作成後にテストを有効にして動作を検証することを推奨します。テストモードで実行している場合、Kaspersky Endpoint Security for Windows は、アプリケーションコントロールルールで起動が禁止されている実行ファイルをブロックせず、その起動について管理サーバーに通知します。

   アプリケーションコントロールルールのテストでは、次の手順の実施を推奨します：

   - 必要に応じたテスト期間を指定する。必要なテスト期間は数日から 2 カ月ほどまで、ルールに応じて異なります。

   - アプリケーションコントロールの動作テストによって記録されたイベントを分析する。

   Kaspersky Security Center Web コンソールの使用方法：Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定これらの手順に従って、設定プロセスで**テストモード**を有効にします。

5. **アプリケーションコントロール機能におけるカテゴリ設定の変更**

   必要に応じて、アプリケーションコントロール設定に変更を行います。テスト結果に応じて、アプリケーションコントロールコンポーネントのイベントに関連していた実行ファイルを「手動でコンテンツを追加するカテゴリ」に追加できます。

   実行手順の説明：

   - 管理コンソール：イベントに関連する実行ファイルのアプリケーションカテゴリへの追加

   - Kaspersky Security Center Web コンソール：イベントに関連する実行ファイルのアプリケーションカテゴリへの追加

6. **アプリケーションコントロールルールの実運用での適用**

   アプリケーションコントロールルールのテストとカテゴリの設定が完了したら、運用モードで実際にアプリケーションコントロールルールを適用できます。

   Kaspersky Security Center Web コンソールの使用方法：Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定これらの手順に従って、設定プロセスで**テストモード**を無効にします。

7. **アプリケーションコントロールの設定の検証**

   次の手順がすべて完了していることを確認してください：

- 実行ファイルのカテゴリを作成しました。
- カテゴリを使用してアプリケーションコントロールルールの設定します。
- アプリケーションコントロールルールの実運用での適用。

結果

シナリオが完了すると、管理対象デバイス上の実行ファイルの起動がコントロールされます。ユーザーは、組織で許可されている実行ファイルのみを実行することができ、組織で禁止されている実行ファイルを実行することはできません。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ
- Kaspersky Security for Virtualization Light Agent

アプリケーションコントロールモードとカテゴリ

アプリケーションコントロールコンポーネントは、ユーザーによる実行ファイルの起動の試行を監視します。アプリケーションコントロールルールを使用して、実行ファイルの起動を制御できます。

アプリケーションコントロールコンポーネントは、Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security 11.2 for Linux 以降のバージョン、および Kaspersky Security for Virtualization Light Agent で使用できます。このセクションでは、Kaspersky Endpoint Security for Windows でのアプリケーションコントロール機能の設定方法について説明します。

アプリケーションコントロールルールのいずれにも一致しない設定の実行ファイルの起動は、コンポーネントの選択された動作モードによって規制されます：

- *拒否リスト*：このモードは、ブロックルールで指定された実行ファイル以外のすべての実行ファイルの起動を許可する場合に使用します。既定ではこのモードが選択されます。
- *許可リスト*。このモードは、許可ルールで指定された実行ファイル以外のすべての実行ファイルの起動をブロックしたい場合に使用します。

アプリケーションコントロールルールは、実行ファイルのカテゴリを通じて実装されます。Kaspersky Security Center では、3 つのカテゴリの種別を使用できます：

- 手動でコンテンツを追加するカテゴリ：ファイルのメタデータ、ハッシュコード、証明書、KL カテゴリ、ファイルパスなど、実行ファイルをカテゴリに含める条件を指定します。
- 選択したデバイスの実行ファイルを含むカテゴリ：デバイスを指定して、デバイス上に存在する実行ファイルを自動的にカテゴリに含めます。
- 選択したフォルダーの実行ファイルを含むカテゴリ：フォルダーを指定して、フォルダー上に存在する実行ファイルを自動的にカテゴリに含めます。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ
- Kaspersky Security for Virtualization Light Agent

クライアントデバイス上の実行ファイルのリストの取得と表示

ユーザーが実行ファイルを起動しようとすると、このファイルは自動的にアプリケーションコントロールのリストに追加されます。インベントリタスクを作成して、管理対象デバイスに保存されている実行ファイルのリストを取得できます。実行ファイルのインベントリを実行するには、インベントリタスクを作成する必要があります。

実行ファイルのインベントリ機能は、次のアプリケーションで使用できます：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux（バージョン 11.2 およびそれ以降）
- Kaspersky Security for Virtualization 4.0 Light Agent 以降のバージョン

インストールされているアプリケーションに関する情報を取得しながらデータベースの負荷を軽減できます。これを行うには、ソフトウェアの標準セットがインストールされている参照デバイスでインベントリタスクを実行することをお勧めします。

クライアントデバイス上の実行ファイルのインベントリタスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. ［**新規タスク設定**］ページの［**アプリケーション**］ドロップダウンリストで、クライアントデバイスのオペレーティングシステムの種別に応じて、Kaspersky Endpoint Security for Windows または Kaspersky Endpoint Security for Linux を選択します。
4. ［**タスク種別**］ドロップダウンリストから［**インベントリ**］を選択します。
5. ［**タスク作成の終了**］ページで、［**終了**］をクリックします。

新規タスクウィザードの終了後、指定した設定で**インベントリ**タスクが作成されます。必要に応じて、作成したタスクの設定を編集できます。作成したタスクはタスクリストに表示されます。

インベントリタスクの詳細については、次のヘルプを参照してください：

- Kaspersky Endpoint Security for Windows のヘルプ
- Kaspersky Endpoint Security for Linux のヘルプ
- Kaspersky Security for Virtualization Light Agent

インベントリタスクの実行が完了すると、管理対象デバイス上に保管された実行ファイルのリストが作成され、このリストを表示できるようになります。

インベントリでは、次の形式の実行ファイルが検出されます：MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR、HTML。

クライアントデバイス上に保管された実行ファイルのリストを表示するには：

メインメニューで、［**操作**］→［**サードパーティ製品**］→［**実行ファイル**］の順に選択します。

クライアントデバイス上に保管された実行ファイルのリストが表示されます。

管理対象デバイスの実行ファイルをカスペルスキーに送るには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**実行ファイル**］の順に移動します。
2. カスペルスキーに送る実行ファイルのリンクをクリックします。
3. 表示されたウィンドウで、［**デバイス**］セクションに移動し、実行ファイルの送信元の管理対象デバイスのチェックボックスをオンにします。

   実行ファイルを送信する前に、［**管理サーバーから切断しない**］を選択して管理対象デバイスが管理サーバーに直接接続されていることを確認してください。

4. ［**カスペルスキーに送信**］をクリックします。

選択した実行ファイルがダウンロードされ、カスペルスキーに送信されます。

コンテンツが手動で追加されるアプリケーションカテゴリの作成

組織内で起動を許可またはブロックする実行ファイルのテンプレートとしての条件を、単独でまたは組み合わせて指定できます。一定の条件に一致する実行ファイルをまとめて管理するために、アプリケーションカテゴリを作成してアプリケーションコントロールの設定で使用できます。

コンテンツが手動で追加されるアプリケーションカテゴリを作成するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションカテゴリ**］の順に移動します。

   アプリケーションカテゴリのリストが表示されます。

2. ［**追加**］をクリックします。

   新規カテゴリウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ［**カテゴリの作成方法の選択**］ステップで、［**手動でコンテンツを追加するカテゴリ：実行ファイルのデータを手動でカテゴリに追加します**］を選択します。
4. ［**条件**］ステップで［**追加**］をクリックして、作成中のカテゴリに含めるファイルの条件を追加します。
5. ［**条件の基準**］ステップで、カテゴリを作成するルールの種別をリストから選択します：

- **KL カテゴリから選択**

  このオプションをオンにすると、カスペルスキー製品のカテゴリを、アプリケーションカテゴリにアプリケーションを追加する条件として指定できます。指定したカスペルスキー製品カテゴリのアプリケーションが、アプリケーションカテゴリに追加されます。

- **リポジトリから証明書を選択**

  このオプションをオンにすると、保管領域の証明書を指定できます。指定された証明書に従って署名された実行ファイルが、アプリケーションカテゴリに追加されます。

- **アプリケーションのパスを指定（マスクをサポート）**

  このオプションをオンにすると、クライアントデバイス上のファイルやフォルダーのパスを指定できます。指定したファイルやフォルダーに含まれる実行ファイルが、アプリケーションカテゴリに追加されます。「*C:\path_to_exe**」などの正規表現を使用できます。例：*C:\Program Files\Internet Explorer**。

- **リムーバブルドライブ**

  このオプションをオンにすると、アプリケーションを実行するメディアの種別（任意のドライブまたはリムーバブルドライブ）を指定できます。指定した種別のドライブ上で実行されたアプリケーションが、アプリケーションカテゴリに追加されます。

- **ハッシュ、メタデータ、証明書のいずれか**：

  - **実行ファイルリストから選択**

    このオプションをオンにすると、クライアントデバイス上の実行ファイルのリストを使用して、アプリケーションを選択してカテゴリに追加できます。

  - **アプリケーションレジストリから選択**

    このオプションをオンにすると、アプリケーションレジストリが表示されます。アプリケーションをレジストリから選択し、次のようなファイルのメタデータを指定できます：

    - ファイル名。
    - ファイルバージョン。バージョンの正確な数字を指定することも、「次より多い：5.0」のような条件を指定することもできます。
    - アプリケーション名。
    - アプリケーションのバージョン。バージョンの正確な数字を指定することも、「次より多い：5.0」のような条件を指定することもできます。
    - 製造元。

  - **手動で指定**

このオプションをオンにした場合、ファイルのハッシュ、メタデータ、証明書のいずれかを、アプリケーションカテゴリにアプリケーションを追加する条件として指定する必要があります。

ファイルのハッシュ

ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、このカテゴリ内のファイルに、Kaspersky Security Center によるハッシュ値計算のアルゴリズムを選択する必要があります。計算されたハッシュ値に関する情報は、管理サーバーのデータベースに保存されます。ハッシュ値の保存でデータベースのサイズが大幅に増えることはありません。

暗号学的ハッシュ関数 SHA256 はアルゴリズムに脆弱性が発見されておらず、現在最も信頼できる暗号化機能と判断されています。SHA256 計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降でサポートされています。ハッシュ関数 MD5 の計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のすべてのバージョンでサポートされます。

カテゴリ内のファイルに、Kaspersky Security Center によるハッシュ値計算のオプションを選択します：

- ネットワークにインストールされているセキュリティ製品のすべてのインスタンスが Kaspersky Endpoint Security 10 Service Pack 2 for Windows またはそれ以降のバージョンである場合は、［**SHA256**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンで、実行ファイルの SHA256 ハッシュ値の基準に従って作成したカテゴリは追加しないでください。セキュリティ製品の動作に不具合が生じることがあります。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 MD5 を使用することができます。

- ネットワークに Kaspersky Endpoint Security 10 Service Pack 2 for Windows より以前のバージョンの製品がインストールされている場合は、［**MD5 ハッシュ**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョン向けの実行ファイルの MD5 チェックサムの基準に従って作成したカテゴリは追加できません。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 SHA256 を使用できます。

- ネットワークにある別々の端末で Kaspersky Endpoint Security 10 の以前のバージョンと以降のバージョンと両方が使用されている場合は、［**SHA256**］と［**MD5 ハッシュ**］の両方をオンにしてください。

メタデータ

このオプションをオンにすると、ファイル名、バージョン、製造元などのファイルのメタデータを指定できます。メタデータが管理サーバーに送信されます。同じメタデータを含む実行ファイルがアプリケーションカテゴリに追加されます。

証明書

このオプションをオンにすると、保管領域の証明書を指定できます。指定された証明書に従って署名された実行ファイルが、アプリケーションカテゴリに追加されます。

- **ファイル、MSI パッケージ、アーカイブフォルダーから選択**

このオプションをオンにすると、MSI インストーラーファイルを、アプリケーションカテゴリにアプリケーションを追加する条件として指定できます。アプリケーションのインストーラーのメタデータが管理サーバーに送信されます。インストーラーのメタデータが指定の MSI インストーラーと同じアプリケーションが、アプリケーションカテゴリに追加されます。

選択した基準が、条件のリストに追加されます。

アプリケーションカテゴリの作成基準は、個数の制限なく必要な数だけ追加できます。

6. ［**除外**］ステップで［**追加**］をクリックして、作成中のカテゴリから除外するファイルの条件を追加します。

7. ［**条件の基準**］ステップで、カテゴリ作成用のルールの種別を選択したときと同様に、リストからルールの種別を選択します。

ウィザードを最後まで完了すると、アプリケーションカテゴリが作成されます。新しいルールがアプリケーションカテゴリのリストに表示されます。アプリケーションコントロールを設定時に作成したアプリケーションカテゴリを使用できます。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ
- Kaspersky Security for Virtualization Light Agent

選択したデバイスの実行ファイルを含むアプリケーションカテゴリの作成

選択したデバイス上に存在する実行ファイルを、許可またはブロックする実行ファイルのテンプレートとして使用できます。選択したデバイス上に存在する実行ファイルを基準に、カテゴリを作成してアプリケーションコントロールの設定で使用できます。

抽出したデバイスからの実行ファイルを含むカテゴリを作成するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションカテゴリ**］の順に選択します。

   カテゴリ一覧のページが表示されます。

2. ［**追加**］をクリックします。

   新規カテゴリウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ［**カテゴリの作成方法の選択**］ステップで、カテゴリ名を指定して［**選択したデバイスの実行ファイルを含むカテゴリ：デバイスの実行ファイルが自動的に処理され、メトリックがカテゴリに追加されます**］をオンにします。

4. ［**追加**］をクリックします。

5. 表示されるウィンドウで、カテゴリの作成に実行ファイルを使用するデバイスを抽出します。

6. 次の設定を指定します：

   - **ハッシュ値計算アルゴリズム**

ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、このカテゴリ内のファイルに、Kaspersky Security Center によるハッシュ値計算のアルゴリズムを選択する必要があります。計算されたハッシュ値に関する情報は、管理サーバーのデータベースに保存されます。ハッシュ値の保存でデータベースのサイズが大幅に増えることはありません。

暗号学的ハッシュ関数 SHA256 はアルゴリズムに脆弱性が発見されておらず、現在最も信頼できる暗号化機能と判断されています。SHA256 計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降でサポートされています。ハッシュ関数 MD5 の計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のすべてのバージョンでサポートされます。

カテゴリ内のファイルに、Kaspersky Security Center によるハッシュ値計算のオプションを選択します：

- ネットワークにインストールされているセキュリティ製品のすべてのインスタンスが Kaspersky Endpoint Security 10 Service Pack 2 for Windows またはそれ以降のバージョンである場合は、［**SHA256**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンで、実行ファイルの SHA256 ハッシュ値の基準に従って作成したカテゴリは追加しないでください。セキュリティ製品の動作に不具合が生じることがあります。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 MD5 を使用することができます。

- ネットワークに Kaspersky Endpoint Security 10 Service Pack 2 for Windows より以前のバージョンの製品がインストールされている場合は、［**MD5 ハッシュ**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョン向けの実行ファイルの MD5 チェックサムの基準に従って作成したカテゴリは追加できません。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 SHA256 を使用できます。

ネットワークにある別々の端末で Kaspersky Endpoint Security 10 の以前のバージョンと以降のバージョンと両方が使用されている場合は、［**SHA256**］と［**MD5 ハッシュ**］の両方をオンにしてください。

既定では、［**このカテゴリのファイルの SHA256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）**］が選択されています。

［**このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）**］は既定ではオフです。

- **データを管理サーバーのリポジトリと同期**

指定したフォルダーでの変更内容を管理サーバーに定期的にチェックさせる場合は、このオプションを使用します。

既定では、このオプションはオフです。

このオプションをオンにする場合、指定したフォルダーでの変更内容をチェックする間隔（時間単位）を指定します。既定の間隔は 24 時間です。

- **ファイル種別**

このセクションでは、アプリケーションカテゴリを作成するのに使用するファイルの種別を指定できます。

すべてのファイル：カテゴリの作成時にすべてのファイルが使用されます。既定では、このオプションがオンです。

アプリケーションカテゴリ以外のファイルのみ：カテゴリの作成時に、アプリケーションカテゴリ以外のファイルのみが使用されます。

- **フォルダー**

このセクションでは、選択したデバイス上で、アプリケーションカテゴリを作成するのに使用するファイルが含まれているフォルダーを指定できます。

すべてのフォルダー：カテゴリの作成時にすべてのフォルダーのファイルが使用されます。既定では、このオプションがオンです。

指定フォルダー：カテゴリの作成時に指定したフォルダーのファイルのみが使用されます。このオプションをオンにする場合、フォルダーのパスを指定する必要があります。

ウィザードが終了すると、実行ファイルのカテゴリが作成されます。カテゴリーのリストに表示されます。作成したカテゴリは、アプリケーションコントロールの設定時に使用できます。

選択したフォルダーの実行ファイルを含むアプリケーションカテゴリの作成

選択したフォルダー上に存在する実行ファイルを、組織内で許可またはブロックする実行ファイルの条件として使用できます。選択したフォルダー上に存在する実行ファイルを基準に、アプリケーションカテゴリを作成してアプリケーションコントロールの設定で使用できます。

選択したフォルダーの実行ファイルを含むカテゴリを作成するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションカテゴリ**］の順に移動します。

   カテゴリー覧のページが表示されます。

2. ［**追加**］をクリックします。

   新規カテゴリウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ［**カテゴリの作成方法の選択**］ステップで、カテゴリ名を指定して［**特定のフォルダーの実行ファイルを含むカテゴリ：指定されたフォルダーにコピーされたアプリケーションの実行ファイルが自動的に処理され、メトリックがカテゴリに追加されます**］を選択します。

4. カテゴリの作成に使用される実行ファイルのフォルダーを指定します。

5. 次の設定を定義します：

   - **ダイナミックリンクライブラリ（DLL）をこのカテゴリに含める**

     アプリケーションカテゴリにはダイナミックリンクライブラリ（DLL 形式のファイル）が含まれ、アプリケーションコントロールコンポーネントでは、システムで実行されているそのようなライブラリの処理を記録します。このカテゴリに DLL ファイルを含めると、Kaspersky Security Center のパフォーマンスが低下することがあります。

     既定では、このチェックボックスはオフです。

   - **このカテゴリ内のスクリプトデータを含める**

     アプリケーションカテゴリにはスクリプトのデータが含まれ、ウェブ脅威対策によってスクリプトはブロックされません。このカテゴリにスクリプトデータを含めると、Kaspersky Security Center のパフォーマンスが低下することがあります。

     既定では、このチェックボックスはオフです。

- **ハッシュ値計算アルゴリズム**：**このカテゴリのファイルの SHA256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）/ このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）**

  ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、このカテゴリ内のファイルに、Kaspersky Security Center によるハッシュ値計算のアルゴリズムを選択する必要があります。計算されたハッシュ値に関する情報は、管理サーバーのデータベースに保存されます。ハッシュ値の保存でデータベースのサイズが大幅に増えることはありません。

  暗号学的ハッシュ関数 SHA256 はアルゴリズムに脆弱性が発見されておらず、現在最も信頼できる暗号化機能と判断されています。SHA256 計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降でサポートされています。ハッシュ関数 MD5 の計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のすべてのバージョンでサポートされます。

  カテゴリ内のファイルに、Kaspersky Security Center によるハッシュ値計算のオプションを選択します：

  - ネットワークにインストールされているセキュリティ製品のすべてのインスタンスが Kaspersky Endpoint Security 10 Service Pack 2 for Windows またはそれ以降のバージョンである場合は、［**SHA256**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンで、実行ファイルの SHA256 ハッシュ値の基準に従って作成したカテゴリは追加しないでください。セキュリティ製品の動作に不具合が生じることがあります。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 MD5 を使用することができます。

  - ネットワークに Kaspersky Endpoint Security 10 Service Pack 2 for Windows より以前のバージョンの製品がインストールされている場合は、［**MD5 ハッシュ**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョン向けの実行ファイルの MD5 チェックサムの基準に従って作成したカテゴリは追加できません。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 SHA256 を使用できます。

  ネットワークにある別々の端末で Kaspersky Endpoint Security 10 の以前のバージョンと以降のバージョンと両方が使用されている場合は、［**SHA256**］と［**MD5 ハッシュ**］の両方をオンにしてください。

  既定では、［**このカテゴリのファイルの SHA256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）**］が選択されています。

  ［**このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）**］は既定ではオフです。

- **変更のあったフォルダーを強制スキャンする**

  このオプションを有効にすると、カテゴリコンテンツ追加のフォルダーでの変更が定期的にチェックされます。チェックボックスに隣接する入力フィールドで、チェックの頻度を時間単位で指定できます。既定では、24 時間ごとに強制的にチェックされます。

  このオプションを無効にすると、フォルダーが強制的にチェックされることはありません。ファイルの修正、追加または削除があった場合、サーバーはそのファイルにアクセスを試みます。

  既定では、このオプションはオフです。

ウィザードが終了すると、実行ファイルのカテゴリが作成されます。カテゴリーのリストに表示されます。カテゴリはアプリケーションコントロールの設定で使用できます。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ

- Kaspersky Security for Virtualization Light Agent

アプリケーションカテゴリのリストの表示

設定された実行ファイルのカテゴリと各カテゴリの設定の一覧を表示できます。

アプリケーションカテゴリのリストを表示するには：

メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションカテゴリ**］の順に選択します。

カテゴリ一覧のページが表示されます。

アプリケーションカテゴリのプロパティを表示するには、

カテゴリの名前をクリックします。

カテゴリのプロパティウィンドウが表示されます。プロパティはいくつかのタブにグループ化されています。

イベントに関連する実行ファイルのアプリケーションカテゴリへの追加

Kaspersky Endpoint Security for Windows のポリシーでアプリケーションコントロールの設定を完了させると、イベントのリストに次のイベントが表示されます：

- **アプリケーションの起動が禁止されました**（*緊急*イベント）：このイベントは、アプリケーションコントロールの設定で、実際にルールを適用するように指定した場合に表示されます。
- **アプリケーションの起動がテストモードでブロックされています**（*情報*イベント）：このイベントは、アプリケーションコントロールの設定で、ルールをテストするように指定した場合に表示されます。
- **アプリケーションの起動禁止に関する管理者へのメッセージ**（*警告*イベント）。このイベントは、アプリケーションコントロールの設定で実際にルールを適用するように指定しており、起動時にブロックされたアプリケーションへのアクセスをユーザーが要求した場合に表示されます。

アプリケーションコントロールの動作に関するイベントを表示するために、イベントの抽出を作成しておくことを推奨します。

アプリケーションコントロールイベントの対象となった実行ファイルを、既存のアプリケーションカテゴリや新規に作成するアプリケーションカテゴリに追加できます。実行ファイルは、手動でコンテンツを追加するタイプのアプリケーションカテゴリにのみ追加できます。

アプリケーションコントロールイベントの対象となった実行ファイルをアプリケーションカテゴリに追加するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
   イベントの抽出のリストが表示されます。
2. アプリケーションコントロールに関するイベントを表示するためのイベントの抽出を選択し、イベントの抽出を実行します。

アプリケーションコントロールに関するイベントを表示するためのイベントの抽出をまだ作成していない場合は、代わりに「**最近のイベント**」などの事前定義済みのイベントの抽出を選択して実行することもできます。

イベントのリストが表示されます。

3. 対象となった実行ファイルをアプリケーションカテゴリに追加するイベントを選択し、［**カテゴリへ割り当て**］をクリックします。

   新規カテゴリウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

4. ウィザードのウィンドウで、関連する設定を指定します：

   - ［**イベントに関係する実行ファイルへの処理**］セクションで、次のいずれかのオプションをオンにします：

     - **新規アプリケーションカテゴリへ追加**

       イベントに関連する実行ファイルを元に新しいアプリケーションカテゴリを作成する場合は、このオプションをオンにします。

       既定では、このオプションがオンです。

       このオプションを選択する場合は、新しいカテゴリ名を指定してください。

     - **アプリケーションカテゴリへ追加**

       イベントに関連する実行ファイルを既存のアプリケーションカテゴリに追加する場合は、このオプションをオンにします。

       既定では、このオプションはオフです。

       このオプションを選択する場合は、実行ファイルの追加先として、手動でコンテンツを追加するタイプのアプリケーションカテゴリを選択してください。

   - ［**ルールの種別**］セクションで、次のいずれかを選択します：

     - **除外しない場合のルール**
     - **除外に追加する場合のルール**

   - ［**条件として使用する情報**］セクションで、次のいずれかのオプションをオンにします：

     - **証明書の詳細情報（証明書がないファイルの場合 SHA256 ハッシュ）**

       ファイルが証明書によって署名されていることがあります。複数のファイルが同じ証明書で署名されていることがあります。たとえば、同じアプリケーションの異なるバージョンが同じ証明書で署名されていたり、同じ開発元の様々なアプリケーションが同じ証明書で署名されていたりすることがあります。証明書を選択した場合、アプリケーションの複数のバージョンまたは同じ開発元の複数のアプリケーションが同じカテゴリに属す場合があります。

       それぞれのファイルには固有の SHA256 ハッシュ関数があります。SHA256 ハッシュ関数を選択した場合、1つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

       実行ファイルの証明書の詳細（または証明書がないファイルの SHA256 ハッシュ機能）をカテゴリルールに追加する場合は、このオプションを選択します。

       既定では、このオプションがオンです。

- **証明書の詳細情報（証明書のないファイルはスキップ）**

  ファイルが証明書によって署名されていることがあります。複数のファイルが同じ証明書で署名されていることがあります。たとえば、同じアプリケーションの異なるバージョンが同じ証明書で署名されていたり、同じ開発元の様々なアプリケーションが同じ証明書で署名されていたりすることがあります。証明書を選択した場合、アプリケーションの複数のバージョンまたは同じ開発元の複数のアプリケーションが同じカテゴリに属す場合があります。

  実行ファイルの証明書の詳細をカテゴリルールに追加する場合は、このオプションを選択します。実行ファイルに証明書がない場合、そのファイルはスキップされます。このファイルに関する情報は、カテゴリに追加されません。

- **SHA256 のみ（ハッシュのないファイルはスキップ）**

  それぞれのファイルには固有の SHA256 ハッシュ関数があります。SHA256 ハッシュ関数を選択した場合、1 つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

  実行ファイルの SHA256 ハッシュ機能の詳細だけを追加する場合、このオプションをオンにします。

- **MD5 のみ（非推奨、Kaspersky Endpoint Security 10 Service Pack 1 の場合のみ）**

  それぞれのファイルには固有の MD5 ハッシュ関数があります。MD5 ハッシュ関数を選択した場合、1 つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

  実行ファイルの MD5 ハッシュ機能の詳細だけを追加する場合、このオプションを選択します。Kaspersky Endpoint Security 10 Service Pack 1 for Windows およびそれ以前のすべてのバージョンで、MD5 ハッシュ機能の計算がサポートされています。

5. ［OK］をクリックします。

ウィザードが完了すると、アプリケーションコントロールのイベントに関連付けられていた実行ファイルが、既存のアプリケーションカテゴリまたは新規に作成したアプリケーションカテゴリに追加されます。変更または新規に作成したアプリケーションカテゴリの設定を表示できます。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ
- Kaspersky Security for Virtualization Light Agent

Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定

アプリケーションコントロールカテゴリの作成が完了すると、Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定時にこれらのカテゴリを使用できます。

Kaspersky Endpoint Security for Windows ポリシーでアプリケーションコントロール機能を設定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
   ポリシーのリストが表示されます。

2. **Kaspersky Endpoint Security for Windows** のポリシーをクリックします。
   ポリシーの設定ウィンドウが表示されます。

3. ［**アプリケーション設定**］→［**セキュリティコントロール**］→［**アプリケーションコントロール**］の順に移動します。
   ［**アプリケーションコントロール**］ウィンドウでアプリケーションコントロール設定が表示されます。

4. ［**アプリケーションコントロール**］は既定でオンになっています。［**Application Control DISABLED**］がオフの位置に切り替えられていることを確認します。

5. ［**Application Control Settings**］設定で、動作モードを有効にしてアプリケーションコントロールルールを適用し、Kaspersky Endpoint Security for Windows がアプリケーションの起動をブロックできるようにします。
   アプリケーションコントロールルールをテストする場合は、［**Application Control Settings**］セクションでテストモードを有効にします。テストモードでは、Kaspersky Endpoint Security for Windows はアプリケーションの起動をブロックしませんが、適用されたルールに関する情報をレポートに記録します。［**レポートの表示**］をクリックすると、この情報を表示できます。

6. Kaspersky Endpoint Security for Windows で、ユーザーがアプリケーションを起動したときの DLL モジュールの読み込みを監視する場合は、［**DLL モジュールの読み込みを管理**］をオンにします。
   モジュールに関する情報とモジュールを読み込んだアプリケーションに関する情報がレポートに保存されます。
   Kaspersky Endpoint Security for Windows は、［**DLL モジュールの読み込みを管理**］がオンになった後に読み込まれた DLL モジュールとドライバーのみを監視します。Kaspersky Endpoint Security for Windows の起動前に読み込まれていた DLL モジュールとドライバーも含めてすべての DLL モジュールとドライバーを監視する場合、［**DLL モジュールの読み込みを管理**］をオンにした後にコンピューターを再起動してください。

7. （省略可能な手順）［**メッセージのテンプレート**］セクションで、アプリケーションの起動がブロックされたときに表示されるメッセージのテンプレートとお手元に送信されるメッセージのテンプレートを編集できます。

8. ［**アプリケーションコントロールモード**］設定で、［**拒否リスト**］モードまたは［**許可リスト**］モードを選択します。
   既定では、［**拒否リスト**］モードが選択されています。

9. ［**ルールリストの設定**］をクリックします。
   ［**拒否リストと許可リスト**］ウィンドウで、アプリケーションカテゴリを追加できます。既定では、［**拒否リスト**］モードをオンにするとは［**拒否リスト**］タブが選択され、［**許可リスト**］モードをオンにするとは［**許可リスト**］タブが選択されます。

10. ［**拒否リストと許可リスト**］ウィンドウで［**追加**］をクリックします。
    ［**アプリケーションコントロールルール**］ウィンドウが表示されます。

11. ［**カテゴリを選択してください**］をクリックします。
    ［**アプリケーションカテゴリ**］ウィンドウが開きます。

12. 作成済みのアプリケーションカテゴリを追加します。
    ［**編集**］をクリックすると、作成済みのカテゴリの設定を編集できます。
    新しいカテゴリを作成するには、［**追加**］をクリックします。

リストからカテゴリを削除するには、［**削除**］をクリックします。

13. アプリケーションカテゴリのリストの編集が完了したら、［**OK**］をクリックします。
［**アプリケーションカテゴリ**］ウィンドウが閉じます。

14. ［**アプリケーションコントロール**ルール］ウィンドウの［**オブジェクトとその権限**］セクションで、アプリケーションコントロールルールを適用するユーザーとユーザーのグループのリストを作成します。

15. ［**OK**］をクリックして、設定を保存し［**アプリケーションコントロールルール**］ウィンドウを閉じます。

16. ［**OK**］をクリックして、設定を保存し［**拒否リストと許可リスト**］ウィンドウを閉じます。

17. ［**OK**］をクリックし、設定を保存して［**アプリケーションコントロール**］ウィンドウを閉じます。

18. Kaspersky Endpoint Security for Windows ポリシー設定のウィンドウを閉じます。

アプリケーションコントロールの設定が適用されます。ポリシーのクライアントデバイスへの適用が完了すると、実行ファイルの起動が管理されるようになります。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ
- Kaspersky Security for Virtualization Light Agent

クライアントデバイスにインストールされているアプリケーションのリストの取得と表示

Kaspersky Security Center は、Linux または Windows を実行している管理対象クライアントデバイスにインストールされているすべてのソフトウェアのインベントリを作成します。

ネットワークエージェントが、デバイスにインストールされているアプリケーションのリストを作成し、管理サーバーに送信します。ネットワークエージェントがアプリケーションリストを更新するには約 10 ～ 15 分かかります。

Windows ベースのクライアントデバイスの場合、ネットワークエージェントは、インストールされているアプリケーションに関する大部分の情報を Windows レジストリから受け取ります。Linux ベースのクライアントデバイスの場合、パッケージマネージャーはインストールされているアプリケーションに関する情報をネットワークエージェントに提供します。

［**アプリケーションレジストリ**］セクションのアプリケーションが Linux デバイス上で検出された場合、アプリケーションのプロパティには関連する実行ファイルに関する情報が含まれません。

管理対象デバイスにインストールされているアプリケーションのリストを表示するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。

このページでは、管理対象デバイスにインストールされているアプリケーションが表形式で表示されます。アプリケーションを選択して、製造元名、バージョン番号、実行ファイルのリスト、該当するアプリケーションがインストールされているデバイスのリスト、適用可能なソフトウェアアップデートのリスト、検知されたソフトウェア脆弱性のリストなど、様々なプロパティを表示します。

2. インストールされたアプリケーションの表のデータは、次のようにしてグループ化およびフィルタリングできます：

   - 表の右上隅にある設定アイコン（ ）をクリックします。

     呼び出された［**列の設定**］メニューで、表に表示する列を選択します。アプリケーションがインストールされたクライアントデバイスのオペレーティングシステムの種別を表示するには、［**OS の種別**］列を選択します。

   - 表の右上隅にあるフィルターアイコン（ ）をクリックして、呼び出されたメニューでフィルター条件を指定して適用します。

     インストールされているアプリケーションをフィルタリングした表が表示されます。

特定の管理対象デバイスにインストールされているアプリケーションのリストを表示するには：

メインメニューで、［**デバイス**］→［**管理対象デバイス**］→［**<デバイス名>**］→［**詳細**］→［**アプリケーションレジストリ**］の順に移動します。このメニューで、アプリケーションのリストを CSV ファイルまたは TXT ファイルにエクスポートできます。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ
- Kaspersky Security for Virtualization Light Agent

定義データベースからのサードパーティ製品のインストールパッケージの作成

Kaspersky Security Center Web コンソールでは、インストールパッケージを使用してサードパーティ製品のリモートインストールを実行できます。このようなサードパーティ製品は、専用の定義データベースに格納されています。この定義データベースは、*管理サーバーのリポジトリへのアップデートのダウンロードタスク*を初めて実行した時に自動的に作成されます。

定義データベースからサードパーティ製品のインストールパッケージを作成するには：

1. メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動します。
2. ［**追加**］をクリックします。
3. 開いた新規パッケージウィザードページで、［**カスペルスキーのデータベースからアプリケーションを選択してインストールパッケージを作成する**］をオンにして、［**次へ**］をクリックします。
4. 開いたアプリケーションのリストで、関連するアプリケーションを選択し、［**次へ**］をクリックします。
5. ドロップダウンリストから関連するローカリゼーション言語を選択し、［**次へ**］をクリックします。

このステップは、アプリケーションに複数の言語オプションが用意されている場合にのみ表示されます。

6. インストールについて使用許諾契約書に同意するよう求められたら、開いた［**使用許諾契約書**］ページで、リンクをクリックして製造元の Web サイトで使用許諾契約書を読み、［**この使用許諾契約書の内容をすべて確認し、理解した上で条項に同意します**］をオンにします。

7. 開いた［**新規インストールパッケージの名前**］ページの［**パッケージ名**］にインストールパッケージの名前を入力し、［**次へ**］をクリックします。

新しく作成されたインストールパッケージが管理サーバーにアップロードされるまで待ちます。パッケージの作成プロセスが成功したことを通知するメッセージが新規パッケージウィザードに表示されたら、［**終了**］をクリックします。

新しく作成されたインストールパッケージがインストールパッケージのリストに表示されます。このパッケージは、*アプリケーションのリモートインストール*タスクを作成または再設定する際に選択できます。

定義データベースからのサードパーティ製品のインストールパッケージの設定に関する表示と変更

以前に定義データベースに一覧表示されているサードパーティ製品のインストールパッケージを作成している場合は、後でこれらのパッケージの設定を表示および変更できます。

定義データベースから作成されたサードパーティ製品のインストールパッケージの設定を変更することは、脆弱性とパッチ管理ライセンスの下でのみ行うことができます。

定義データベースからサードパーティ製品のインストールパッケージの設定を表示および変更するには：

1. メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動します。

2. 表示されたインストールパッケージのリストで、関連するパッケージの名前をクリックします。

3. 開いたプロパティページで、必要に応じて設定を変更します。

4. ［**保存**］をクリックします。

変更した設定が保存されます。

定義データベースからのサードパーティ製品のインストールパッケージの設定

サードパーティ製品のインストールパッケージの設定は、次のタブにグループ化されています：

既定で表示されるのは以下の一覧に表示されている設定の一部のみであるため、［**フィルター**］をクリックしてリストから関連する列名を選択することで、対応する列を追加できます。

- ［**全般**］タブ：
  - 手動で編集できるインストールパッケージの名前を含む入力フィールド
  - **アプリケーション**

    インストールパッケージが作成されるサードパーティ製品の名前。
  - **バージョン**

    インストールパッケージが作成されるサードパーティ製品のバージョン番号。
  - **サイズ**

    サードパーティのインストールパッケージのサイズ（キロバイト単位）。
  - **作成日時**

    サードパーティのインストールパッケージが作成された日時。
  - **パス**

    サードパーティのインストールパッケージが保存されているネットワークフォルダーのパス。
- ［**インストール手続き**］タブ：
  - **必要なシステムコンポーネントをインストールする**

    このオプションをオンにすると、アップデートのインストール前にインストールが必要な一般システムコンポーネントをすべて自動的にインストールします。インストールが必要な対象としては、オペレーティングシステムのアップデートなどが考えられます。

    このオプションをオフにすると、必須コンポーネントを手動でインストールすることが必要となる場合があります。

    既定では、このオプションはオフです。
  - アップデートのプロパティを表示し、次の列を含む表：
    - **名前**

      アップデートの名前。
    - **説明**

      アップデートの説明。
    - **ソース**

      アップデート元、つまり、Microsoft または別のサードパーティ開発元のいずれによってリリースされたものであるか。

- **種別**

  アップデートの種別、つまり、対象とするのがドライバーまたはアプリケーションのいずれであるか。

- **カテゴリ**

  Microsoft のアップデート（緊急更新プログラム、定義更新プログラム、ドライバー、機能パック、セキュリティ更新プログラム、サービスパック、ツール、更新プログラムロールアップ、更新プログラム、またはアップグレード）に対して表示される Windows Server Update Services（WSUS）カテゴリ。

- **MSRC による重要度**

  Microsoft Security Response Center（MSRC）によって定義されたアップデートの重要度。

- **重要度**

  カスペルスキーによって定義されたアップデートの重要度。

- **パッチ重要度レベル**

  カスペルスキー製品を対象とする場合のパッチの重要度。

- **記事**

  アップデートについて説明するナレッジベースの記事の識別子（ID）。

- **セキュリティ情報**

  アップデートについて説明するセキュリティ情報の ID。

- **新しいバージョンのインストール未割り当て**

  アップデートのステータスが「インストール用に未割り当て」であるかどうかを表示します。

- **インストール予定**

  アップデートのステータスが「インストール予定」であるかどうかを表示します。

- **インストール中**

  アップデートのステータスが「インストール中」であるかどうかを表示します。

- **インストール済み**

  アップデートのステータスが「インストール済み」であるかどうかを表示します。

- **失敗**

アップデートのステータスが「失敗」であるかどうかを表示します。

- **再起動が必要です**

  アップデートのステータスが「再起動が必要」であるかどうかを表示します。

- **登録日**

  アップデートが登録された日時を表示します。

- **対話モードでのインストール**

  アップデートのインストール中にユーザーとの対話が必要であるかどうかを表示します。

- **取り消し**

  アップデートが取り消された日時を表示します。

- **アップデート承認の状況**

  アップデートのインストールが承認済みであるかどうかを表示します。

- **リビジョン**

  アップデートの現在のリビジョン番号を表示します。

- **アップデート ID**

  アップデートの ID を表示します。

- **アプリケーションのバージョン**

  アプリケーションのアップデート後のバージョン番号を表示します。

- **より古い**

  該当するアップデートを置換できる他のアップデートを表示します。

- **より新しい**

  このアップデートで置換できる他のアップデートを表示します。

- **使用許諾契約書の条項に同意する必要があります**

  アップデート時に使用許諾契約書（EULA）への同意が必要であるかどうかを表示します。

- **詳細 URL**

アップデートの製造元の名前を表示します。

- **アプリケーションファミリー**

  アップデートが属するアプリケーションファミリーの名前を表示します。

- **アプリケーション**

  アップデートが属するアプリケーションの名前を表示します。

- **ローカリゼーション言語**

  アップデートの言語を表示します。

- **新しいバージョンのインストール未割り当て**

  アップデートのステータスが「新しいバージョンのインストール用に未割り当て」であるかどうかを表示します。

- **必須アップデートのインストールが必要**

  アップデートのステータスが「必須コンポーネントのインストールが必要」であるかどうかを表示します。

- **ダウンロード方法**

  アップデートのダウンロード方法を表示します。

- **パッチ**

  アップデートがパッチであるかどうかを表示します。

- **未インストール**

  アップデートのステータスが「未インストール」であるかどうかを表示します。

- ［**設定**］タブには、インストール中にコマンドラインパラメータとして使用される、インストールパッケージの設定とその名前、説明、および値が表示されます。パッケージにそのような設定が用意されていない場合は、対応するメッセージが表示されます。これらの設定の値を変更できます。

- ［**変更履歴**］タブにはインストールパッケージのリビジョンが表示され、次の列が含まれます：

  - **リビジョン**ーインストールパッケージのリビジョン番号を表示します。
  - **時間**ーインストールパッケージ設定が変更された日時。
  - **ユーザー**ーインストールパッケージの設定を変更したユーザーの名前。
  - **処理**ーリビジョン内のインストールパッケージで実行された処理を一覧表示します。

- **説明**ーインストールパッケージの設定に加えられた変更に関連するリビジョンの説明。

  既定では、オブジェクトのリビジョンの説明は空になっています。リビジョンに説明を追加するには、関連するリビジョンを選択して、［**説明の編集**］をクリックします。［説明］ウィンドウで、リビジョンの説明を入力します。

アプリケーションタグ

Kaspersky Security Center と、アプリケーションレジストリからアプリケーションにタグを付けることができます。タグとは、アプリケーションに割り当てるラベルで、アプリケーションのグループ化と検索に使用できます。アプリケーションに割り当てたタグは、デバイスの抽出の条件として使用できます。

たとえば、「ブラウザー」というタグを作成し、すべてのブラウザー（Microsoft Internet Explorer、Google Chrome、Mozilla Firefox など）に割り当てるなどの使い方ができます。

アプリケーションタグの作成

アプリケーションタグを作成するには：

1. メインメニューで、［**操作** ］→［**サードパーティ製品**］→［**アプリケーションタグ**］の順に選択します。
2. ［**追加**］をクリックします。
   新規タグの入力ウィンドウが表示されます。
3. タグの名前を入力します。
4. ［**OK**］をクリックして変更内容を保存します。

アプリケーションタグのリストに新しいタグが表示されます。

アプリケーションタグの名前変更

アプリケーションタグの名前を変更するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションタグ**］の順に選択します。
2. 名前を変更するタグの横のチェックボックスをオンにし、［**編集**］をクリックします。
   タグのプロパティウィンドウが表示されます。
3. タグの名前を変更します。
4. ［**OK**］をクリックして変更内容を保存します。

アプリケーションタグのリストに更新したタグが表示されます。

アプリケーションへのタグの割り当て

アプリケーションにタグを割り当てるには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。
2. タグを割り当てるアプリケーションの名前をクリックします。
3. ［**タグ**］タブを選択します。

   タブには管理サーバー上のすべてのアプリケーションタグが表示されます。選択したアプリケーションに割り当てられているタグでは、［**タグの割り当て**］列のチェックボックスがオンになっています。
4. 新たに割り当てるタグの［**タグの割り当て**］列のチェックボックスをオンにします。
5. ［**保存**］をクリックして変更内容を保存します。

アプリケーションにタグが割り当てられます。

アプリケーションに割り当てたタグの削除

アプリケーションからタグを削除するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。
2. タグを削除するアプリケーションの名前をクリックします。
3. ［**タグ**］タブを選択します。

   タブには管理サーバー上のすべてのアプリケーションタグが表示されます。選択したアプリケーションに割り当てられているタグでは、［**タグの割り当て**］列のチェックボックスがオンになっています。
4. 削除するタグの［**タグの割り当て**］列のチェックボックスをオフにします。
5. ［**保存**］をクリックして変更内容を保存します。

アプリケーションからタグが解除されます。

解除されたアプリケーションタグ自身は削除されません。必要に応じて、手動で削除できます。

アプリケーションタグの削除

アプリケーションタグを削除するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションタグ**］の順に選択します。

2. リストから削除するアプリケーションタグを選択します。

3. ［**削除**］をクリックします。

4. 表示されたウィンドウで［**OK**］をクリックします。

アプリケーションタグが削除されます。削除されたタグが割り当てられていたすべてのアプリケーションから、このタグが自動的に削除されます。

監視とレポート

このセクションでは Kaspersky Security Center の監視機能とレポート機能について説明しています。これらの機能を使用して、インフラストラクチャの状況、保護ステータス、統計情報を確認できます。

Kaspersky Security Center の導入後または運用中に、必要に応じて監視とレポート機能の設定を最適な状態に編集できます。

シナリオ：監視とレポート

このセクションでは、Kaspersky Security Center の監視機能とレポート機能を設定する手順を説明しています。

必須条件

組織のネットワークへの Kaspersky Security Center の導入後、監視を開始し、動作状況のレポートを生成できます。

組織のネットワークにおける監視の実施とレポートの利用は、以下の手順で進みます：

1. **デバイスのステータスの切り替えの設定**

   特定の条件に応じたデバイスのステータスの設定方法を確認します。各種設定を変更することで、重要度レベルが「*緊急*」または「*警告*」のイベントの数を変えることができます。デバイスのステータスの切り替えを設定する時には、次の点に注意してください：

   - 新しい設定が組織の情報セキュリティポリシーと矛盾しない。
   - 組織のネットワークにおける重要なセキュリティイベントに迅速に対応できる。

2. **クライアントデバイスで発生したイベントに関する通知の設定**

   実行手順の説明：

   クライアントのデバイス上でイベントの通知（メール、SMS、ファイルの実行）を設定します。

3. **ウイルスアウトブレイクイベントについてのセキュリティネットワーク対応の変更**

   対象となるしきい値は管理サーバーのプロパティで変更できます。このイベントが発生した時に有効になるより基準の厳しいポリシーを作成したり、イベント発生時に実行されるタスクを作成できます。

4. **緊急および警告の通知について推奨される処理の実行**

実行手順の説明：

組織のネットワークに応じて、推奨される処理を実行する

5. **組織のネットワークのセキュリティステータスの確認**

   実行手順の説明：

   - ［保護ステータス］ウィジェットを確認する
   - ［保護ステータスレポート］を生成し確認する
   - ［エラーに関するレポート］を生成し確認する

6. **保護されていないクライアントデバイスの検出**

   実行手順の説明：

   - ［新しいデバイス］ウィジェットを確認する
   - ［製品導入レポート］を生成し確認する

7. **クライアントデバイスの保護状態の確認**

   実行手順の説明：

   - ［保護ステータス］および［脅威の統計］カテゴリからレポートを生成して確認する
   - ［緊急］についてのイベント抽出を開始して確認する

8. **データベースでのイベント情報による負荷の評価と制限**

   管理対象アプリケーションの動作中に発生したイベントに関する情報は、クライアントデバイスから送信され、管理サーバーデータベースに記録されます。管理サーバーの負荷を軽減するには、データベースに保管される可能性のあるイベント数の最大値を評価し、上限を設定します。

   実行手順の説明：

   - データベースの容量の計算
   - イベント数の上限の設定

9. **ライセンス情報の確認**

   実行手順の説明：

   - ［ライセンス使用状況］ウィジェットをダッシュボードに追加して確認をする
   - ［ライセンス使用レポート］を生成し確認する

結果

これらの手順が完了すると、組織のネットワークの保護に関する情報を確認できるようになり、今後のセキュリティ対策の計画や脅威への対応に役立てることができます。

監視機能とレポート機能の種別の概要

組織ネットワーク内のセキュリティ関連のイベントに関する情報は管理サーバーデータベースに保存されます。イベントの情報に基づいて、Kaspersky Security Center Web コンソールでは、組織ネットワークを対象とした次の種別の監視機能とレポート機能を使用できます。

- ダッシュボード
- レポート
- イベントの抽出
- 通知

ダッシュボード

ダッシュボードでは、組織ネットワーク内でのセキュリティトレンドをグラフや表などを通して視覚的に把握し、監視できます。

レポート

レポート機能を使用することで、組織ネットワークのセキュリティに関する詳細な数値データを取得し、これらの情報をファイルに保存したり、メールで送信したり、印刷することができます。

イベントの抽出

イベントの抽出は、管理サーバーのデータベース内に保存されているイベントを一定の条件を指定して抽出し、画面上に表示できる機能です。これらのイベントは、次のカテゴリに従ってグループ化されます：

- 重要度：**緊急イベント**、**機能エラー**、**警告**、**情報イベント**
- 発生時期：**最近のイベント**
- 種別：**ユーザー要求**、**監査イベント**

また、Kaspersky Security Center Web コンソールで編集可能な設定を使用して、ユーザー定義のイベントの抽出を作成し表示できます。

通知

通知機能を使用してイベントのアラート通知を受け取ることで、推奨される処理や担当者が適切と考える対応を行うまでの時間を短縮できます。

ダッシュボードとウィジェット

このセクションでは、ダッシュボードとダッシュボードで利用できるウィジェットについて説明します。このセクションでは、ウィジェットを管理する方法と、ウィジェットの設定について説明します。

ダッシュボードの使用

ダッシュボードでは、組織ネットワーク内でのセキュリティトレンドをグラフや表などを通して視覚的に把握し、監視できます。

Kaspersky Security Center Web コンソールの［**監視とレポート**］セクションで、［**ダッシュボード**］をクリックすると、ダッシュボードが表示されます。

ダッシュボードでは、カスタマイズ可能なウィジェットを利用できます。円グラフや表、棒グラフ、リストなどの各種形式で表示できる様々なウィジェットを選択できます。ウィジェットに表示される情報は自動的に更新されます。更新には1～2分かかります。更新の間隔はウィジェットごとに異なります。設定メニューを使用して、任意のタイミングで手動でウィジェットを更新できます。

既定では、ウィジェットには管理サーバーのデータベースに保存されているイベントの情報が含まれています。

Kaspersky Security Center Web コンソールには、次のカテゴリのウィジェットが既定のウィジェットのセットとして指定されています：

- **保護ステータス**
- **製品の導入**
- **アップデート**
- **脅威の統計**
- **その他**

一部のウィジェットのテキスト情報にはリンクが含まれている場合があります。リンクをクリックすると詳細情報を確認できます。

ダッシュボードの設定では、必要に応じて、ウィジェットの追加、非表示への変更、サイズや表示の変更、移動、設定の変更を行うことができます。

ダッシュボードへのウィジェットの追加

ダッシュボードにウィジェットを追加するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. ［**Web ウィジェットを追加または復元**］をクリックします。
3. 使用可能なウィジェットのリストから、ダッシュボードに追加するウィジェットを選択します。

   ウィジェットはカテゴリ別にグループ化されています。カテゴリに含まれるウィジェットのリストを表示するには、カテゴリ名の横にあるアイコン（▸）をクリックします。
4. ［**追加**］をクリックします。

   選択したウィジェットがダッシュボードの一番下に追加されます。

   追加したウィジェットの表示と設定を変更できます。

ダッシュボードでウィジェットを非表示にする操作

ダッシュボードで表示中のウィジェットを非表示にするには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 非表示にするウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. ［**Web ウィジェットを非表示にする**］を選択します。
4. ［**警告**］ウィンドウが表示されたら、［**OK**］をクリックします。

選択したウィジェットが表示されなくなります。いつでも、このウィジェットをもう一度ダッシュボードに追加できます。

ダッシュボードでのウィジェットの移動

ダッシュボードでウィジェットを移動するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 移動するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. ［**移動**］を選択します。
4. ウィジェットを移動する場所をクリックします。選択できるのは別のウィジェットの表示位置のみです。

選択したウィジェットの表示位置が入れ替わります。

ウィジェットのサイズと表示形式の変更

グラフを表示するウィジェットでは、グラフの形式（棒グラフまたは折れ線グラフ）を変更できます。一部のウィジェットではウィジェットのサイズを「コンパクト」「中サイズ」「最大」に変更できます。

ウィジェットの表示形式を変更するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 編集するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. 次のいずれかの手順を実行します：
   - ウィジェットを棒グラフとして表示するには、［**グラフの種別：棒**］をオンにします。
   - ウィジェットを折れ線グラフとして表示するには、［**グラフの種別：折れ線**］をオンにします。
   - ウィジェットの表示領域を変更するには、次の値のうちの1つを選択してください：

- **コンパクト**
- **コンパクト（棒グラフのみ）**
- **中サイズ（円グラフ）**
- **中サイズ（棒グラフ）**
- **最大**

選択したウィジェットの表示形式が変更されます。

ウィジェットの設定の変更

ウィジェットの設定を変更するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 変更するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. ［**設定を表示する**］を選択します。
4. ウィジェットの設定ウィンドウが表示されるので、必要に応じてウィジェットの設定を変更します。
5. ［**保存**］をクリックして変更内容を保存します。

選択したウィジェットの設定が変更されます。

どのような設定項目が存在するかは、ウィジェットごとに異なります。一般的な設定項目としてはたとえば次のような設定があります：

- **Web ウィジェットの範囲**（管理グループやデバイスの抽出など、ウィジェットが情報を表示する対象オブジェクトの範囲）。
- **タスクの選択**（ウィジェットが情報を表示する対象タスクの範囲）。
- **時間**（［開始日から終了日まで］、［開始日から現在まで］、［今日から指定した日数だけ過去にさかのぼった範囲を対象］のいずれかの形式で指定できる、ウィジェットが情報を表示する対象期間）。
- **ステータスを「緊急」にする条件**および**ステータスを「警告」にする条件**（ステータス信号の色を決定するルール）。

ウィジェットの設定を変更した後、ウィジェット上のデータを手動で更新できます。

ウィジェットのデータを更新するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 移動するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. ［**更新**］を選択します。

ウィジェットのデータが更新されました。

ダッシュボードのみモードについて

幹部社員など、ネットワークを管理してはいないが、Kaspersky Security Center でネットワークの保護ステータスを表示する必要がある社員に対して［ダッシュボードのみモード］を設定することができます。ユーザーがこのモードを有効にすると、事前設定されたウィジェットのあるダッシュボードのみが表示されます。このように、すべての管理対象デバイスの保護ステータスや、最近検知された脅威数、またはネットワーク内で頻繁に検知される脅威など、ウィジェットで指定された統計情報を管理できます。

ユーザーがダッシュボードのみモードで作業する場合、次の制限事項が適用されます：

- ユーザーにはメインメニューは表示されません。そのためネットワーク保護の設定などを変更することはできません。
- ユーザーはウィジェットに対して表示もしくは非表示にするなどの操作を行うことはできません。そのため、オブジェクトの計算ルールや時間間隔の指定など、ユーザーに必要なすべてのウィジェットをダッシュボードに表示できるように設定する必要があります。

自分自身にダッシュボードのみモードを割り当てることはできません。このモードで作業したい時は、システム管理者、マネージドサービスプロバイダー（MSP）、または［**一般的な機能：ユーザー権限**］機能領域の**オブジェクト ACL の変更**権限を持つユーザーに問い合わせてください。

ダッシュボードのみモードの設定

ダッシュボードのみモードの設定を始める前に、次の要件を満たしていることを確認してください：

- ［**一般的な機能：ユーザー権限**］機能領域の**オブジェクト ACL の変更**権限を持っている。この権限を持っていない場合、モードの設定用タブは表示されません。
- ［**一般的な機能:：基本機能**］の機能領域の**読み取り**権限を持っている。

ネットワークで管理サーバーの階層が配置されている場合、ダッシュボードのみモードを設定するには［**ユーザーとロール**］→［**ユーザーとグループ**］セクションの［**ユーザー**］タブでユーザーアカウントが使用できるサーバーに移動します。プライマリサーバーまたは物理セカンダリサーバーを選択できます。仮想サーバーでモードを調整することはできません。

ダッシュボードのみモードを設定するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. ダッシュボードのウィジェットを調整するユーザーアカウント名をクリックします。
3. アカウント設定ウィンドウが表示されたら、［**ダッシュボード**］を選択します。
   表示されたタブに、ユーザーに表示されるものと同じダッシュボードが表示されます。
4. ［**ダッシュボードのみモードでコンソールを表示**］オプションがオンになっている場合は切り替えスイッチをオフにします。

このオプションがオンになっていると、自身もダッシュボードを変更することができません。このオプションをオフにした後、ウィジェットを管理できるようになります。

5. ダッシュボードの表示を設定します。カスタマイズ可能なアカウントを持つユーザー向けに、［**ダッシュボード**］タブで事前設定されたウィジェットのセットが使用可能です。ユーザーはウィジェットのサイズや設定を変更したり、ダッシュボードからウィジェットを追加したり削除したりすることはできません。そのため、ユーザーに対してネットワーク保護の統計が表示されるようにウィジェットを調整します。［**監視とレポート**］→［**ダッシュボード**］セクションで行うのと同様の操作を［**ダッシュボード**］タブで実行します：

   - ダッシュボードに新しいウィジェットを追加します。
   - ユーザーに必要ないウィジェットを非表示にします。
   - 必要な順番にウィジェットを移動します。
   - ウィジェットの表示方法やサイズを変更します。
   - ウィジェットの設定を変更します。

6. ［**ダッシュボードのみモードでコンソールを表示**］オプションの切り替えスイッチをオンにします。

   その後、ユーザーはダッシュボードのみを使用できるようになります。ユーザーは統計情報を監視できますが、ネットワーク保護の設定やダッシュボードの表示を変更することはできません。ユーザーとお客様ご自身にも同じダッシュボードが表示され、お客様もダッシュボードを変更することはできません。

   このオプションをオフにしておくと、ユーザーにはメインメニューが表示され、ユーザーは Kaspersky Security Center でセキュリティ設定やウィジェットの変更を含む、様々な操作を実行することができます。

7. ダッシュボードのみモードの設定を完了したら、［**保存**］をクリックします。この後、準備したダッシュボードがユーザーに表示されます。

8. ユーザーが、サポートされるカスペルスキー製品の統計を表示するアクセス権を必要とする場合は、ユーザーの権限を設定します。設定すると、カスペルスキー製品のデータがユーザーのこれらのアプリケーションのウィジェットに表示されるようになります。

ユーザーはカスタマイズされたアカウントで Kaspersky Security Center にログインし、ダッシュボードのみモードでネットワーク保護の統計を監視できるようになりました。

レポート

このセクションでは、レポートの使用、カスタムレポートテンプレートの管理、レポートテンプレートを使用した新規レポートの作成、レポートの配信タスクの作成について説明します。

レポートの使用

レポート機能を使用することで、組織ネットワークのセキュリティに関する詳細な数値データを取得し、これらの情報をファイルに保存したり、メールで送信したり、印刷することができます。

Kaspersky Security Center Web コンソールの［**監視とレポート**］セクションで、［**レポート**］をクリックすると、レポートが表示されます。

既定では、レポートには過去 30 日の情報が含まれます。

Kaspersky Security Center には、次のカテゴリのレポートが既定のレポートのセットとして指定されています：

- **保護ステータス**
- **製品の導入**
- **アップデート**
- **脅威の統計**
- **その他**

カスタムレポートテンプレートの作成、レポートテンプレートの編集、レポートテンプレートの削除を行うことができます。

既存のテンプレートに基づくレポートの作成、ファイルへのレポートのエクスポート、レポートの配信タスクの作成を行うことができます。

レポートテンプレートの作成

レポートテンプレートを作成するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. ［**追加**］をクリックします。
   新規レポートテンプレートウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. レポート名を入力し、レポートの種類を選択します。
4. ウィザードの［**範囲**］ステップで、このレポートテンプレートに基づいたレポートでデータの表示対象にするクライアントデバイス（管理グループ、デバイスの抽出、指定したデバイス、ネットワーク内のすべてのデバイス）を指定します。
5. ウィザードの［**レポート期間**］ステップで、レポートの対象期間を指定します。次の値を設定できます：
   - 指定した 2 つの日付の間の期間
   - 指定日からレポート作成日までの期間
   - レポート作成日から指定した日数だけ過去にさかのぼった期間

   一部のレポートではこのページが表示されない場合もあります。
6. ［**OK**］をクリックしてウィザードを終了します。
7. 次のいずれかの手順を実行します：
   - ［**保存して実行**］をクリックすると、新しいレポートテンプレートを保存して、テンプレートに基づくレポートを実行できます。
     レポートテンプレートが保存されます。レポートが生成されます。

- ［**保存**］をクリックすると、新しいレポートテンプレートを保存できます。
  レポートテンプレートが保存されます。

新しいテンプレートを使用して、レポートの作成と表示ができます。

レポートテンプレートのプロパティの表示と編集

レポートテンプレートについて、レポートテンプレートの名前やレポートに表示されるフィールドなどの基本的なプロパティを表示し、編集できます。

レポートテンプレートのプロパティを表示したり編集するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. プロパティの表示と編集を行うレポートテンプレートに隣接するチェックボックスを選択します。
   あるいは、まずレポートを生成して、次に［**編集**］をクリックします。
3. ［**レポートテンプレートのプロパティを開く**］をクリックします。
   ［**レポート「<レポート名>」の編集**］ウィンドウの［**全般**］タブが表示されます。
4. レポートテンプレートのプロパティを編集します。
   - ［**全般**］タブ：
     - レポートテンプレート名
     - **表示する項目数の上限**

       このオプションをオンにすると、詳細なレポートデータの表に表示されるエントリ数に、指定した上限値が設定されます。

       レポートのエントリは、レポートテンプレートの［**フィールド**］→［**詳細フィールド**］セクションで指定したルールに従って並べ替えられ、合致するエントリのうち表示順が上のエントリだけが維持されます。詳細レポートのタイトルには、レポートテンプレートで設定したその他の条件に合致するエントリの合計数と表示されている数が表示されます。

       このオプションをオフにすると、詳細なレポートデータの表にはすべての使用可能なエントリが表示されますこのオプションをオフにすることは推奨されません。表示されるレポートエントリの数を制限することにより、DBMS（データベース管理システム）の負荷を減らし、レポートの生成とエクスポートの所要時間を削減できます。一部のレポートではエントリ数が多すぎる場合があります。このような場合、すべてのエントリに目を通し分析することは困難です。また、こうしたレポートの生成中にデバイスのメモリ不足が発生し、レポート自体を表示できない可能性もあります。

       既定では、このオプションはオンです。既定値は 1000 です。

     - **グループ**

       レポートの作成対象にするクライアントデバイスを変更するには、［**設定**］をクリックします。一部のレポートの種別では、このボタンを使用できない場合があります。実際の設定は、レポートテンプレートの作成時に指定した設定によって異なります。

     - **時間**

       レポートの対象期間を変更するには、［**設定**］をクリックします。一部のレポートの種別では、このボタンを使用できない場合があります。次の値を設定できます：

- 指定した 2 つの日付の間の期間
- 指定日からレポート作成日までの期間
- レポート作成日から指定した日数だけ過去にさかのぼった期間

- **セカンダリまたは仮想管理サーバーのデータを含める**

  このオプションをオンにすると、レポートテンプレートを作成する管理サーバーに属するセカンダリ管理サーバーおよび仮想管理サーバーからの情報をレポートに含めます。

  現在の管理サーバーのデータのみを表示する場合は、このオプションをオフにします。

  既定では、このオプションはオンです。

- **ネスト数の上限**

  対象の管理サーバーに属するセカンダリ管理サーバーおよび仮想管理サーバーのうち、指定したネスト数以内のサーバーのデータをレポートに含めます。

  既定値は 1 です。ツリー内でより下位に位置するセカンダリ管理サーバーの情報を取得する必要がある場合、この値を変更することができます。

- **データの待機時間（分）**

  レポートを生成する前に、レポートテンプレートを作成する管理サーバーは、セカンダリ管理サーバーからデータが送信されるのを、指定した分数だけ待機します。指定した時間が経過してもセカンダリ管理サーバーからデータを取得できなかった場合は、これらのデータを除外してレポートが実行されます。［**セカンダリ管理サーバーのデータをキャッシュする**］を有効にすると、実際のデータの代わりにキャッシュデータがレポートに表示されます。無効にすると、［**該当なし**］と表示されます。

  既定値は 5 分です。

- **セカンダリ管理サーバーのデータをキャッシュする**

  セカンダリ管理サーバーからレポートテンプレートを作成する管理サーバーに定期的にデータが送信されます。送信されたデータはキャッシュに保存されます。

  レポートの生成時に現在の管理サーバーがセカンダリ管理サーバーからデータを取得できなかった場合、キャッシュから取得したデータがレポートに表示されます。データがキャッシュに送信された日付も合わせて表示されます。

  このオプションをオンにすると、最新のデータを取得できなかった場合でもセカンダリ管理サーバーの情報を表示できます。ただし、表示されるデータが最新のものではない場合があります。

  既定では、このオプションはオフです。

- **キャッシュの更新頻度（時間）**

  セカンダリ管理サーバーからレポートテンプレートを作成する管理サーバーに定期的にデータが送信されます。この期間は時間単位で指定できます。0 時間を指定すると、レポートの生成時にのみデータが送信されます。

  既定値は 0 です。

- **セカンダリ管理サーバーから詳細情報を転送する**

生成されたレポートの詳細なレポートデータの表に、レポートテンプレートを作成する管理サーバーのセカンダリ管理サーバーから取得したデータを含めます。

このオプションをオンにすると、レポートの生成にかかる時間が長くなり、管理サーバー間のトラフィックも増大します。ただし、1つのレポートですべてのデータを表示できるメリットもあります。

このオプションをオンにする他に、先に詳細なレポートデータを分析してエラーが発生しているセカンダリ管理サーバーを特定した上で、エラーが発生している管理サーバーのみを対象にレポートを生成するという方法も活用できます。

既定では、このオプションはオフです。

- ［**フィールド**］タブ

  レポートで表示されるフィールドを選択し、［**上へ**］と［**下へ**］を使用して、フィールドの順序を変更します。［**追加**］または［**編集**］をクリックすると、該当するフィールドに基づいて情報の並べ替えとフィルター処理を行えるかどうかを設定できます。

  ［**詳細フィールドのフィルター**］で、［**フィルターの変換**］をクリックすることでも拡張フィルタリング形式の使用を開始できます。この形式は、論理演算子「OR」を使用することで様々なフィールドに指定された条件を結合できます。ボタンをクリックした後、［**フィルターの変換**］パネルが右側に開きます。［**フィルターの変換**］をクリックして変換を確定します。［**詳細フィールド**］セクションで論理演算子「OR」を使用することで適用される条件付きの変換されたフィルターを定義できるようになります。

  複雑なフィルタリング条件をサポートする形式にレポートを変換すると、以前の Kaspersky Security Center (11 より前のバージョン) でレポートを使用できなくなることがあります。また、このような互換性のないバージョンの製品を実行しているセカンダリの管理サーバーからのデータは、変換されたレポートに含めることができません。

5. ［**保存**］をクリックして変更内容を保存します。
6. ［**レポート <レポート名> の編集**］ウィンドウを閉じます。

レポートテンプレートのリストに更新したレポートテンプレートが表示されます。

レポートのファイルへのエクスポート

レポートを、XML ファイル、HTML ファイル、または PDF ファイルにエクスポートできます。

レポートをファイルにエクスポートするには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. ファイルにエクスポートするレポートに隣接するチェックボックスをオンにします。
3. ［**レポートのエクスポート**］をクリックします。
4. 表示されるウィンドウの［**名前**］でレポートファイル名を変更できます。既定では、ファイル名は選択したレポートテンプレートの名前に一致します。
5. レポートのファイル種別（XML、HTML、PDF）を選択します。
6. ［**レポートのエクスポート**］をクリックします。

選択した形式のレポートがデバイス（の既定のフォルダー）にダウンロードされるか、あるいはブラウザー標準の「**名前を付けて保存**」ウィンドウが開いてファイルの保存先を指定できます。

レポートがファイルに保存されます。

レポートの生成と表示

レポートを作成および表示するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. レポートの作成に使用するレポートテンプレートの名前をクリックします。

   選択したテンプレートを使用してレポートが作成され、表示されます。

> レポートデータは、管理サーバーのローカリゼーションセットに従って表示されます。

レポートには次のデータが表示されます：

- ［**サマリー**］タブ：
  - レポート名とレポート種別、概要説明、レポート期間、レポートが作成されたデバイスグループに関する情報。
  - 代表的なレポートのデータを示している図表。
  - 計算されたレポートの指標を含む表。
- **[詳細]**タブで、詳細レポートデータの表が表示されます。

レポート配信タスクの作成

選択したレポートを配信するタスクを作成できます。

レポート配信タスクを作成するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. レポート配信タスクを作成するレポートテンプレートの横にあるチェックボックスをオンにします。
3. ［**配信タスクを作成**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
4. ウィザードの**新規タスク設定**ステップで、タスク名を入力します。
   既定名は［**レポートの配信**］です。この名前のタスクが既に存在する場合は、タスク名にシーケンス番号（<N>）が追加されます。
5. ウィザードの**レポート設定**ステップで、次の設定を指定します：

a. タスクでレポートを配信するレポートテンプレート。

b. レポート形式（HTML、XLS、PDF）。

wkhtmltopdf ツールはレポートを PDF に変換するために必要です。PDF を選択すると、管理サーバーはデバイスに wkhtmltopdf ツールがインストールされているかどうか確認します。ツールがインストールされていない場合は、管理サーバーデバイスにツールをインストールする必要があることに関するメッセージが表示されます。手動でツールをインストールして次の手順に進みます。

c. レポートをメールで送信するかどうかと、送信する場合のメール通知設定。

最大 20 個のメールアドレスを指定できます。メールアドレスを区切るには、**Enter** キーを押します。カンマで区切られたメールアドレスのリストを貼り付けて、**Enter** キーを押すこともできます。

d. レポートをフォルダーに保存するかどうかと、保存する場合に同じフォルダーにある以前のレポートを上書きするかどうか、および（共有フォルダーの場合に）フォルダーへのアクセスに特定のアカウントを使用するかどうか。

6. ウィザードの**タスクスケジュールの設定**ステップで、タスクの開始スケジュールを選択します。

以下のタスクスケジュールオプションが使用可能です：

- **手動**

  タスクは、自動的には実行されません。手動でのみ開始できます。

  既定では、このオプションがオンです。

- **N 分ごと**

  タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

  既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

- **N 時間ごと**

  指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

  既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

- **N 日ごと**

  日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

  既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

- **N 週間ごと**

  指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

  既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

- **毎月**

毎月、指定した日付の指定した時刻にタスクを定期的に実行します。
指定した日付が存在しない月には、月の最終日にタスクを実行します。
既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **指定した日**

毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。
規定では、日付は選択されていません。規定の開始時間は18:00 です。

- **ウイルスアウトブレイク検知次第**

［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

- ワークステーションとファイルサーバー向けアンチウイルス製品
- 境界防御向けアンチウイルス製品
- メールサーバー向けアンチウイルス製品

既定では、すべてのアプリケーション種別がオンです。

ウイルスアウトブレイクを検知したセキュリティ製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。このオプションは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。たとえば、［**デバイスの電源をオンにする**］をオンにして*管理対象デバイスの管理*タスクを実行し、その完了後にトリガータスクとして *ウイルススキャン*タスクを実行できます。

テーブルからトリガータスクと、このタスクを完了する必要があるステータス（［**正常終了**］または［**失敗**］）を選択する必要があります。

必要に応じて、次のようにテーブル内のタスクを検索、並べ替え、フィルタリングできます。

- タスク名で検索するには、検索フィールドにタスク名を入力します。
- 並べ替えアイコンをクリックすると、タスクが名前順に並べ替えられます。
  既定では、タスクはアルファベットの昇順で並べ替えられます。
- フィルターアイコンをクリックし、開いたウィンドウでタスクをグループ別にフィルターし、［**適用**］をクリックします。

7. ウィザードのこのステップでは、その他のタスクスケジュール設定を指定します：

- ［**タスクのスケジュール**］セクションで、以前に選択したスケジュールをチェックまたは再設定し、時間間隔、日付または曜日を設定し、ウイルスアウトブレイク条件を設定するか、タスクを開始するトリガーとして別のタスクを完了します。該当するスケジュールを選択した場合は、このセクションで開始時間を指定することもできます。
- ［**追加設定**］セクションで、次の設定を指定します：

- **未実行のタスクを実行する**

  このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

  このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

  このオプションをオフにすると、スケジュールされたタスクのみクライアントデバイスで実行されます。**手動**、**1回**、**即時**のスケジュールの場合、タスクはネットワーク上で表示可能なクライアントデバイスでのみ実行されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

  既定では、このオプションはオフです。

- **タスクの開始を自動的かつランダムに遅延させる**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内で自動的かつランダムに遅延させる（分）**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  既定では、このオプションはオフです。既定の時間は1分です。

- **次の時間を超える場合はタスクを停止する**

  指定した時間が経過すると、タスクが完了したかどうかに関係なくタスクが自動的に停止します。

  実行に時間がかかり過ぎているタスクを中断したい時に、このオプションを使用します。

  既定では、このオプションはオフです。既定のタスク実行時間は120分です。

8. ウィザードの**タスクを実行するアカウントの選択**ステップで、タスクの実行に使用するユーザーアカウントの資格情報を指定します。

9. タスク作成後に他のタスク設定を変更したい場合は、ウィザードの**タスク作成の終了**ステップで、［**タスクの作成が完了したらタスクの詳細を表示する**］オプションをオンにします（既定でオンになっています）。

10. タスクを作成しウィザードを終了するには、［**終了**］をクリックします。

    レポート配信タスクが作成されます。［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスク設定ウィンドウが表示されます。

レポートテンプレートの削除

レポートのテンプレートを削除するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］の順に選択します。
2. 削除するレポートテンプレートの隣にあるチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで、［**OK**］をクリックして処理を確定します。

選択したレポートテンプレートが削除されます。これらのレポートテンプレートがレポートの配信タスクに含まれていた場合、タスクからも該当するレポートテンプレートが削除されます。

イベントとイベントの抽出

このセクションでは、イベントとイベントの抽出、Kaspersky Security Center コンポーネントで発生するイベントの種別、頻出イベントのブロック管理について説明します。

Kaspersky Security Center のイベントについて

Kaspersky Security Center では、管理サーバーと管理対象デバイスにインストールされた他のカスペルスキー製品の動作中に発生したイベントの情報を受信できます。イベントに関する情報は管理サーバーデータベースに保存されます。

イベント種別

Kaspersky Security Center には、次のイベント種別があります：

- 一般イベント：管理対象となるカスペルスキー製品すべてで共通して発生するイベントです。一般イベントの例としては「ウイルスアウトブレイク」があります。一般イベントでは、構文と形式が厳密に定義されています。一般イベントは、レポートやダッシュボードなどで使用されます。
- 管理対象のカスペルスキー製品それぞれに固有のイベント：管理対象となるカスペルスキーの各製品には、独自のイベントのセットがあります。

イベントソース

イベントは、次の製品で生成される可能性があります：

- Kaspersky Security Center のコンポーネント：
  - 管理サーバー
  - ネットワークエージェント
  - iOS MDM サーバー
  - Exchange モバイルデバイスサーバー
- 管理対象のカスペルスキー製品

  管理対象のカスペルスキー製品によって生成されるイベントの詳細は、該当する製品のドキュメントを参照してください。

製品によって生成されるイベントの完全なリストは、アプリケーションポリシーの［**イベントの設定**］タブで確認できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示できます。

イベントの重要度

各イベントには固有の重要度があります。発生した状況に応じて、イベントには様々な重要度が割り当てることができます。イベントの重要度には次の 4 つがあります：

- *緊急イベント*は、データの損失、誤動作、または重大なエラーを招きかねない重大な問題が発生したことを示すイベントです。
- *機能エラー*は、アプリケーションの動作中または手順の実行中に重大な問題、エラー、または誤動作の発生を示すイベントです。
- *警告*は、必ずしも重大ではなくても、将来問題が発生する可能性があることを示すイベントです。こうしたイベントの発生後、データや機能を失わずにアプリケーションを復元できるのであれば、ほとんどのイベントは警告を意味します。
- *情報*イベントは、操作が適切に完了したこと、アプリケーションが適切に動作していること、手順が完了したことを伝えるために発生するイベントです。

各イベントには保管期間が定義されており、保管期間中、ユーザーは Kaspersky Security Center でイベントを表示または変更することができます。一部のイベントは既定により、管理サーバーデータベースに保管されません。保管期間がゼロと定義されているためです。管理サーバーデータベースに 1 日以上保管されるイベントだけを外部システムにエクスポートできます。

イベントの抽出の使用

イベントの抽出は、管理サーバーのデータベース内に保存されているイベントを一定の条件を指定して抽出し、画面上に表示できる機能です。これらのイベントは、次のカテゴリに従ってグループ化されます：

- 重要度：**緊急イベント**、**機能エラー**、**警告**、**情報イベント**
- 発生時期：**最近のイベント**
- 種別：**ユーザー要求**、**監査イベント**

また、Kaspersky Security Center Web コンソールで編集可能な設定を使用して、ユーザー定義のイベントの抽出を作成し表示できます。

Kaspersky Security Center Web コンソールの［**監視とレポート**］セクションで、［**イベントの抽出**］をクリックすると、イベントの抽出が表示されます。

既定では、イベントの抽出には過去 7 日の情報が含まれます。

Kaspersky Security Center には、事前定義された次の既定のイベントの抽出のセットが用意されています：

- 重要度別のイベント：
  - **緊急イベント**
  - **機能エラー**
  - **警告**
  - **情報メッセージ**
- **ユーザー要求**（管理対象製品のイベント）
- **最近のイベント**（過去 1 週間を対象）
- **監査イベント**

ユーザー定義の抽出を追加で作成し設定できます。ユーザー定義の抽出では、イベントが発生したデバイスの属性（デバイス名、IP アドレスの範囲、管理グループ）、イベントの種別と重要度、製品名とコンポーネント名、および対象期間によってイベントをフィルターできます。検索対象に、タスクの実行結果を含めることもできます。また、1 つ以上の単語を入力して検索する、シンプルな検索フィールドも使用できます。この場合、入力した単語のいずれかが、いずれかの属性（イベント名、説明、コンポーネント名など）に含まれるイベントがすべて一致対象として表示されます。

事前定義の抽出とユーザー定義の抽出の両方で、表示するイベント数と検索対象にするレコード数を制限できます。両方のオプションの値が、Kaspersky Security Center でイベントの抽出が表示されるまでの所要時間に影響します。データベースのサイズが大きいほど、プロセスの所要時間が長くなります。

次のことができます：

- イベントの抽出のプロパティの編集
- イベントの抽出の生成
- イベントの抽出の詳細の表示
- イベントの抽出の削除
- 管理サーバーのデータベースからのイベントの削除

イベントの抽出の作成

イベントの抽出を作成するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に移動します。
2. ［**追加**］をクリックします。

3. ［**新規のイベントの抽出**］ウィンドウで、新しいイベントの抽出の設定を指定します。必要に応じて、ウィンドウの各セクションでこの操作を行います。

4. ［**保存**］をクリックして変更内容を保存します。
   確認ウィンドウが開きます。

5. イベントの抽出の結果を表示するには、［**抽出の結果に移動**］をオンにしたままにします。

6. ［**保存**］を選択して、イベントの抽出の作成を確定させます。

［**抽出の結果に移動**］をオンにしたままの場合、イベントの抽出結果が表示されます。オフにした場合、新しいイベントの抽出が追加されたイベントの抽出のリストが表示されます。

イベントの抽出の編集

イベントの抽出を編集するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。

2. 編集するイベントの抽出に隣接するチェックボックスをオンにします。

3. ［**プロパティ**］をクリックします。
   イベントの抽出の設定ウィンドウが表示されます。

4. イベントの抽出のプロパティを編集します。

   > 製品導入時から利用できる定義済みのイベントの抽出では、［**全般**］タブ（抽出の名前以外）、［**時間**］タブ、［**アクセス権**］タブのプロパティのみを編集できます。

   ユーザー定義の抽出では、すべてのプロパティを編集できます。

5. ［**保存**］をクリックして変更内容を保存します。

編集したイベントの抽出がリストに表示されます。

イベントの抽出のリストの表示

イベントの抽出を表示するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。

2. 開始するイベントの抽出に隣接するチェックボックスをオンにします。

3. 次のいずれかの手順を実行します：

   - イベントの抽出結果の表示で並べ替えを設定したい場合は、次の操作を実行します：

     a. ［**並べ替えを再設定して実行**］をクリックします。

b. ［**イベントの抽出の並べ替えの再設定**］ウィンドウが表示されるので、並べ替えの設定を指定します。

c. 抽出名をクリックします。

- 管理サーバーでの並べ替え順序を変更せずにイベントのリストを表示する場合は、抽出名をクリックします。

イベントの抽出結果が表示されます。

イベントの抽出のエクスポート

Kaspersky Security Center では、イベントの抽出とその設定を KLO ファイルに保存できます。この KLO ファイルを使用して、Kaspersky Security Center Windows と Kaspersky Security Center Linux の両方に保存したイベントの抽出をインポートできます。

エクスポートできるのは、ユーザー定義のイベントの抽出のみであることに注意してください。既定の Kaspersky Security Center セットからのイベントの抽出（事前定義された抽出）は、ファイルに保存できません。

イベントの抽出をエクスポートするには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
2. エクスポートするイベントの抽出に隣接するチェックボックスをオンにします。

   複数のイベントの抽出を同時にエクスポートすることはできません。複数の抽出を選択すると、［**エクスポート**］が無効になります。
3. ［**エクスポート**］をクリックします。
4. 開いた［**名前を付けて保存**］ウィンドウで、イベントの抽出ファイル名とパスを指定し、［**保存**］をクリックします。

   ［**名前を付けて保存**］ウィンドウは、Google Chrome、Microsoft Edge、または Opera を使用している場合にのみ表示されます。別のブラウザーを使用する場合、イベントの抽出ファイルは自動的に［**Downloads**］フォルダーに保存されます。

イベントの抽出のインポート

Kaspersky Security Center では、KLO ファイルからイベントの抽出をインポートできます。KLO ファイルには、エクスポートされたイベントの抽出とその設定が含まれています。

イベントの抽出をインポートするには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
2. ［**インポート**］をクリックし、インポートするイベントの抽出ファイルを選択します。
3. 表示されたウィンドウで、KLO ファイルのパスを指定し、［**開く**］をクリックします。選択できるイベントの抽出イベントの抽出ファイルは 1 つだけです。

イベントの抽出処理が開始されます。

インポート結果の通知が表示されます。イベントの抽出が正常にインポートされた場合は、［**インポートの詳細を表示**］をクリックしてイベントの抽出のプロパティを表示できます。

インポートが成功すると、イベントの抽出が抽出リストに表示されます。イベントの抽出の設定もインポートされます。

> 新しくインポートされたイベントの抽出と同じ名前のイベントの抽出が既に存在している場合、インポートされたイベントの抽出の名前に、たとえば **(1)**、**(2)** のようなインデックス「**(<次の連番>)**」が付きます。

イベントの詳細の表示

イベントの詳細を表示するには：

1. イベントの抽出を開始します。
2. 目的のイベントの時刻をクリックします。
   ［**イベントのプロパティ**］ウィンドウが開きます。
3. 表示されたウィンドウでは、次の操作を実行できます：
   - 選択したイベントの情報の表示
   - イベントの抽出結果の1つ前または1つ後のイベントへの移動
   - イベントが発生したデバイスの情報への移動
   - イベントが発生したデバイスが属する管理グループへの移動
   - （タスクに関係しているイベントの場合）該当タスクへの移動

イベントのファイルへのエクスポート

イベントをファイルにエクスポートするには：

1. イベントの抽出を開始します。
2. 目的のイベントに隣接するチェックボックスをオンにします。
3. ［**ファイルへのエクスポート**］をクリックします。

選択したイベントがファイルにエクスポートされます。

イベントに含まれるオブジェクトの履歴の表示

リビジョン管理をサポートするオブジェクトの作成イベントまたは変更イベントからは、オブジェクトの履歴画面に移動することができます。

イベントからオブジェクトの履歴を表示するには：

1. イベントの抽出を開始します。
2. 目的のイベントに隣接するチェックボックスをオンにします。
3. ［**変更履歴**］をクリックします。

   オブジェクトの変更履歴が表示されます。

イベントの削除

イベントを削除するには：

1. イベントの抽出を開始します。
2. 目的のイベントの横にあるチェックボックスをオンにします。
3. ［**削除**］をクリックします。

   選択したイベントは削除され、このイベントは復元できません。

イベントの抽出の削除

削除できるのはユーザー定義のイベントの抽出のみです。製品組み込みで定義済みのイベントの抽出は削除できません。

イベントの抽出を削除するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
2. 削除するイベントの抽出に隣接するチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**OK**］をクリックします。

   イベントの抽出が削除されます。

イベントの保管期間の設定

Kaspersky Security Center では、管理サーバーと管理対象デバイスにインストールされた他のカスペルスキー製品の動作中に発生したイベントの情報を受信できます。イベントに関する情報は管理サーバーデータベースに保存されます。一部のイベントを既定値の期間より長くまたは短く保管することが必要な場合があります。イベントの既定の保管期間を変更できます。

管理サーバーのデータベースに保存しなくてよいイベントがある場合は、管理サーバーポリシーとカスペルスキー製品ポリシー、または管理サーバーのプロパティ（管理サーバーのイベントのみ）で適切な設定を無効にできます。これにより、データベースに保存されるイベント種別の数を減らすことができます。

イベントの保管期間が長いほど、データベースが容量の上限に達するのが早くなります。一方で、イベントの保存期間を長くすることで、監視や レポートのタスクをより長い期間実行することができます。

管理サーバーデータベースへのイベントの保管期間を指定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. 次のいずれかの手順を実行します：
   - ネットワークエージェントまたは管理対象カスペルスキー製品のイベントの保存期間を設定するには、対応するポリシーの名前をクリックします。

     ポリシーのプロパティページが表示されます。
   - 管理サーバーイベントを構成するには、メインメニューで、必要な管理サーバーの名前の横にある設定アイコン（ ）をクリックします。

     管理サーバーのポリシーがある場合は、このポリシーの名前をクリックできます。

     管理サーバーのプロパティページまたは管理サーバーポリシーのプロパティページが表示されます。
3. ［**イベントの設定**］タブを選択します。

   ［**緊急**］セクションのイベント種別のリストが表示されます。
4. ［**機能エラー**］、［**警告**］、［**情報**］のいずれかのセクションを選択します。
5. 右側のペインのイベント種別のリストで、保存期間を変更するイベントのリンクをクリックします。

   表示されるウィンドウの［**イベント登録**］セクションで、［**管理サーバーのデータベースに保存（日）**］が有効になっています。
6. このスイッチの下に、イベントを保存する日数を入力します。
7. 管理サーバーのデータベースにイベントを保存しない場合は、［**管理サーバーのデータベースに保存（日）**］を無効にします。

   管理サーバーのプロパティウィンドウで管理サーバーのイベントを設定し、Kaspersky Security Center 管理サーバーのポリシーでイベントの設定がロックされている場合、この画面でイベントの保管期間を編集することはできません。
8. ［OK］をクリックします。

   ポリシーのプロパティウィンドウが閉じます。

以降、選択した種別のイベントを管理サーバーが受け取ったイベントの保存期間は、変更した期間保存されるようになります。管理サーバーが以前受け取ったイベントの保存期間は変更されません。

Kaspersky Security Center のコンポーネントでのイベント

Kaspersky Security Center の各コンポーネントには、独自のイベント種別のセットがあります。このセクションでは、Kaspersky Security Center 管理サーバーとネットワークエージェント、iOS MDM サーバーで発生するイベントの種別について説明します。カスペルスキー製品で発生する可能性のあるイベントの種別は、このセクションの説明には含まれていません。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

イベント種別のデータ構造の説明

イベント種別ごとに、表示名、識別子（ID）、英字コード、内容の説明、既定の保管期間を記載しています。

- **イベント種別の表示名**：イベントを設定してそれが発生すると、この列のテキストが Kaspersky Security Center で表示されます。
- **イベント種別の ID**：イベント解析用のサードパーティ製品を使用してイベントを処理すると、この列の数字コードが使用されます。
- **イベント種別**（英字コード）：Kaspersky Security Center データベースで提供されるパブリックビューを使用してイベントの参照と処理を行う場合とイベントを SIEM システムにエクスポートする場合に、この列のコードが使用されます。
- **説明**：この列では、イベントが発生する状況と可能な対応が説明されています。
- **既定の保管期間**：この列には、イベントが管理サーバーデータベースに保管され、管理サーバーのイベントリストに表示される日数が記載されています。この期間が過ぎると、イベントが削除されます。イベントの保管期間の値が「0」の場合、これらのイベントについては検知のみが行われ、管理サーバーのイベントリストへの表示は行われません。こうしたイベントをオペレーティングシステムのイベントログに保存するように設定した場合、それらの保存先でイベントを確認できます。

  イベントの保存期間を変更できます：

  - 管理コンソール：イベントの保管期間の設定
  - Kaspersky Security Center Web コンソール：イベントの保管期間の設定

その他のデータには次のフィールドが含まれることがあります：

- **event_id**：自動で生成および割り当てられたデータベース内のイベントの一意な数字。**イベント種別の ID** とは異なります。
- **task_id**：イベントを発生させたタスクの識別子（該当する場合）
- **severity**：以下のセキュリティレベル（重要度の昇順）のうちの 1 つ：

  0) 無効なセキュリティレベル

  1) 情報

  2) 警告

  3) エラー

  4) 重要

管理サーバーのイベント

このセクションには、管理サーバーに関するイベントの情報が記載されています。

管理サーバーの緊急イベント

次の表は、重要度が「**緊急**」に分類される Kaspersky Security Center 管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

管理コンソールの［管理サーバーのプロパティ］ウィンドウでポートを指定した場合、**Kaspersky Security Center は、監視およびアラート用のシステムである Prometheus によって取得されるメトリクス**と緊急イベントを公開します。Prometheus はメトリクスと緊急イベントを取得し、イベントごとにアラートを生成します。

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

管理サーバーの緊急イベント

イベント種別の表示名	イベント種別の ID	イベント種別	説明	既定の保管期間
ライセンス数の上限を超えました	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	1 日に 1 回、Kaspersky Security Center はライセンス管理の上限の超過が発生していないかどうかを確認します。	180 日間

			この種別のイベントは、クライアントデバイスにインストールされているカスペルスキー製品で、ライセンスの上限の超過を管理サーバーが検出しており、単一のライセンスに紐付けられていて現在使用中のライセンス単位数がそのライセンスで本来許可されている合計ライセンス単位数の 110% を超えている場合に記録されます。 このイベントが発生した場合でも、クライアントデバイスの保護は継続されます。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストを確認します。使用されていないデバイスを削除します。 • 製品を使用できるデバイス数の上限が増えるように、ライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。 Kaspersky Security Center では、ライセンス数の上限を超過した時にイベントを生成するルールを指定できます。	
ウイルスアウトブレイク	26（ファイル脅威対策の場合）	GNRL_EV_VIRUS_OUTBREAK	この種別のイベントは、複数の管理対象デバイスで検知された悪意のあるオブジェクトの数が短期間のうちにしきい値を超えた場合に記録されます。 このイベントには、次の方法で対応できます： • 対象となるしきい値を管理サーバーのプロパティで編集します。 • このイベントの発生時に有効になるより基準の厳しいポリシーを作成したり、イベント発生時に実行されるタスクを作成します。	180 日間
ウイルスアウトブレイク	27（メール脅威対策の場合）	GNRL_EV_VIRUS_OUTBREAK	この種別のイベントは、複数の管理対象デバイスで検知された悪意のあるオブジェクトの数が短期間のうちにしきい値を超えた場合に記録されます。 このイベントには、次の方法で対応できます： • 対象となるしきい値を管理サーバーのプロパティで編集します。 • このイベントの発生時に有効になるより基準の厳しいポリシーを作成したり、イベント発生時に実行されるタスクを作成します。	180 日間
ウイルスアウトブレイク	28（ファイアウォールの場合）	GNRL_EV_VIRUS_OUTBREAK	この種別のイベントは、複数の管理対象デバイスで検知された悪意のあるオブジェクトの数が短期間のうちにしきい値を超えた場合に記録されます。 このイベントには、次の方法で対応できます： • 対象となるしきい値を管理サーバーのプロパティで編集します。 • このイベントの発生時に有効になるより基準の厳しいポリシーを作成したり、イベント発生時に実行されるタスクを作成します。	180 日間
デバイスが管理対象外になりました	4111	KLSRV_HOST_OUT_CONTROL	この種別のイベントは、デバイスはネットワーク上で可視だが管理サーバーに接続していない状態が指定期間を超えて継続すると記録されます。 デバイス上でネットワークエージェントの正常な動作を妨げている要素を特定します。原因としては、ネットワークの問題や、ネットワークエージェントがデバイスから削除された状況などが考えられます。	180 日間
デバイスのステータスが「緊急」です	4113	KLSRV_HOST_STATUS_CRITICAL	この種別のイベントは、管理対象デバイスに「*緊急*」ステータスが割り当てられると記録されます。デバイスのステータスが「*緊急*」に切り替わる条件を設定できます。	180 日間
このライセン	4124	KLSRV_LICENSE_BLACKLISTED	この種別のイベントは、使用しているアクティベーションコードまたはライセンス情報ファイルがカスペルスキーで拒否	180 日間

ス情報ファイルは拒否リストに追加されています			リストに登録されると記録されます。 詳細は、テクニカルサポートに問い合わせてください。	
機能が制限されています	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	この種別のイベントは、Kaspersky Security Center の動作モードが変更されて基本機能のみが使用可能になり、脆弱性とパッチ管理機能およびモバイルデバイス管理機能が使用できない時に記録されます。 イベントが発生する理由と対応は次の通りです： • ライセンスの有効期限が終了している：Kaspersky Security Center の全機能を使用できるモードで必要なライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。 • ライセンスの上限で指定された台数を超過して管理サーバーでデバイスを管理している：管理サーバーの管理グループから別の管理サーバーの管理グループにデバイスを移動します（移動先の管理サーバーのライセンスの上限内で）。	180 日間
ライセンスの有効期間がまもなく終了します	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	この種別のイベントは、製品版ライセンスの有効期限が近づいている時に発生します。 1 日に 1 回、Kaspersky Security Center はライセンス有効期間の終了日が近づいているかどうかを確認します。この種別のイベントは、ライセンスの有効期限まで残り 30 日、15 日、5 日および 1 日となった時に発生します。日数は変更できません。管理サーバーがライセンスの有効期限より前に指定された日にオフになった場合は翌日までイベントは発生しません。 製品版ライセンスの有効期間が終了した場合は、Kaspersky Security Center は基本機能のみを提供します。 このイベントには、次の方法で対応できます： • 予備のライセンスが管理サーバーに追加されていることを確認します。 • 定額制サービスをご利用の場合は、必ず更新してください。支払い期日までに決済された場合、無制限の定額制サービスは自動的に更新されます。	180 日間
証明書の有効期間が終了しています	4132	KLSRV_CERTIFICATE_EXPIRED	このタイプのイベントは、モバイルデバイス管理用の管理サーバー証明書の有効期間が終了すると発生します。 期限切れの証明書をアップデートする必要があります。	180 日間
カスペルスキー製品モジュールのアップデートが取り消されました	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	この種別のイベントは、カスペルスキーのテクニカルスペシャリストにより、より新しいバージョンの製品にアップデートする必要があるなどの理由でシームレスアップデートの利用が拒否された場合（アップデートのステータスとして「*取り消し*」が表示）に記録されます。このイベントは、Kaspersky Security Center のアップデートパッチを対象としており、管理対象のカスペルスキー製品モジュールとの関連はありません。イベントでは、シームレスアップデートがインストールされなかった理由に関する情報が提供されます。	180 日間
監査：SIEM へエクスポートできませんでした	5130	KLAUD_EV_SIEM_EXPORT_ERROR	このタイプのイベントは、SIEM システムとの接続エラーが原因で SIEM システムへのイベントのエクスポートが失敗した場合に発生します。	180 日間

管理サーバーの機能エラーイベント

次の表は、重要度が「**機能エラー**」に分類される Kaspersky Security Center 管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

管理サーバーの機能エラーイベント

イベント種別の表示名	イベント種別の ID	イベント種別	説明	既定の保管期間
実行時エラー	4125	KLSRV_RUNTIME_ERROR	この種別のイベントは、不明な問題が生じた時に記録されます。 ほとんどの場合、問題は DBMS の問題、ネットワークの問題、またはソフトウェアやハードウェアの問題から発生しています。 エラー情報の詳細は、イベントの説明で参照できます。	180 日間
インストール数の上限を超えたライセンス認証済みアプリケーショングループがあります	4126	KLSRV_INVLICPROD_EXCEDED	この種別のイベントは、管理サーバーによって 1 時間ごとに生成されます。この種別のイベントは、Kaspersky Security Center でサードパーティ製品を管理していて、サードパーティ製品のライセンスで設定された上限を超えると記録されます。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストを確認します。該当するサードパーティ製品が使用されていないデバイスからサードパーティ製品を削除します。 • 製品を使用できるデバイス数の上限が増えるように、サードパーティ製品のライセンスを追加します。 ライセンス認証済みアプリケーショングループ機能を使用することで、サードパーティ製品のライセンスを管理できます。ライセンス認証済みアプリケーショングループには、管理者が設定した基準を満たすサードパーティ製品が含まれます。	180 日間
クラウドセグメントのポーリングに失敗しました	4143	KLSRV_KLCLOUD_SCAN_ERROR	この種別のイベントは、管理サーバーがクラウド環境でネットワークセグメントのポーリングに失敗した時に発生します。イベントの説明に記載されている詳細情報を読み、適宜対応します。	保管されません
指定フォルダーにアップデートをコピーできませんでした	4123	KLSRV_UPD_REPL_FAIL	この種別のイベントは、ソフトウェアアップデートが指定したフォルダーでなく共有フォルダーにコピーされた場合に記録されます。 このイベントには、次の方法で対応できます： • 指定したフォルダーへのアクセスに使用されたユーザーアカウントに、書き込み権限があるかどうかを確認します。 • フォルダーにアクセスするためのユーザー名とパスワードが変更されていないかどうか確認します。 • インターネット接続がイベント発生の原因の可能性もあるので、これをチェックします。定義データベースとソフトウェアモジュールのアップデート手順に従って操作します。	180 日間
ディスクに空き容量がありません	4107	KLSRV_DISK_FULL	この種別のイベントは、管理サーバーがインストールされているデバイスのハードディスクの空き容量が不足すると発生します。 デバイスのディスク領域を解放します。	180 日間
共有フォルダーが使用できません	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	この種別のイベントは、管理サーバーの共有フォルダーが利用できない場合に記録されます。 このイベントには、次の方法で対応できます：	180 日間

			• （共有フォルダーのある）管理サーバーが起動されていて利用可能な状態であることを確認します。 • フォルダーにアクセスするためのユーザー名とパスワードが変更されていないかどうか確認します。 • ネットワーク接続の問題がないか確認します。	
管理サーバーデータベースが使用できません	4109	KLSRV_DATABASE_UNAVAILABLE	この種別のイベントは、管理サーバーのデータベースが利用できなくなっている場合に記録されます。 このイベントには、次の方法で対応できます： • SQL サーバーがインストールされているリモートサーバーが利用できる状態になっているかを確認します。 • DBMS ログを確認し、管理サーバーデータベースを使用できなくなっている理由を特定します。たとえば、メンテナンスの実施が原因となって、SQL サーバーがインストールされているリモートサーバーが利用できなくなっている可能性などがあります。	180 日間
管理サーバーデータベースに空き容量がありません	4110	KLSRV_DATABASE_FULL	この種別のイベントは、管理サーバーのデータベースに空き容量がないと記録されます。 管理サーバーのデータベースが容量の上限に達してデータベースへの情報の記録ができなくなると、管理サーバーが正常に機能しなくなります。 このイベントが発生する主な原因は使用中の DBMS の種別に応じて 2 つあり、それぞれ適切な対応方法が異なります： • SQL Server Express Edition を DBMS として使用している場合： SQL Server Express のヘルプを参照して、使用中のバージョンのデータベースサイズの上限を確認します。管理サーバーのデータベースが、このデータベースサイズの上限に達した可能性があります。 管理サーバーデータベースに保存されるイベントの数を制限してください。 管理サーバーデータベースにアプリケーションコントロールコンポーネントから送信されたイベントの数が多すぎます。これには、管理サーバーデータベースでのアプリケーションコントロールイベントの保管期間に関する Kaspersky Endpoint Security for Windows ポリシーの設定を変更することで対応できます。 • SQL Server Express Edition 以外の DBMS を使用している場合： 管理サーバーのデータベースに保存されるイベントの数を制限しないでください。 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください。 DBMS の選定に関する情報を確認します。	180 日間

管理サーバーの警告イベント

次の表は、重要度が「**警告**」に分類される Kaspersky Security Center 管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

管理サーバーの警告イベント

イベント種別の	イベン	イベント種別	説明	既定の

表示名	ト種別の ID			保管期間
頻出イベントが検出されました		KLSRV_EVENT_SPAM_EVENTS_DETECTED	このタイプのイベントは、管理サーバーが管理対象デバイスで頻出イベントを検知した時に発生します。詳細については、次のセクションを参照してください：「頻出イベントのブロック」。	90 日間
ライセンス数の上限を超えました	4098	KLSRV_EV_LICENSE_CHECK_100_110	1 日に 1 回、Kaspersky Security Center はライセンス管理の上限の超過が発生していないかどうかを確認します。 この種別のイベントは、クライアントデバイスにインストールされているカスペルスキー製品でライセンスの上限の超過が発生していることを管理サーバーが検知し、なおかつ単一のライセンスに紐付けられていて現在使用中のライセンス単位数がそのライセンスで本来許可されている合計ライセンス単位数の 100% から 110% の範囲内の場合に記録されます。 このイベントが発生した場合でも、クライアントデバイスの保護は継続されます。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストを確認します。使用されていないデバイスを削除します。 • 製品を使用できるデバイス数の上限が増えるように、ライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。 Kaspersky Security Center では、ライセンス数の上限を超過した時にイベントを生成するルールを指定できます。	90 日間
デバイスがネットワーク上で長期間アクティブになっていません	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	この種別のイベントは、管理対象デバイスが一定時間休止状態である場合に発生します。 このイベントが最も高頻度で発生するのは、管理対象デバイスが廃止された場合です。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストからデバイスを手動で削除します。 • 管理コンソールを使用して、または Kaspersky Security Center Web コンソールを使用して［**デバイスがネットワーク上で長期間アクティブになっていません**］イベントが作成されるまでの期間を指定します。 • 管理コンソールを使用して、または Kaspersky Security Center Web コンソールを使用して、デバイスがグループから自動的に削除されるまでの期間を指定します。	90 日間
デバイスの名前が競合しています	4102	KLSRV_EVENT_HOSTS_CONFLICT	この種別のイベントは、管理サーバーが 2 つ以上の管理対象デバイスを単一のデバイスと判断した場合に発生します。 このイベントが最も高頻度で発生するのは、クローンされたハードディスクが管理対象デバイスでのソフトウェアの導入に使用され、ネットワークエージェントを参照デバイスの専用ディスククローンモードに切り替えなかった場合です。 この問題を回避するには、このデバイスのハードディスクを複製する前に、参照デバイスでネットワークエージェントをディスククローンモードに切り替えます。	90 日間
デバイスのステータスが「警告」です	4114	KLSRV_HOST_STATUS_WARNING	この種別のイベントは、管理対象デバイスに「*警告*」ステータスが割り当てられると記録されます。デバイスのステータスが「*警告*」に切り替わる条件を設定できます。	90 日間
インストール数が上限に近づいているライセンス認証済みアプ	4127	KLSRV_INVLICPROD_FILLED	この種別のイベントは、ライセンス認証済みアプリケーショングループに含まれるサードパーティ製品のインストール数が、ライセンスのプロパティで指	90 日間

リケーショングループがあります			定された最大許容値の 90% に達すると発生します。 このイベントには、次の方法で対応できます： • 一部の管理対象デバイスでサードパーティ製品を使用していない場合は、これらのデバイスからアプリケーションを削除します。 • サードパーティ製品のインストール数が近い将来に許可される最大数を超えることが予想される場合は、事前にサードパーティのライセンスを取得する対象デバイスの数を増やすことを検討してください。 ライセンス認証済みアプリケーショングループ機能を使用することで、サードパーティ製品のライセンスを管理できます。	
証明書が要求されました	4133	KLSRV_CERTIFICATE_REQUESTED	この種別のイベントは、モバイルデバイス管理用の証明書を自動的に再発行できない場合に発生します。 考えられるイベントの原因と適切な対応について以下に示します。 • ［**可能であれば証明書を自動で再発行**］がオフにされている証明書に対して自動再発行が開始されました。これは、証明書の作成中に発生したエラーが原因であると考えられます。証明書の手動再発行が必要になる場合があります。 • 公開鍵インフラストラクチャと統合している場合、PKI との統合および証明書の発行に使用されるアカウントの SAM-Account-Name 属性の欠落が原因であると考えられます。アカウントのプロパティを確認します。	90 日間
証明書が削除されました	4134	KLSRV_CERTIFICATE_REMOVED	この種別のイベントは、管理者がモバイルデバイス管理用の任意の種別の証明書（一般、メール、VPN）を削除した場合に発生します。 証明書を削除すると、この証明書を介して接続されたモバイルデバイスは、管理サーバーへの接続に失敗します。 このイベントは、モバイルデバイスの管理に関連した誤動作を調査する際に有用な場合があります。	90 日間
APNs 証明書の有効期間が終了しています	4135	KLSRV_APN_CERTIFICATE_EXPIRED	この種別のイベントは、APNs証明書の有効期限が切れた場合に発生します。 手動で APNs 証明書を更新し、iOS MDM サーバーにインストールする必要があります。	保管されません
APNs 証明書の有効期間がまもなく終了します	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	この種別のイベントは、APNs 証明書の有効期限が切れるまでの残日数が 14日未満の場合に発生します。 APNs 証明書の有効期限が切れた場合は、手動で APNs 証明書を更新し、iOS MDM サーバーにインストールする必要があります。 有効期限に達する前に APNs 証明書の更新スケジュールを設定することを推奨します。	保管されません
モバイルデバイスに FCM メッセージを送信できませんでした	4138	KLSRV_GCM_DEVICE_ERROR	この種別のイベントは、Android オペレーティングシステムを搭載した管理対象のモバイルデバイスに接続するために Firebase Cloud Messaging（FCM）を使用するようにモバイルデバイス管理が設定されており、FCM サーバーが管理サーバーから受信したリクエストの一部を処理できない場合に発生します。これは、一部の管理対象モバイルデバイスがプッシュ通知を受信しないことを意味します。 イベントの説明の詳細に記載されている HTTP コードを読み、適宜対応します。FCM サーバーから受信した HTTP コードと関連エラーの詳細については、Firebase サービスのドキュメントを参照してください（「ダウンストリームメッセージのエラー応答コード」の章を参照）。	90 日間
FCM メッセージ	4139	KLSRV_GCM_HTTP_ERROR	この種別のイベントは、モバイルデバイス管理が	90 日

を FCM サーバーに送信している時に HTTP エラーが発生しました			Android オペレーティングシステムを搭載した管理対象モバイルデバイスに接続するために Firebase Cloud Messaging（FCM）を使用するように設定されており、FCM サーバーが 200（OK）以外の HTTP コードで管理サーバーのリクエストに応答する場合に発生します。 考えられるイベントの原因と適切な対応について以下に示します。 • FCM サーバー側の問題。イベントの説明の詳細に記載されている HTTP コードを読み、適宜対応します。FCM サーバーから受信した HTTP コードと関連エラーの詳細については、Firebase サービスのドキュメントを参照してください（「ダウンストリームメッセージのエラー応答コード」の章を参照）。 • プロキシサーバー側の問題（プロキシサーバーを使用している場合）。イベントの説明の詳細に記載されている HTTP コードを読み、適宜対応します。	間
FCM メッセージを FCM サーバーに送信できませんでした	4140	KLSRV_GCM_GENERAL_ERROR	この種別のイベントは、Firebase Cloud Messaging HTTP プロトコルを使用する際の管理サーバー側での予期しないエラーが原因で発生します。 イベントの説明に記載されている詳細情報を読み、適宜対応します。 ご自分で問題の解決方法を見つけられない場合は、カスペルスキーのテクニカルサポートへのお問い合わせを推奨します。	90 日間
ハードディスクの空き容量が残りわずかです	4105	KLSRV_NO_SPACE_ON_VOLUMES	この種別のイベントは、管理サーバーがインストールされているデバイスのハードディスク容量が不足した場合に発生します。 デバイスのディスク領域を解放します。	90 日間
管理サーバーデータベースに空き容量が残りわずかです	4106	KLSRV_NO_SPACE_IN_DATABASE	この種別のイベントは、管理サーバーのデータベースの空き容量が非常に少なくなっている場合に記録されます。状況を修正しないと、すぐに管理サーバーデータベースの容量が上限に達し、管理サーバーが正常に動作しなくなります。 使用されている DBMS の種別に応じた、このイベントが発生する原因と適切な対応方法を次に示します。 SQL Server Express Edition を DBMS として使用している場合： • SQL Server Express のヘルプを参照して、使用中のバージョンのデータベースサイズの上限を確認します。管理サーバーのデータベースが、もうすぐこのデータベースサイズの上限に達する可能性があります。 • 管理サーバーデータベースに保存されるイベントの数を制限してください。 • 管理サーバーデータベースにアプリケーションコントロールコンポーネントから送信されたイベントの数が多すぎます。これには、管理サーバーデータベースでのアプリケーションコントロールイベントの保管期間に関する Kaspersky Endpoint Security for Windows ポリシーの設定を変更することで対応できます。 SQL Server Express Edition 以外の DBMS を使用している場合： • 管理サーバーのデータベースに保存されるイベントの数を制限しないでください • 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください DBMS の選定に関する情報を確認します。	90 日間
セカンダリ管理	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	この種別のイベントは、セカンダリ管理サーバーへ	90 日

サーバーとの接続が中断されました			の接続が中断された場合に発生します。 セカンダリ管理サーバーがインストールされているデバイスの Kaspersky イベントログを読み、適宜対応します。	間
プライマリ管理サーバーとの接続が中断されました	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	この種別のイベントは、プライマリ管理サーバーへの接続が中断された場合に発生します。 プライマリ管理サーバーがインストールされているデバイスの Kaspersky イベントログを読み、適宜対応します。	90 日間
カスペルスキー製品モジュールの新しいアップデートが登録されました	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	この種別のイベントは、インストールの承認が必要な管理対象デバイスにインストールされているカスペルスキーソフトウェアの新しいアップデートを管理サーバーが登録する場合に発生します。 管理コンソールまたは Kaspersky Security Center Web コンソールを使用して、アップデートを承認または拒否します。	90 日間
データベースのイベントの上限数を超えました。イベントの削除が開始されました	4145	KLSRV_EVP_DB_TRUNCATING	この種別のイベントは、管理サーバーのデータベース容量が上限に達して、データベース内の古いイベントの削除が開始された時に記録されます。 このイベントには、次の方法で対応できます： • 管理サーバーデータベースに保管されるイベント数の上限を変更してください • 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください	保管されません
データベースのイベントの上限数を超えました。このイベントは削除されました	4146	KLSRV_EVP_DB_TRUNCATED	この種別のイベントは、管理サーバーのデータベース容量が上限に達して、データベース内の古いイベントが削除された時に記録されます。 このイベントには、次の方法で対応できます： • 管理サーバーデータベースに保管できるイベント数の上限を変更してください • 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください	保管されません

管理サーバーの情報イベント

次の表は、重要度が「**情報**」に分類される Kaspersky Security Center 管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

管理サーバーの情報イベント

イベント種別の表示名	イベント種別の ID	イベント種別	既定の保管期間	備考
ライセンス使用率が 90% を超えています	4097	KLSRV_EV_LICENSE_CHECK_90	30 日間	
新しいデバイスが検出されました	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 日間	
デバイスが自動的にグループに追加されました	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 日間	
デバイスがルールに従って自動的に移動されました	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 日間	
デバイスがグループから削除されました：ネットワーク上で長期間アクティブになっていません	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 日間	
インストール数が上限に近づいている（95% を超える数を使用済み）ライセンス認証済みアプリケーショングループが	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 日間	

あります				
カスペルスキーへ分析のために送付するファイルが見つかりました	4131	KLSRV_APS_FILE_APPEARED	30 日間	
このモバイルデバイス上で FCM 送信者 ID が変更されました	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 日間	
指定のフォルダーにアップデートがコピーされました	4122	KLSRV_UPD_REPL_OK	30 日間	
セカンダリ管理サーバーとの接続が確立されました	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 日間	
プライマリ管理サーバーとの接続が確立されました	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 日間	
定義データベースがアップデートされました	4144	KLSRV_UPD_BASES_UPDATED	30 日間	
監査：管理サーバーとの接続が確立されました	4147	KLAUD_EV_SERVERCONNECT	30 日間	
監査：オブジェクトが変更されました	4148	KLAUD_EV_OBJECTMODIFY	30 日間	このイベントは次のオブジェクトの変更を追跡します： • 管理グループ • セキュリティグループ • ユーザー • パッケージ • タスク • ポリシー • サーバー • 仮想サ

				ーバー
監査：オブジェクトのステータスが変更されました	4150	KLAUD_EV_TASK_STATE_CHANGED	30 日間	たとえば、このイベントはタスクがエラーで失敗した時に発生します。
監査：グループ設定が変更されました	4149	KLAUD_EV_ADMGROUP_CHANGED	30 日間	
監査：管理サーバーへの接続が切断されました	4151	KLAUD_EV_SERVERDISCONNECT	30 日間	
監査：オブジェクトのプロパティが変更されました	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 日間	このイベントは、次のプロパティの変更を追跡します： • ユーザー • ライセンス • サーバー • 仮想サーバー
監査：ユーザーの権限が変更されました	4153	KLAUD_EV_OBJECTACLMODIFIED	30 日間	
監査：管理サーバーから暗号化キーがインポートまたはエクスポートされました	5100	KLAUD_EV_DPEKEYSEXPORT	30 日間	

ネットワークエージェントのイベント

このセクションには、ネットワークエージェントに関するイベントの情報が記載されています。

ネットワークエージェントの機能エラーイベント

次の表は、重要度が「**機能エラー**」に分類される Kaspersky Security Center ネットワークエージェントのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

ネットワークエージェントの機能エラーイベント

イベント種別の表示名	イベント種別の ID	イベント種別	説明	既定の保管期間
アップデートのインストールエラー	7702	KLNAG_EV_PATCH_INSTALL_ERROR	この種別のイベントは、Kaspersky Security Center コンポーネントの自動アップデートおよびパッチ適用に失敗した時に記録されます。このイベントは、管理対象のカスペルスキー製品のアップデートとの関連はありません。 イベントの説明を確認します。管理サーバーで Windows 関連の問題がこのイベントの原因となっている可能性があります。イベントの説明で Windows の設定に関する問題が言及されている場合、その問題を解決してください。	30 日間
サードパーティ製品のアップデートをインストールできませんでした	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	この種別のイベントは、脆弱性とパッチ管理とモバイルデバイス管理を使用していて、サードパーティ製品のアップデートに失敗した時に記録されます。 サードパーティ製品へのリンクが有効かどうかを確認します。イベントの説明を確認します。	30 日間
Windows Update 更新プログラムをインストールできませんでした	7717	KLNAG_EV_WUA_INSTALL_ERROR	この種別のイベントは、Windows の更新プログラムの適用に失敗した時に記録されます。ネットワークエージェントポリシーで Windows アップデートの設定を行ってください。 イベントの説明を確認します。該当するエラーに関する説明がマイクロソフト サポート技術情報で提供されていないかを検索してください。問題の解決が困難な場合は、マイクロソフトのテクニカルサポートにお問い合わせください。	30 日間
ユーザー管理：エラー	7723	KLNAG_EV_USR_MNG_ERR	一般警告イベント。	30 日間
Sudo ファイルを参照値に復元できませんでした	7726	KLNAG_EV_SUDOER_RESTORED_ERR	イベントには、ファイル sudoers の置換エラーの説明が含まれています。	30 日間
ルート証明書をインストールできませんでした	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	イベントには、証明書のインストールエラーの説明が含まれます。	30 日間
ルート証明書を削除できません	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	イベントには、証明書削除エラーの説明が含まれます。	30 日間

ネットワークエージェントの警告イベント

次の表は、重要度が「**警告**」に分類される Kaspersky Security Center のネットワークエージェントのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

ネットワークエージェントの警告イベント

イベント種別の表示名	イベント種別の ID	イベント種別	既定の保管期間
ソフトウェアモジュールのアップデートのインストール中に警告が発生しました	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 日間
サードパーティ製品のアップデートのインストールが警告を出力して完了しました	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 日間
サードパーティ製品のアップデートのインストールが延期されました	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 日間

セキュリティ問題が発生しました	549	GNRL_EV_APP_INCIDENT_OCCURED	30 日間
KSN プロキシサーバーが起動しました。KSN 可用性をチェックできませんでした	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 日間
ユーザー管理：警告	7722	KLNAG_EV_USR_MNG_WRN	30 日間
検出された Sudo ファイルは参照値と一致しません	7724	KLNAG_EV_SUDOER_DIFFERENT	30 日間

ネットワークエージェントの情報イベント

次の表は、重要度が「**情報**」に分類される Kaspersky Security Center のネットワークエージェントのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

ネットワークエージェントの情報イベント

イベント種別の表示名	イベント種別の ID	イベント種別	既定の保管期間
ソフトウェアモジュールのアップデートがインストールされました	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 日間
ソフトウェアモジュールのアップデートのインストールを開始しました	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 日間
アプリケーションがインストールされました	7703	KLNAG_EV_INV_APP_INSTALLED	30 日間
アプリケーションがアンインストールされました	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 日間
監視対象アプリケーションがインストールされました	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 日間
監視対象アプリケーションがアンインストールされました	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 日間
サードパーティ製品がインストールされました	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 日間
新しいデバイスが追加されました	7708	KLNAG_EV_DEVICE_ARRIVAL	30 日間
デバイスが削除されました	7709	KLNAG_EV_DEVICE_REMOVE	30 日間
新しいデバイスが検出されました	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 日間
デバイスが認証されました	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 日間
Windows デスクトップ共有：ファイルが読み取られました	7712	KLUSRLOG_EV_FILE_READ	30 日間
Windows デスクトップ共有：ファイルが変更されました	7713	KLUSRLOG_EV_FILE_MODIFIED	30 日間
Windows デスクトップ共有：アプリケーションが起動しました	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 日間
Windows デスクトップ共有：開始しました	7715	KLUSRLOG_EV_WDS_BEGIN	30 日間
Windows デスクトップ共有：停止しました	7716	KLUSRLOG_EV_WDS_END	30 日間
サードパーティ製品のアップデートがインストールされました	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 日間

サードパーティ製品のアップデートのインストールを開始しました	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 日間
KSN プロキシサーバーが起動しました。KSN 可用性チェックが完了しました	7719	KSNPROXY_STARTED_CON_CHK_OK	30 日間
KSN プロキシが停止しました	7720	KSNPROXY_STOPPED	30 日間

iOS MDM サーバーイベント

このセクションには、iOS MDM サーバーに関するイベントの情報が記載されています。

iOS MDM サーバーの機能エラーイベント

次の表は、重要度が「**機能エラー**」に分類される Kaspersky Security Center iOS MDM サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

iOS MDM サーバーの機能エラーイベント

イベント種別の表示名	イベント種別	既定の保管期間
プロファイルのリストをリクエストできませんでした	PROFILELIST_COMMAND_FAILED	30 日間
プロファイルをインストールできませんでした	INSTALLPROFILE_COMMAND_FAILED	30 日間
プロファイルを削除できませんでした	REMOVEPROFILE_COMMAND_FAILED	30 日間
プロビジョニングプロファイルのリストをリクエストできませんでした	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 日間
プロビジョニングプロファイルをインストールできませんでした	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 日間
プロビジョニングプロファイルを削除できませんでした	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 日間
デジタル証明書のリストをリクエストできませんでした	CERTIFICATELIST_COMMAND_FAILED	30 日間
インストール済みアプリケーションのリストをリクエストできませんでした	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 日間
モバイルデバイスに関する一般情報をリクエストできませんでした	DEVICEINFORMATION_COMMAND_FAILED	30 日間
セキュリティ情報をリクエストできませんでした	SECURITYINFO_COMMAND_FAILED	30 日間
モバイルデバイスをロックできませんでした	DEVICELOCK_COMMAND_FAILED	30 日間
パスワードをリセットできませんでした	CLEARPASSCODE_COMMAND_FAILED	30 日間
モバイルデバイスのデータを消去できませんでした	ERASEDEVICE_COMMAND_FAILED	30 日間
アプリをインストールできませんでした	INSTALLAPPLICATION_COMMAND_FAILED	30 日間
アプリのリデンプションコードを設定できませんでした	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 日間
管理対象アプリのリストをリクエストできませんでした	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 日間
管理対象アプリを削除できませんでした	REMOVEAPPLICATION_COMMAND_FAILED	30 日間
ローミング設定が拒否されました	SETROAMINGSETTINGS_COMMAND_FAILED	30 日間
アプリの動作でエラーが発生しました	PRODUCT_FAILURE	30 日間
コマンドの結果に無効なデータが含まれています	MALFORMED_COMMAND	30 日間
プッシュ通知を送信できませんでした	SEND_PUSH_NOTIFICATION_FAILED	30 日間
コマンドを送信できませんでした	SEND_COMMAND_FAILED	30 日間
デバイスが見つかりません	DEVICE_NOT_FOUND	30 日間

iOS MDM サーバーの警告イベント

次の表は、重要度が「**警告**」に分類される Kaspersky Security Center iOS MDM サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

iOS MDM サーバーの警告イベント

イベント種別の表示名	イベント種別	既定の保管期間
ロックされたモバイルデバイスを接続する試行を検出しました	INACTICE_DEVICE_TRY_CONNECTED	30 日間
プロファイルが削除されました	MDM_PROFILE_WAS_REMOVED	30 日間
クライアント証明書を再使用する試行を検出しました	CLIENT_CERT_ALREADY_IN_USE	30 日間
非アクティブなデバイスを検出しました	FOUND_INACTIVE_DEVICE	30 日間
リデンプションコードが必要です	NEED_REDEMPTION_CODE	30 日間
デバイスから削除されたポリシーにプロファイルが含まれていました	UMDM_PROFILE_WAS_REMOVED	30 日間

iOS MDM サーバーの情報イベント

次の表は、重要度が「**情報**」に分類される Kaspersky Security Center iOS MDM サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

iOS MDM サーバーの情報イベント

イベント種別の表示名	イベント種別	既定の保管期間
新しいモバイルデバイスが接続されました	NEW_DEVICE_CONNECTED	30 日間
プロファイルのリストをリクエストしました	PROFILELIST_COMMAND_SUCCESSFULL	30 日間
プロファイルがインストールされました	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 日間
プロファイルが削除されました	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 日間
プロビジョニングプロファイルのリストをリクエストしました	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 日間
プロビジョニングプロファイルがインストールされました	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 日間
プロビジョニングプロファイルが削除されました	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 日間
デジタル証明書のリストをリクエストしました	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 日間
インストール済みアプリケーションのリストをリクエストしました	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 日間
モバイルデバイスに関する一般情報をリクエストしました	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 日間
セキュリティ情報をリクエストしました	SECURITYINFO_COMMAND_SUCCESSFULL	30 日間
モバイルデバイスをロックしました	DEVICELOCK_COMMAND_SUCCESSFULL	30 日間
パスワードがリセットされました	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 日間
データがモバイルデバイスから削除されました	ERASEDEVICE_COMMAND_SUCCESSFULL	30 日間
アプリがインストールされました	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 日間
アプリのリデンプションコードが設定されました	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 日間

管理対象アプリのリストをリクエストしました	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 日間
管理対象アプリが削除されました	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 日間
ローミング設定が適用されました	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 日間

頻出イベントのブロック

このセクションでは、頻出イベントのブロックの管理および頻出イベントのブロックの解除について説明します。

頻出イベントのブロックについて

単一または複数の管理対象デバイスにインストールされた Kaspersky Endpoint Security for Windows などの管理対象アプリケーションは、管理サーバーに対して同様の種別のイベントを大量に送信することがあります。頻出イベントを受信すると、管理サーバーのデータベース高負荷がかかり、他のイベントが上書きされる場合があります。管理サーバーは、受信したイベントの総量がデータベースで指定した制限を超えた場合、頻出イベントをブロックします。

管理サーバーは頻出イベントの受信を自動的にブロックします。ユーザー自身による頻出イベントのブロックや、ブロックするイベントの選択はできません。

イベントがブロックされているかどうかを確認したい場合、通知リストを表示するか、そのイベントが管理サーバーのプロパティの［**頻出イベントのブロック**］セクションに存在するかどうかで確認できます。イベントがブロックされている場合、次を実行します：

- データベースの上書きを防止したい場合、このような種別のイベントの受信のブロックを継続できます。
- たとえば、管理サーバーに頻出イベントが送信される原因を見つける場合などには、頻出イベントのブロックを解除してこの種別のイベントの受信を継続できます。
- 頻出イベントの受信が再度ブロックされるまで受信を継続する場合は、頻出イベントのブロック対象から削除することができます。

頻出イベントのブロックの管理

管理サーバーは頻出イベントの自動受信をブロックしますが、ブロックを解除してイベントの受信を継続することができます。また、以前にブロック解除したイベントを再度ブロックすることもできます。

頻出イベントのブロックを管理するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（ ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**頻出イベントのブロック**］セクションを選択します。
3. ［**頻出イベントのブロック**］セクションで次の操作を実行します：
   - 頻出イベントの受信のブロックを解除する場合：

a. ブロック解除する頻出イベントを選択し、［**除外**］をクリックします。

b. ［**保存**］をクリックします。

- 頻出イベントをブロックする場合は：

a. ブロックする頻出イベントを選択し、［**ブロック**］をクリックします。

b. ［**保存**］をクリックします。

管理サーバーはブロック解除された頻出イベントを受け取り、ブロック対象の頻出イベントは受け取りません。

頻出イベントのブロックの解除

頻出イベントのブロックを解除して、管理サーバーが再度ブロックするまでこれらの頻出イベントを受信できます。

頻出イベントのブロックを解除するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**頻出イベントのブロック**］セクションを選択します。
3. ［**頻出イベントのブロック**］セクションで、ブロックを解除するイベントの行をクリックします。
4. ［**ブロックから削除**］をクリックします。

イベントは頻出イベントのリストから削除されます。管理サーバーはこの種別のイベントを受信します。

Kaspersky Security for Microsoft ExchangeServer からのイベントの受信

Kaspersky Endpoint Security for Windows などの管理対象アプリケーションの操作中のイベントに関する情報は、管理対象デバイスから転送され、管理サーバーデータベースに登録されます。既定では、Kaspersky Security for Microsoft Exchange Servers 9.0 MR6 およびそれ以前のバージョンからのイベントは管理サーバーのデータベースに登録されません。組織内の管理対象デバイスに Kaspersky Security for Microsoft Exchange Servers 9.0 MR6 およびそれ以前のバージョンがインストールされていて、この製品からイベントを受信する場合は、klscflag ユーティリティを使用してこの製品のイベント登録を有効にします。

Kaspersky Security for Microsoft Exchange Servers のイベント登録を有効にするには：

1. 管理サーバーデバイスで、管理者権限を持つアカウントで Windows コマンドプロンプトを実行します。
2. カレントディレクトリを Kaspersky Security Center のインストールフォルダ（通常は C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center）に変更します。
3. 次のコマンドのいずれかを実行します：

- Windows Server のフェールオーバークラスターにインストールされた管理サーバーの場合：

```
klscflag.exe --stp cluster -fset -pv klserver -n
KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
```

- カスペルスキーのフェールオーバークラスターノードにインストールされた管理サーバーの場合：

  ```
  klscflag.exe --stp klfoc -fset -pv klserver -n
  KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
  ```

- クラスターで動作していない管理サーバーの場合：

  ```
  klscflag.exe -fset -pv klserver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d
  -v 0
  ```

Kaspersky Security for Microsoft Exchange Servers のイベント登録が有効になります。

Kaspersky Security for Microsoft Exchange Servers では、イベントの保存期間を設定したり、管理サーバーリポジトリに保存する必要のあるイベントを選択したりすることはできません。リポジトリに保存できるイベントの最大数を設定できます。この設定は、すべてのカスペルスキー製品から受信したイベントに適用されます。

通知とデバイスのステータス

このセクションでは、通知の表示、通知の配信の設定、デバイスのステータスの使用、デバイスのステータス変更を有効にする方法について説明します。

通知機能の使用

通知機能を使用してイベントのアラート通知を受け取ることで、推奨される処理や担当者が適切と考える対応を行うまでの時間を短縮できます。

次の種別の通知を、通知方法の選択に応じて使用できます：

- 画面表示による通知
- SMS 通知
- メール通知
- 実行ファイルまたはスクリプトの実行で通知

画面表示による通知

画面表示による通知では、重要度別にアラート通知を確認できます（*緊急*、*警告*、*情報*）。

画面表示による通知には 2 種類のステータスがあります：

- *確認済み*：推奨される処理として記載されている処理を行ったか、通知に手動でこのステータスを割り当てた場合に、このステータスが付与されます。
- *未確認*：推奨される処理として記載されている処理を未実行か、通知に「確認済み」のステータスを手動で割り当てていない場合に、このステータスが付与されます。

既定では、通知リストには「*未確認*」ステータスの通知が表示されます。

画面表示される通知を確認し、リアルタイムでの対応を行うことで、組織ネットワークの監視業務を実行できます。

メール、SMS、または実行ファイルやスクリプトの実行による通知

Kaspersky Security Center では、必要に応じて、重要だと考えられる任意のイベントに対して通知の送信を設定し、組織ネットワークの監視に役立てることができます。任意のイベントで、メール、SMS、または実行ファイルやスクリプトの実行による通知を設定できます。

メールまたは SMS で通知を受け取った場合、イベント内容を確認して必要な対応を決定できます。この対応は組織のネットワークに対して最も適切なものである必要があります。実行ファイルまたはスクリプトの実行を設定する場合は、イベントに対する対応を事前に指定できます。また、実行ファイルまたはスクリプトの実行による対応を、イベントに対する初期対応として考えることもできます。この場合、実行ファイルの実行後に、イベントに対して必要な追加対応を担当者自身が実施できます。

画面表示による通知の確認

通知は次の 3 通りの方法で画面表示できます：

- ［**監視とレポート**］→［**通知**］セクション。ここで定義済みのカテゴリに関連する通知を確認できます。
- どのセクションからもメニュー上部のアイコンを使用して開くことができる別のウィンドウ。この方法を使用すると、通知を確認済みとしてマークできます。
- ［**監視とレポート**］→［**ダッシュボード**］セクションの［**選択した深刻度別の通知**］ウィジェット。ウィジェットで、重要度が *緊急*と *警告*のイベントの通知のみ確認できます。

イベントに応答するなど、処理を実行できます。

定義済みのカテゴリから通知を確認するには：

1. メインメニューで、［**監視とレポート**］→［**通知**］に移動します。
   ［**すべての通知**］カテゴリが左側のペインで選択されており、右側のペインですべての通知が表示されます。
2. 左側のペインで、次のカテゴリのいずれかを選択します：
   - **製品の導入**
   - **デバイス**
   - **プロテクション**
   - **アップデート**（ダウンロード可能なカスペルスキー製品とダウンロードされた定義データベースのアップデートに関する通知が含まれます）
   - **脆弱性攻撃ブロック**
   - **管理サーバー**（管理サーバーのみに関するイベントが含まれます）

- **参考リンク**（カスペルスキーのリソース（たとえば、カスペルスキーのテクニカルサポート、カスペルスキーのコミュニティ、販売代理店リストのページ、ウイルス百科事典など）へのリンクが含まれます）

- **カスペルスキーニュース**（カスペルスキー製品のリリースに関する情報が含まれます）

選択したカテゴリの通知のリストが表示されます。リストには次が含まれます：

- 情報の内容に関連するアイコン：導入、保護、アップデート、デバイスの管理、脆弱性攻撃ブロック、管理サーバー。
- 通知の重要度：重要度が、**緊急の通知**（）、**警告の通知**（）、**情報の通知**の通知が表示されます。リスト内の通知は重要度に応じてグループ化されています。
- **通知**：通知の説明が含まれます。
- **処理**：コンソールで実行可能な、推奨される処理へのリンクが含まれます。それぞれのリンクをクリックすると、たとえば、リポジトリに移動してデバイスにセキュリティ製品をインストールしたり、デバイスまたはイベントのリストを確認できます。通知に推奨される処理を実行すると、この通知に*確認済み*のステータスが割り当てられます。
- **ステータス登録後の時間**：通知が管理サーバーに登録された時点から経過した日数または時間数が含まれます。

別のウィンドウで、画面表示による通知を重要度別に確認するには：

1. Kaspersky Security Center Web コンソールの右上端で、フラグアイコン（）をクリックします。

   フラグアイコンに赤い丸印が表示されている場合は、確認されていない通知があります。

   通知のリストを含むウィンドウが開きます。既定では、［**すべての通知**］タブが選択されており、*緊急*、*警告*、*情報*の重要度別に通知がグループ化されています。

2. ［**システム**］タブを選択します。

   重要度が*緊急*（）と*警告*（）の通知のリストが表示されます。通知のリストには以下が含まれます：

   - カラーマーカー：緊急の通知には赤色のマーカーが使用されます。警告の通知には黄色のマーカーが使用されます。
   - 情報の内容を示すアイコン：導入、保護、アップデート、デバイスの管理、脆弱性攻撃ブロック、管理サーバー。
   - 通知の説明。
   - フラグアイコン：通知に*未確認*のステータスが割り当てられている場合、［フラグ］アイコンは灰色です。灰色の［フラグ］アイコンを選択して通知に*確認済み*のステータスを割り当てると、アイコンは白色に変更されます。
   - 推奨される処理へのリンク：リンクをクリックした後で推奨される処理を実行すると、通知は*確認済み*のステータスになります。
   - 通知が管理サーバーに登録された時点から経過した日数または時間数。

3. ［**詳細**］タブを選択します。

重要度が*情報*の通知のリストが表示されます。

リストの各項目の構成は、［**システム**］タブのリスト（前述の説明を参照）と同じです。カラーマーカーが使用されない点のみ異なります。

通知が管理サーバーに登録された期間で通知をフィルタリングできます。フィルターを管理するには、［**フィルターの表示**］をオンにします。

ウィジェットで画面表示による通知を確認するには：

1. ［**ダッシュボード**］セクションで、［**Web ウィジェットを追加または復元**］を選択します。
2. 表示されたウィンドウで、［**その他**］のカテゴリをクリックし、［**選択した深刻度別の通知**］ウィジェットを選択して、［追加］をクリックします。

   これによりウィジェットが［**ダッシュボード**］タブに表示されます。既定では、重要度が*緊急*の通知がウィジェットに表示されます。

   ウィジェットの［**設定**］をクリックしてウィジェットの設定を変更すると、重要度が*警告*の通知を表示できます。または、*警告*の重要度を指定して［**選択した深刻度別の通知**］ウィジェットを追加できます。

   通知リストのウィジェットには表示領域のサイズの制限があるため、表示される通知は 2 つまでです。これらの 2 つの通知は最新のイベントに関連します。

通知リストのウィジェットには以下が含まれます：

- 情報の内容に関連するアイコン：導入 ()、保護 ()、アップデート()、デバイスの管理 ()、脆弱性攻撃ブロック ()、管理サーバー ()。
- 推奨される処理へのリンクを含む通知の説明：リンクをクリックした後で推奨される処理を実行すると、通知は「*確認済み*」のステータスになります。
- 通知が管理サーバーに登録された時点から経過した日数または時間数。
- その他の通知へのリンク：このリンクをクリックすると、［**監視とレポート**］セクションの［**通知**］セクションに表示される通知リストの画面に移動します。

デバイスのステータスの概要

Kaspersky Security Center は、各管理対象デバイスにステータスを割り当てます。特定のステータスは、ユーザーが定義した条件を満たしているかどうかによって異なります。場合によっては、デバイスにステータスを割り当てるときに、Kaspersky Security Center はネットワーク内のデバイスの可視性フラグを考慮します（下の表を参照）。Kaspersky Security Center が 2 時間以内にネットワーク内のデバイスを見つけられない場合、デバイスの可視性フラグは「*不可視*」に設定されます。

ステータスは次の通りです：

- *緊急*または*緊急 / 可視*
- *警告*または*警告 / 可視*
- *OK* または *OK / 可視*

次の表では、「*緊急*」または「*警告*」ステータスをデバイスに割り当てるために満たすべき既定の条件を、可能なすべての値とともに一覧で表示します。

デバイスにステータスを割り当てる条件

条件	条件の説明	設定可能な値
セキュリティ製品がインストールされていません	デバイスにネットワークエージェントはインストールされていますが、セキュリティ製品はインストールされていません。	• 切り替えスイッチをオン • 切り替えスイッチをオフ
ウイルスが多数検知されました	*マルウェアスキャン*タスクなどのウイルス検知タスクによりデバイスでウイルスが検知され、検知数が指定された値を超えました。	0より大きい値
リアルタイム保護レベルが管理者の設定と異なります	デバイスはネットワーク上で可視ですが、リアルタイム保護レベルがデバイスのステータスの条件として管理者によって設定されたレベルと異なっています。	• 停止 • 一時停止 • 実行中
マルウェアスキャンが長期間実行されていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、*マルウェアのスキャン*タスクもローカルスキャンタスクも実行されていない状態が指定期間を越えて続いています。この条件は、7日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。	1日より大きい値
定義データベースがアップデートされていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、このデバイスで定義データベースがアップデートされていない状態が指定期間を越えて続いています。この条件は、1日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。	1日より大きい値
長期間接続されていません	デバイスにネットワークエージェントはインストールされていますが、デバイスがオフになっており、デバイスが管理サーバーに接続されていない状態が指定期間を越えて続いています。	1日より大きい値
アクティブな脅威を検知しました	［**アクティブな脅威**］フォルダー内の未処理オブジェクトの数が指定の値を上回っています。	0項目より大きい値
再起動が必要です	デバイスはネットワーク上で可視ですが、アプリケーションが選択した理由でデバイスの再起動を必要とする状態が指定期間を越えて続いています。	0分より大きい値
競合アプリケーションがインストールされています	デバイスはネットワーク上で可視ですが、ネットワークエージェントから実行されたソフトウェアインベントリにより、競合するアプリケーションがデバイスにインストールされていることを検知しました。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
ソフトウェアの脆弱性が検知されました	デバイスはネットワーク上で可視でネットワークエージェントもインストールされていますが、*脆弱性とアプリケーションのアップデートの検索*タスクが、デバイスにインストールされているアプリケーションで指定された重要度の脆弱性を検知しました。	• 緊急 • 高 • 中 • 脆弱性を修正できない場合は無視する • 修正プログラムがインストール用に割り当てられている場合は無視する
ライセンスの有効期間が終了しました	デバイスはネットワーク上で可視ですが、ライセンスの有効期間が終了しています。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
ライセンスの有効期間がまもなく終了します	デバイスはネットワーク上で可視ですが、ライセンスの有効期間の残り日数が指定した期間以下しかありません。	0日より大きい値
Windows Update 更新プログラムの	デバイスはネットワーク上で可視ですが、*Windows Update の同期の実行*タスクが実行されていない状態が指定期間を越えて続いています。	1日より大きい値

チェックが長期間実行されていません		
暗号化ステータスが無効です	デバイスにネットワークエージェントはインストールされていますが、デバイスの暗号化結果が割り当て条件として指定されているものと合致しました。	• ユーザーが拒否したため、ポリシーに準拠していない（外部デバイスのみ）。 • エラーにより、ポリシーに準拠していない。 • ポリシーを適用したら再起動する必要がある。 • 暗号化ポリシーが指定されていない。 • サポートされていない。 • ポリシーを適用するとき。
モバイルデバイスの設定がポリシーに適合していません	コンプライアンスルールをチェックしたところ、モバイルデバイスの設定が Kaspersky Endpoint Security for Android ポリシーで指定された設定と異なります。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
未処理のセキュリティ問題が検出されました	未処理のセキュリティ問題がデバイス上でいくつか見つかりました。セキュリティ問題は、クライアントデバイスにインストールしたカスペルスキー製品によって自動で作成されるか、管理者が手動で作成します。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
製品が定義したデバイスのステータス	デバイスのステータスが管理対象アプリケーションによって定義されています。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
デバイスに空き容量がありません	デバイスの空き容量が指定された値未満またはデバイスと管理サーバーを同期できませんでした。デバイスが管理サーバーと正常に同期されなおかつデバイスの空き容量が指定値以上になった場合、ステータスが［*緊急*］または［*警告*］から［*OK*］に変更されます。	0 MB より大きい値。
デバイスが管理対象外になりました	デバイスの検索中、デバイスはネットワークで認識されましたが、管理サーバーとの同期に 3 回以上失敗しました。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
プロテクションが無効です	デバイスはネットワーク上で可視ですが、デバイス上でセキュリティ製品が無効になっている状態が指定期間を越えて続いています。 この場合、セキュリティ製品の状態は*停止中*または*エラー*となり、*開始中*、*実行中*、*中断中*とは異なります。	0 分より大きい値
セキュリティ製品が実行されていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、セキュリティ製品が実行されていません。	• 切り替えスイッチをオフ • 切り替えスイッチをオン

Kaspersky Security Center では、指定した条件が満たされると、管理グループのデバイスのステータスが自動的に切り替わるように設定できます。指定した条件が満たされると、クライアントデバイスには、「*緊急*」または「*警告*」のステータスのいずれかが割り当てられます。指定した条件を満たしていない場合、クライアントデバイスには「*OK*」ステータスが割り当てられます。

1つの条件の複数の値に対して異なるステータスを対応させることができます。たとえば、［**定義データベースがアップデートされていません**］条件の値が「**3 日より大きい値**」の場合はクライアントデバイスに「*警告*」ステータスが割り当てられ、条件値が「**7 日より大きい値**」の場合は「*緊急*」ステータスが割り当てられます。

Kaspersky Security Center を以前のバージョンからアップグレードしても、ステータスを「*緊急*」または「*警告*」に割り当てるための［**定義データベースがアップデートされていません**］条件の値は変更されません。

Kaspersky Security Center によってデバイスにステータスが割り当てられると、一部の条件（条件説明の列を参照）で可視性フラグが考慮されます。たとえば、ある管理対象デバイスは［定義データベースがアップデートされていません］条件を満たしていたために「*緊急*」ステータスが割り当てられました。のちにデバイスには可視性フラグが設定され、その後、そのデバイスは「*OK*」ステータスが割り当てられます。

デバイスのステータスの切り替えの設定

デバイスに「*緊急*」または「*警告*」ステータスを割り当てる条件を変更できます。

デバイスのステータスの「緊急」への切り替えを有効にするには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. グループのリストが開いたら、デバイスのステータスの切り替えを設定するグループ名をクリックします。
3. プロパティウィンドウが開いたら、［**デバイスのステータス**］タブを選択します。
4. 左側のペインで、［**緊急**］を選択します。
5. 右側のペインの［**指定されている場合は「緊急」に設定**］セクションで、デバイスに［*緊急*］ステータスを割り当てる条件をオンにします。

   親ポリシーでロック状態になっていない設定のみ変更できます。

6. リスト内の条件の横にあるラジオボタンをオンにします。
7. リストの左上にある［**編集**］をクリックします。
8. 選択した条件に対して適切な値を設定します。
   すべての条件に値を設定できるわけではありません。
9. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*緊急*」ステータスが割り当てられます。

デバイスのステータスの「警告」への切り替えを有効にするには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. グループのリストが開いたら、デバイスのステータスの切り替えを設定するグループ名をクリックします。
3. プロパティウィンドウが開いたら、［**デバイスのステータス**］タブを選択します。
4. 左側のペインで、［**警告**］を選択します。
5. 右側のペインの［**指定されている場合は「警告」に設定**］セクションで、デバイスに［*警告*］ステータスを割り当てる条件をオンにします。

   親ポリシーでロック状態になっていない設定のみ変更できます。

6. リスト内の条件の横にあるラジオボタンをオンにします。
7. リストの左上にある［**編集**］をクリックします。
8. 選択した条件に対して適切な値を設定します。
   すべての条件に値を設定できるわけではありません。
9. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*警告*」ステータスが割り当てられます。

通知の設定

Kaspersky Security Center で発生するイベントに関する通知を設定できます。次の種別の通知を、通知方法の選択に応じて使用できます：

- メール：イベントが発生すると、指定されたメールアドレスに通知を送信します。
- SMS：イベントが発生すると、指定された電話番号に通知を送信します。
- 実行ファイル：イベントが発生すると、管理サーバーで実行ファイルが実行されます。

Kaspersky Security Center で発生したイベントの通知の配信を設定するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウの［**全般**］タブが表示されます。
2. ［**通知**］セクションをクリックし、右側のペインで、設定する通知方法のタブを選択します：
   - **メール**

［**メール**］タブでは、メールによるイベントの通知を設定できます。

［**受信者（メールアドレス）**］に、通知の送信先となるメールアドレスを指定します。このフィールドでは、複数のアドレスをセミコロンで区切って指定することができます。

［**SMTP サーバー**］に、メールサーバーのアドレスをセミコロンで区切って指定します。次の値を使用できます：

- IPv4 / IPv6 アドレス
- デバイスの Windows ネットワーク名（NetBIOS 名）
- SMTP サーバーの DNS 名

［**SMTP サーバーのポート**］に、SMTP サーバーの通信ポート番号を指定します。既定のポート番号は 25 です。

［**DNS MX ルックアップを使用**］を有効にすると、IP アドレスの複数の MX レコードを、SMTP サーバーの同一の DNS 名に使用できます。同一 DNS 名に複数の MX レコードが存在し、各レコードのメール受信の優先度の値が異なる場合があります。管理サーバーは SMTP サーバーへのメール通知の 送信を、MX レコードの優先度の昇順に試行します。

［**DNS MX ルックアップを使用**］を有効にし、TLS 設定の使用は有効にしない場合、メール通知を保護する追加の方法として、サーバーデバイスで DNSSEC 設定を使用することを推奨します。

［**ESMTP 認証を使用する**］をオンにすると、［**ユーザー名**］および［**パスワード**］フィールドに ESMTP 認証の設定を指定できます。既定ではこのオプションはオフで、ESMTP 認証設定が使用できない状態になっています。

SMTP サーバーとの接続の TLS 設定を指定できます：

- **TLS を使用しない**

メールの暗号化を無効にする場合に、このオプションを選択できます。

- **TLS を使用する（SMTP サーバーがサポートする場合）**

SMTP サーバーに TLS 接続を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは TLS を使用せずに SMTP サーバーへ接続します。

- **TLS を常に使用し、サーバー証明書の有効性をチェックする**

TLS 認証設定を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは SMTP サーバーへ接続できません。

SMTP サーバーの接続の保護をより強化する目的で、このオプションを使用することを推奨します。このオプションを選択すると、TLS 接続の認証設定を指定できます。

［**TLS を常に使用し、サーバー証明書の有効性をチェックする**］の値を選択する場合は、SMTP サーバーの認証用の証明書を指定し、TLS の任意のバージョンを介した通信を有効にするか、TLS 1.2 以降のバージョンのみを介した通信を有効にするかを選択できます。また、SMTP サーバーでクライアント認証に使用する証明書を指定することもできます。

［**証明書を指定**］をクリックして TLS 接続用の証明書を指定できます。

- SMTP サーバーの証明書ファイルを参照します：

信頼できる証明書認証局から証明書のリストを含むファイルを受け取り、ファイルを管理サーバーへアップロードできます。Kaspersky Security Center は、SMTP サーバーの証明書も信頼できる証明書認証局によって署名されているかどうかをチェックします。信頼できる証明書認証局から SMTP サーバーの証明書を受け取っていない場合、Kaspersky Security Center は SMTP サーバーに接続できません。

- クライアント証明書ファイルを参照します：

信頼できる認証局など、任意の発行元から受け取った証明書を使用できます。次のいずれかの証明書タイプを使用して、証明書とその秘密鍵を指定する必要があります：

- X-509証明書：

証明書を含むファイルと秘密鍵を含むファイルを指定する必要があります。両方のファイルは相互に依存せず、ファイルを読み込む順序は重要ではありません。両方のファイルを読み込む時は、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

- pkcs12 コンテナー：

証明書とその秘密鍵を含む単一のファイルをアップロードする必要があります。ファイルの読み込み時に、秘密鍵をデコードするためのパスワードを指定する必要があります。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

［**件名**］で、メールの件名を指定できます。このフィールドを空白にすることもできます。

［**件名のテンプレート**］ドロップダウンリストで、件名のテンプレートを選択できます。選択したテンプレートに対応する変数が［**件名**］に自動的に入力されます。複数の件名のテンプレートを選択して、メールの件名を構成できます。

［**送信者のメールアドレス**］で、送信者のメールアドレスを指定します。このフィールドを空白にした場合、既定では、宛先のアドレスが使用されます。実在しないアドレスを使用することは避けてください。

［**通知メッセージ**］には、イベントが発生した時に送信される、イベントに関する情報を含む標準的なメッセージが表示されます。このメッセージには、イベント名、デバイス名、ドメイン名といった代替パラメータが含まれます。イベントのより詳細な情報についての代替パラメータを追加して、メッセージを編集することができます。

> 通知テキストにパーセント記号「%」が含まれる場合、メッセージを送信するには 2 つ続けて入力する必要があります。たとえば、「CPU の負荷 100%%」のように入力します。

［**通知数の上限を設定する**］をクリックすると、指定した時間内に送信できる最大通知数を指定できます。

［**テストメッセージの送信**］をクリックすると、通知が正しく設定されているか確認することができます。指定したメールアドレスにテスト通知が送信されます。

- SMS

［**SMS**］タブでは、携帯電話へ送信する様々なイベントの SMS 通知を設定できます。SMS メッセージはメールゲートウェイを通して送信されます。

［**SMTP サーバー**］に、メールサーバーのアドレスをセミコロンで区切って指定します。次の値を使用できます：

- IPv4 / IPv6 アドレス
- デバイスの Windows ネットワーク名（NetBIOS 名）
- SMTP サーバーの DNS 名

［**SMTP サーバーのポート**］に、SMTP サーバーの通信ポート番号を指定します。既定のポート番号は 25 です。

［**ESMTP 認証を使用する**］をオンにすると、［**ユーザー名**］および［**パスワード**］フィールドに ESMTP 認証の設定を指定できます。既定ではこのオプションはオフで、ESMTP 認証設定が使用できない状態になっています。

SMTP サーバーとの接続の TLS 設定を指定できます：

- **TLS を使用しない**

メールの暗号化を無効にする場合に、このオプションを選択できます。

- **TLS を使用する（SMTP サーバーがサポートする場合）**

SMTP サーバーに TLS 接続を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは TLS を使用せずに SMTP サーバーへ接続します。

- **TLS を常に使用し、サーバー証明書の有効性をチェックする**

TLS 認証設定を使用する場合に、このオプションを選択できます。SMTP サーバーが TLS をサポートしていない場合、管理サーバーは SMTP サーバーへ接続できません。

SMTP サーバーの接続の保護をより強化する目的で、このオプションを使用することを推奨します。このオプションを選択すると、TLS 接続の認証設定を指定できます。

［**TLS を常に使用し、サーバー証明書の有効性をチェックする**］の値を選択する場合は、SMTP サーバーの認証用の証明書を指定し、TLS の任意のバージョンを介した通信を有効にするか、TLS 1.2 以降のバージョンのみを介した通信を有効にするかを選択できます。また、SMTP サーバーでクライアント認証に使用する証明書を指定することもできます。

［**証明書を指定**］をクリックして SMTP サーバーのクライアント認証用の証明書を指定できます。

信頼できる証明書認証局から証明書のリストを含むファイルを受け取り、ファイルを管理サーバーへアップロードできます。Kaspersky Security Center は、SMTP サーバーの証明書も信頼できる証明書認証局によって署名されているかどうかをチェックします。信頼できる証明書認証局から SMTP サーバーの証明書を受け取っていない場合、Kaspersky Security Center は SMTP サーバーに接続できません。

［**受信者（メールアドレス）**］に、通知の送信先となるメールアドレスを指定します。このフィールドでは、複数のアドレスをセミコロンで区切って指定することができます。通知は、指定したメールアドレスに関連付けられている電話番号に送信されます。

［**件名**］で、メールの件名を指定できます。

［**件名のテンプレート**］ドロップダウンリストで、件名のテンプレートを選択できます。選択したテンプレートに対応する変数が［**件名**］に入力されます。複数の件名のテンプレートを選択して、メールの件名を構成できます。

［**送信者のメールアドレス：指定されていない場合は、受信者のアドレスを使用します。 注意：実在しないアドレスは使用しないことを推奨します**］で、送信者のメールアドレスを指定します。このフィールドを空白にした場合、既定では、宛先のアドレスが使用されます。実在しないアドレスを使用することは避けてください。

［**SMS メッセージの受信者の電話番号**］フィールドで、SMS 通知の受信者の携帯電話番号を指定します。

［**通知メッセージ**］では、イベントが発生した時に送信される、イベントに関する情報を含む標準的なメッセージを指定できます。このメッセージには、イベント名、デバイス名、ドメイン名などの代替パラメータを含めることができます。

通知テキストにパーセント記号「%」が含まれる場合、メッセージを送信するには 2 つ続けて入力する必要があります。たとえば、「CPU の負荷 100%%」のように入力します。

［**通知数の上限を設定する**］をクリックし、指定した時間内に送信できる最大通知数を指定します。

［**テストメッセージの送信**］をクリックして、通知が正しく設定されているか確認します。指定した宛先にテスト通知が送信されます。

- **実行ファイル**

この通知方法を選択すると、イベントの発生時に起動するアプリケーションを入力フィールドで選択できます。

［**イベント発生時に管理サーバーで実行される実行ファイル**］で、実行するファイルのあるフォルダーとファイル名を指定します。ファイルを指定する前に、通知メッセージで送信されるイベントの詳細を定義するファイルを準備してプレースホルダを指定してください。指定するフォルダーとファイルは、管理サーバー上に配置する必要があります。

［**通知数の上限を設定する**］をクリックすると、指定した時間内に送信できる最大通知数を指定できます。

3. タブで通知の設定を指定します。
4. ［OK］をクリックして、管理サーバーのプロパティウィンドウを閉じます。

保存した通知の配信設定は、Kaspersky Security Center で発生するすべてのイベントに適用されます。

管理サーバーの設定、ポリシーの設定、またはアプリケーションの設定で、［**イベントの設定**］で指定された設定を特定のイベントについて上書きできます。

実行ファイルの起動により表示されるイベント通知

Kaspersky Security Center は、実行ファイルを起動することにより、クライアントデバイスでのイベントについて管理者に通知できます。この実行ファイルには、管理者にリレーするイベントのプレースホルダーを持つ別の実行ファイルを含める必要があります（下表参照）。

イベントを説明するためのプレースホルダー

プレースホルダー	プレースホルダーの説明
%SEVERITY%	イベントの重要度。指定可能な値： • **情報** • **警告** • **エラー** • **緊急**

%COMPUTER%	イベントが発生したデバイスの名前。 デバイス名の最大長は 256 文字です。
%DOMAIN%	イベントが発生したデバイスのドメイン名。
%EVENT%	イベントタイプの名前。 イベントタイプ名の最大長は 50 文字です。
%DESCR%	イベントの説明。 説明の最大長は 1000 文字です。
%RISE_TIME%	イベント作成時間。
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	タスク名。 タスク名の最大長は 100 文字です。
%KL_PRODUCT%	製品名。
%KL_VERSION%	製品のバージョン番号。
%KLCSAK_EVENT_SEVERITY_NUM%	イベントの重要度番号。指定可能な値： • 1 – **情報** • 2 – **警告** • 3 – **エラー** • 4 – **緊急**
%HOST_IP%	イベントが発生したデバイスの IP アドレス。
%HOST_CONN_IP%	イベントが発生したデバイスの接続 IP アドレス。

例：
イベント通知は、%COMPUTER% プレースホルダーを持つ実行ファイル（script2.bat など）を内部で起動する別の実行ファイル（script1.bat など）によって送信されます。イベントが発生すると、管理者のデバイスでファイル script1.bat が起動され、それが %COMPUTER% プレースホルダーを持つファイル script2.bat を起動します。次に管理者は、イベントが発生したデバイスの名前を受信します。

カスペルスキーからの通知

このセクションでは、カスペルスキーからの通知の使用、設定、無効にする方法について説明します。

カスペルスキーからの通知について

カスペルスキーからの通知（［**監視とレポート**］→［**カスペルスキーからの通知**］）には、Kaspersky Security Center のバージョンと、管理対象デバイスにインストールされている管理対象アプリケーションに関連する情報が提供されます。このセクションの情報は、古い通知を削除し、新しい情報を追加することで定期的に更新されます。

Kaspersky Security Center は、現在接続されている管理サーバーおよび管理サーバーの管理対象デバイスにインストールされているカスペルスキー製品に関連するカスペルスキーからの通知のみ表示します。プライマリ、セカンダリ、または仮想サーバーなど管理サーバーの種別に関係なく個別に通知が表示されます。

カスペルスキーからの通知を受け取るために、管理サーバーにはインターネット接続が必要です。

通知には次の種別の情報が含まれます：

- セキュリティ関連告知

  お客様のネットワーク内にインストールされたカスペルスキー製品を最新かつ機能の制限がない状態に保つためのセキュリティ関連告知通知には、カスペルスキー製品の重要なアップデート、既知の脆弱性に対する修正、カスペルスキー製品の問題を修正する方法に関する情報が含まれることがあります。セキュリティ関連告知は既定で有効になっています。通知が必要ない場合は、この機能を無効にできます。

  お客様のネットワーク保護の設定に対応した情報を表示するために、Kaspersky Security Center はデータをカスペルスキーのクラウドサーバーに送信し、ネットワーク内にインストールされたカスペルスキー製品に関連する通知のみを受け取ります。サーバーに送信される可能性のあるデータセットに関しては、Kaspersky Security Center の管理サーバーをインストールする際に同意いただいた使用許諾契約書で説明されています。

- マーケティング関連告知

  マーケティング関連告知には、カスペルスキー製品に関するお得な情報やキャンペーン、カスペルスキーからのニュースなどが含まれます。マーケティング関連の告知は既定で無効になっています。この種類の告知は Kaspersky Security Network (KSN) を有効にした場合のみ受け取ります。KSN を無効にすることでマーケティング関連告知を無効にできます。

  お客様のネットワークのデバイスの保護や日々の作業に役立つ可能性のある情報のみを表示するため、Kaspersky Security Center はカスペルスキーのクラウドサーバーにデータを送信し、適切な通知を受け取ります。サーバーに送信される可能性のあるデータセットは、KSN に関する声明の処理されるデータに関する項で説明されています。

新しい情報は、重要度に基づいて次のカテゴリに分類されます：

1. 緊急の情報
2. 重要なニュース
3. 警告
4. 情報

カスペルスキーからの通知セクションに新しい情報が表示された際に、Kaspersky Security Center Web コンソールには通知の重要度のレベルに応じた通知ラベルが表示されます。ラベルをクリックして、［カスペルスキーからの通知］セクションで通知を表示できます。

カスペルスキーからの通知の設定で、表示する通知のカテゴリや通知を表示する位置を含む設定ができます。

カスペルスキーからの通知を設定する

［カスペルスキーからの通知］セクションで、表示する通知のカテゴリおよび通知を表示する位置を含むカスペルスキーからの通知の設定を変更できます。

カスペルスキーからの通知を設定するには：

1. メインメニューで、［**監視とレポート**］→［**カスペルスキーからの通知**］の順に選択します。
2. ［**設定**］をクリックします。
   カスペルスキーからの通知の設定ウィンドウが開きます。
3. 次の設定を指定します：

   - 表示する通知の重要度を選択します。その他のカテゴリの通知は表示されません。

- 通知ラベルを表示する場所を選択します。ラベルはすべてのコンソールセクション、または［**監視とレポート**］セクションおよびそのサブセクションに表示することができます。

4. ［**OK**］をクリックします。
   カスペルスキーからの通知が設定されました。

カスペルスキーからの通知を無効にする

カスペルスキーからの通知（［**監視とレポート**］→［**カスペルスキーからの通知**］）には、Kaspersky Security Center のバージョンと、管理対象デバイスにインストールされている管理対象アプリケーションに関連する情報が提供されます。通知が必要ない場合は、この機能を無効にできます。

カスペルスキーからの通知には、セキュリティに関するものとマーケティングに関するものの 2 種類の情報があります。これらのお知らせは、種類ごとに無効にできます。

セキュリティ関連告知を無効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**カスペルスキーからの通知**］を選択します。
3. ［**セキュリティ関連告知が［無効］です**］にします。
4. ［**保存**］をクリックします。
   カスペルスキーからの通知が無効になります。

マーケティング関連の告知は既定で無効になっています。マーケティング関連の告知は Kaspersky Security Network (KSN) を有効にした場合のみ受け取ります。KSN を無効にすることでこの種類のお知らせは無効にできます。

マーケティング関連の告知を無効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**KSN プロキシ設定**］セクションを選択します。
3. ［**Kaspersky Security Network の使用が［有効］です**］をオフにします。
4. ［**保存**］をクリックします。
   マーケティング関連の告知が無効になります。

脅威の検知に関する情報の表示

警告に関する情報の表示を有効または無効にできます。

*メインメニューの［**アラート**］セクションでの表示をオンまたはオフにするには：*

1. メインメニューで、アカウント設定に移動して、［**インターフェイスのオプション**］を選択します。

2. 表示される［**Interface options**］ウィンドウで、［**EDR アラートを表示**］をオンまたはオフにします。

3. ［**保存**］をクリックします。

コンソールのメインメニューの［**監視とレポート**］セクションに［**アラート**］サブセクションが表示されます。［**アラート**］サブセクションには、エンドポイントデバイスで検出された脅威に関する情報が表示されます。EDR Optimum のライセンスが追加されている場合は、Kaspersky Security Center Web コンソールは自動的にメインメニューの［**監視とレポート**］セクションに［**アラート**］サブセクションを表示します。また、警告に関する情報を表示するウィジェットを追加することもできます。

検知された脅威の詳細情報を正しくアラートカードに表示するには、Kaspersky Endpoint Agent プラグインおよび互換性のあるバージョンの Kaspersky Endpoint Security プラグイン（Kaspersky Endpoint Security for Linux 12.1 以降、Kaspersky Endpoint Security for Mac 12.1 以降、または Kaspersky Endpoint Security for Windows 12.6 以降）をインストールする必要があります。

［**フィルター**］メニューを使用して、日付とフィールド値でアラートをフィルターします。

［**オブジェクト種別**］フィールドには次の値が含まれます：

- 不明
- ﾌｨｯｼﾝｸﾞ
- ｳｲﾙｽ
- ﾄﾛｲ
- ﾏﾙｳｪｱ
- ﾊﾞｯｸﾄﾞｱ
- ﾜｰﾑ
- その他
- ｱﾄﾞｳｪｱ
- ｱﾀﾞﾙﾄ
- 圧縮
- 疑い

［**自動応答**］フィールドには次の値が含まれます：

- 悪意のあるオブジェクトが検知されました
- オブジェクトが削除されました
- オブジェクトが駆除されました
- オブジェクトが駆除されませんでした
- オブジェクトが隔離に移動されました

- パスワードで保護された圧縮ファイルが検知されました
- ウイルスが検知されました

Cloud Discovery

Kaspersky Security Center は、Windows を実行している管理対象デバイスでのクラウドサービスの使用を監視し、不要と判断されるクラウドサービスへのアクセスをブロックできます。Cloud Discovery は、ブラウザーやデスクトップアプリケーションからこれらのサービスにアクセスしようとするユーザーの試行を追跡します。また、暗号化されていない接続（HTTP プロトコルなどを使用）経由でクラウドサービスにアクセスしようとするユーザーの試行も追跡します。この機能は、シャドー IT によるクラウドサービスの使用を検知して停止するのに役立ちます。

ブロック機能は、Kaspersky Security Center EDR Optimum または XDR Expert ライセンスで Kaspersky Security Center をアクティベートした場合のみ使用できます。

ブロック機能は、Kaspersky Endpoint Security 11.2 for Windows 以降を使用している場合にのみ使用できます。以前のバージョンのセキュリティ製品では、クラウドサービスの使用を監視することしかできませんでした。

Cloud Discovery 機能を有効化し、機能を有効にするセキュリティポリシーまたはプロファイルを選択できます。各セキュリティポリシーまたはプロファイルで個別に機能を有効化または無効化することもできます。ユーザーにアクセスさせたくないクラウドサービスへのアクセスをブロックできます。

クラウドサービスへのアクセスをブロックできるようにするには、次の条件を満たしている必要があります。

- Kaspersky Endpoint Security 11.2 for Windows 以降を使用している。以前のバージョンのセキュリティ製品では、クラウドサービスの使用を監視することしかできませんでした。
- 不要なクラウドサービスへのアクセスをブロックする機能を含む Kaspersky Next のライセンスレベルを購入しました。詳細については、Kaspersky Next ヘルプ を参照してください。

Cloud Discovery ウィジェットと Cloud Discovery レポートには、クラウドサービスへのアクセスの成功およびブロックされた試行に関する情報が表示されます。ウィジェットには、各クラウドサービスのリスクレベルも表示されます。Kaspersky Security Center は、機能が有効になっているセキュリティポリシーまたはプロファイルによってのみ保護されているすべての管理対象デバイスから、クラウドサービスの使用に関する情報を取得します。

ウィジェットを使用して Cloud Discovery を有効にする

Cloud Discovery 機能を使用すると、この機能が有効になっているセキュリティポリシーによってのみ保護されているすべての管理対象デバイスから、クラウドサービスの使用に関する情報を取得できます。Cloud Discovery は、Kaspersky Endpoint Security for Windows ポリシーに対してのみ有効化または無効化できます。

Cloud Discovery 機能を有効にする方法は 2 つあります。

- Cloud Discovery ウィジェットを使用する。
- Kaspersky Endpoint Security for Windows のプロパティを使用する。

Kaspersky Endpoint Security for Windows のポリシーのプロパティで Cloud Discovery 機能を有効にする方法について詳しくは、Kaspersky Endpoint Security for Windows のヘルプの［Cloud Discovery］セクションを参照してください。

Cloud Discovery 機能は、Kaspersky Endpoint Security for Windows のポリシーのパラメータでのみ無効にできることにご注意ください。

Cloud Discovery を有効にするには、［**一般機能：基本機能**］機能領域で［**書き込み**］権限が必要です。

Cloud Discovery ウィジェットを使用して Cloud Discovery 機能を有効にするには：

1. Kaspersky Security Center に移動します。
2. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
3. **Cloud Discovery** ウィジェットで、［**有効にする**］をクリックします。

   Kaspersky Endpoint Security for Windows バージョン 12.4 がインストールされている場合は、Kaspersky Endpoint Security for Windows ポリシープロパティで Cloud Discovery 機能を有効にします。詳細については、Kaspersky Endpoint Security for Windows ヘルプの Cloud Discovery セクションを参照してください。

   Kaspersky Endpoint Security for Windows のバージョン 12.4 より前のバージョンをお持ちの場合は、Kaspersky Endpoint Security for Windows プラグインをバージョン 12.5 にアップデートしてください。

4. 開いた［**Cloud Discovery を有効にする**］ウィンドウで、機能を有効にするセキュリティポリシーを選択し、［**有効にする**］をクリックします。

   次のポリシー設定が自動的に有効になります：**Web ページと連携するため Web トラフィック内にスクリプトを埋め込む**、**Web セッションの監視**、**暗号化された接続のスキャン**。

Cloud Discovery 機能が有効になり、ウィジェットがダッシュボードに追加されます。

Cloud Discovery ウィジェットをダッシュボードに追加する

Cloud Discovery ウィジェットをダッシュボードに追加して、管理対象デバイス上のクラウドサービスの使用を監視できます。

Cloud Discovery ウィジェットをダッシュボードに追加するには、［**一般機能：基本機能**］機能領域で**書き込み**権限を持っている必要があります。

Cloud Discovery ウィジェットをダッシュボードに追加するには：

1. Kaspersky Security Center に移動します。
2. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
3. ダッシュボードで、［**Web ウィジェットを追加または復元**］をクリックします。
4. 使用可能なウィジェットのリストで、山形アイコン（▸）［**その他**］カテゴリの横にあります。

5. ［**Cloud Discovery**］ウィジェットを選択し、［**追加**］をクリックします。

   Cloud Discovery 機能が無効になっている場合は、［ウィジェットを使用して Cloud Discovery を有効にする］セクションの手順に従ってください。

選択したウィジェットはダッシュボードの一番下に追加されます。

クラウドサービスの使用情報を確認する

クラウドサービスへのアクセスの試行に関する情報を示す**クラウド検出**ウィジェットを表示できます。ウィジェットには、各クラウドサービスのリスクレベルも表示されます。Kaspersky Security Center は、この機能が有効になっているセキュリティプロファイルによってのみ保護されているすべての管理対象デバイスから、クラウドサービスの使用に関する情報を取得します。

表示する前に、次のことを確認してください：

- Cloud Discovery ウィジェットがダッシュボードに追加されている。
- Cloud Discovery 機能が有効になっています。
- ［**読み取り**］権限が、［**一般的な機能：基本機能**］の機能領域で許可されている。

Cloud Discovery ウィジェットを表示するには：

1. Kaspersky Security Center に移動します。
2. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。

   ［**Cloud Discovery**］ウィジェットがダッシュボードに表示されます。
3. ［**Cloud Discovery**］ウィジェットの左側で、クラウドサービスのカテゴリを選択します。

   ウィジェットの右側のテーブルには、選択したカテゴリから、ユーザーが最も頻繁にアクセスを試行するサービスが最大 5 つ表示されます。成功した試行とブロックされた試行の両方がカウントされます。
4. ウィジェットの右側で、特定のサービスを選択します。

   以下の表には、サービスへのアクセスを最も頻繁に試行するデバイスが最大 10 個表示されます。このテーブルでは、成功したアクセス試行に関するレポートとブロックされたアクセス試行に関するレポートの 2 種類のレポートを作成できます。

   さらにこのテーブルでは、特定のデバイスのクラウドサービスへのアクセスをブロックすることも可能です。

ウィジェットには、要求された情報が表示されます。

表示されたウィジェットでは、次の操作を実行できます：

- ［**監視とレポート**］→［**レポート**］セクションに進み、Cloud Discovery レポートを表示します。
- 選択したクラウドサービスへのアクセスをブロックまたは許可します。

ブロック機能は、Kaspersky Security Center EDR Optimum または XDR Expert ライセンスで Kaspersky Security Center をアクティベートした場合のみ使用できます。

ブロック機能は、Kaspersky Endpoint Security 11.2 for Windows 以降を使用している場合にのみ使用できます。以前のバージョンのセキュリティ製品では、クラウドサービスの使用を監視することしかできませんでした。

クラウドサービスのリスクレベル

Cloud Discovery は、クラウドサービスごとにリスクレベルを提供します。リスクレベルは、組織のセキュリティ要件に適合しないサービスを判断するのに役立ちます。たとえば、特定のサービスへのアクセスをブロックするかどうかを決定する時に、リスクレベルを考慮することができます。

リスクレベルは推定指標であり、クラウドサービスの品質やサービス提供元に関しては言及していません。リスクレベルは、カスペルスキーのエキスパートによる推奨事項でしかありません。

クラウドサービスのリスクレベルは、Cloud Discovery ウィジェット、および監視対象のすべてのクラウドサービスのリストに表示されます。

不要なクラウドサービスへのアクセスをブロックする

ユーザーにアクセスさせたくないクラウドサービスへのアクセスをブロックできます。以前にブロックされたクラウドサービスへのアクセスを許可することもできます。

他の考慮事項の中でも、特定のサービスへのアクセスをブロックするかどうかを決定する際に、リスクレベルを考慮に入れることを推奨します。

セキュリティポリシーまたはプロファイルのクラウドサービスへのアクセスをブロックまたは許可できます。

不要なクラウドサービスへのアクセスをブロックする方法は 2 つあります。

- Cloud Discovery ウィジェットを使用する。
  この場合、サービスへのアクセスを 1 つずつブロックできます。
- Kaspersky Endpoint Security for Windows のプロパティを使用する。
  この場合、サービスへのアクセスを 1 つずつブロックすることも、1 つのカテゴリ全体をまとめてブロックすることもできます。
  Kaspersky Endpoint Security for Windows のポリシーのプロパティで Cloud Discovery 機能を有効にする方法について詳しくは、Kaspersky Endpoint Security for Windows のヘルプの［Cloud Discovery］セクションを参照してください。

ウィジェットを使用してクラウドサービスへのアクセスをブロックまたは許可するには：

1. Cloud Discovery ウィジェットを開き、必要なクラウドサービスを選択します。
2. ［**サービスを使用するデバイス上位 10**］ペインで、サービスをブロックまたは許可するセキュリティポリシーまたはプロファイルを見つけます。
3. 必要な行の［**ポリシーまたはプロファイルのアクセスステータス**］列で、次のいずれかを実行します。
   - サービスをブロックするには、ドロップダウンリストで［**ブロック**］を選択します。

- サービスを許可するには、ドロップダウンリストで［**許可**］を選択します。

4. ［**保存**］をクリックします。

選択したサービスへのアクセスは、セキュリティポリシーまたはプロファイルに対してブロックまたは許可されています。

Kaspersky Security Center Web コンソールの動作ログ

Kaspersky Security Center Web コンソールの動作ログを使用すると、ソフトウェアの誤動作の原因を調査するのに役立ちます。お客様から Kaspersky Security Center Web コンソールの誤動作についてカスペルスキーのテクニカルサポートにご連絡をいただく際に、サポート担当者が Kaspersky Security Center Web コンソールのログファイルのご提供をお客様にお願いする場合があります。Kaspersky Security Center Web コンソールのログファイルは、「<Kaspersky Security Center Web コンソールをインストールしたフォルダー>/logs」フォルダーに保存されており、アプリケーションを使用したすべての時間について記録されています。ログファイルは、カスペルスキーのテクニカルサポート担当者へ自動的には送信されません。

Kaspersky Security Center Web コンソールの動作ログを有効にするには：

Kaspersky Security Center Web コンソールのセットアップウィザードの［**Kaspersky Security Center Web コンソールの接続設定**］ウィンドウで、［**Kaspersky Security Center Web コンソールの動作の記録を有効にする**］をオンにします。

ログファイルはテキスト形式です。

ログファイル名は、logs-<コンポーネント名>.<デバイス名>-<ファイルのリビジョン番号>.YYYY-MM-DD という形式です。意味は次の通りです。

- <コンポーネント名> は、Kaspersky Security Center コンポーネントまたは Kaspersky Security Center Web コンソールの管理プラグインの名前です。
- <デバイス名>は、<コンポーネント名> が実行されているホストの名前です。
- <ファイルのリビジョン番号> は、<デバイス名> で動作している <コンポーネント名> について作成されたログファイルの番号です。1日で、同じ <コンポーネント名> と <デバイス名> について複数のログファイルが作成できます。ログファイルの最大サイズは 50 メガバイト（MB）です。最大ファイルサイズに到達すると、新しいフォグファイルが作成されます。新しいログファイルの <ファイルのリビジョン番号> は1ずつ増えていきます。
- YYYY、MM、DD は、ログが最初に作成された年、月、日をそれぞれ示します。新しい日付になると、新しいログファイルが作成されます。

Kaspersky Security Center とその他の製品の連携

このセクションでは、Kaspersky Security Center Web コンソールから Kaspersky Managed Detection and Response など、別のカスペルスキー製品へのアクセスを設定する方法について説明します。また、このセクションでは、SIEM システムへのエクスポートを設定する方法についても説明します。

バックグラウンド接続の確立

Kaspersky Security Center Web コンソールがバックグラウンドタスクを実行できるようにするには、Kaspersky Security Center Web コンソールと管理サーバーの間にバックグラウンド接続を確立する必要があります。使用中のアカウントに［**一般的な機能：ユーザー権限**］機能領域の**オブジェクト ACL の変更**権限がある場合のみ、この接続を確立することができます。

Kaspersky Endpoint Security for Windows 12.6 のプラグインをインストールしている、もしくは Kaspersky Endpoint Security for Windows 11.7 以前のバージョンのプラグインからアップデートしていてバックグラウンド接続が確立されていない場合は、バックグラウンド接続を確立する必要がある旨の通知が表示されます。また、サービスアカウントに［**一般的な機能：管理サーバー上での操作**］機能領域の権限を付与する必要があります。

バックグラウンド接続を確立するには：

1. メインメニューで、［**設定**］→［**連携**］の順にクリックします。
2. ［**連携**］セクションで、バックグラウンド接続を確立するためのスイッチ［**連携用のバックグラウンド接続が［有効］です**］の位置に切り替えます。
3. 表示された［**バックグラウンド接続を有効にする**］セクションで、［OK］をクリックします。

Kaspersky Security Center Web コンソールと管理サーバーのバックグラウンド接続が確立されました。管理サーバーはバックグラウンド接続用のアカウントを作成し、このアカウントは Kaspersky Security Center と別のカスペルスキー製品またはソリューション間での連携を管理するサービスアカウントとして使用されます。このサービスアカウントの名前には NWCSvcUser プレフィックスが含まれます。

セキュリティの理由から、管理サーバーはサービスアカウントのパスワードを 30 日ごとに自動で変更します。サービスアカウントは手動で削除できません。管理サーバーは、サービス連携接続を無効にした際にこのアカウントを自動で削除します。管理サーバーは各管理サーバーに対して単一のサービスアカウントを作成し、すべてのサービスアカウントを「ServiceNwcGroup」という名前のセキュリティグループに割り当てます。管理サーバーはこのセキュリティグループを Kaspersky Security Center のインストールプロセス中に自動で作成します。このセキュリティグループは手動で削除できません。

SIEM システムへのイベントのエクスポート

このセクションでは、SIEM システムへのイベントのエクスポートの設定について説明します。

シナリオ：SIEM システムへのイベントのエクスポートの設定

Kaspersky Security Center で設定可能な方法は次のいずれかです：Syslog 形式を使用する任意の SIEM システムへのエクスポート、LEEF 形式と CEF 形式を使用する QRadar、Splunk、ArcSight SIEM システムへのエクスポート、Kaspersky Security Center データベースからイベントを直接 SIEM システムへエクスポート。このシナリオを完了すると、管理サーバーはイベントを SIEM システムに自動的に送信します。

必須条件

Kaspersky Security Center でイベントのエクスポートの設定を開始する前に：

- イベントのエクスポート方法の詳細を参照してください。
- システムの設定値を確認してください。

このシナリオのステップは、任意の順序で実行できます。

イベントを SIEM システムにエクスポートするプロセスは、次の手順で構成されます：

- **Kaspersky Security Center からイベントを受信するように SIEM システムを設定する**

  手順：SIEM システムへのイベントのエクスポートの設定

- **SIEM システムにエクスポートするイベントの選択：**

  実行手順の説明：

  - 管理コンソール：Syslog 形式でエクスポートするカスペルスキー製品のイベントのマーキング、Syslog 形式でエクスポートする一般的なイベントのマーキング
  - Kaspersky Security Center Web コンソール：Syslog 形式でエクスポートするカスペルスキー製品のイベントのマーキング、Syslog 形式でエクスポートする一般的なイベントのマーキング

- **次のいずれかの方法を使用した、SIEM システムへのイベントのエクスポートの設定：**

  - TCP / IP、UDP、または TLS over TCP プロトコルの使用。

    実行手順の説明：

    - 管理コンソール：SIEM システムへのイベントのエクスポートの設定
    - Kaspersky Security Center Web コンソール：SIEM システムへのイベントのエクスポートの設定

  - Kaspersky Security Center データベースからのイベントの直接エクスポートを使用（データベースでは定義済みのパブリックビューのセットを使用できます。これらのパブリックビューの詳細については、「klakdb.chm のドキュメント」を参照してください）。

結果

SIEM システムへのイベントのエクスポートを構成した後、表示できます 結果のエクスポート エクスポートするイベントを選択した場合。

事前準備

Kaspersky Security Center 管理コンソールでイベントの自動エクスポートを設定する場合は、SIEM システム設定の一部を指定する必要があります。Kaspersky Security Center の設定を準備できるように、SIEM システムの設定を事前に確認しておいてください。

SIEM システムへのイベントの自動送信を正しく設定するには、次の設定の値を把握する必要があります：

- **SIEM システムサーバーアドレス**

  現在使用している SIEM システムがインストールされているサーバーの IP アドレスです。SIEM システム設定でこの値を確認してください。

- **SIEM システムサーバーのポート**

Kaspersky Security Center と SIEM システムサーバー間の接続を確立するために使用するポート番号。Kaspersky Security Center の設定と SIEM システムのレシーバ設定でこの値を指定します。

- **プロトコル**

  Kaspersky Security Center から SIEM システムへのメッセージの送信に使われるプロトコル。Kaspersky Security Center の設定と SIEM システムのレシーバ設定でこの値を指定します。

Kaspersky Security Center のイベントについて

Kaspersky Security Center では、管理サーバーと管理対象デバイスにインストールされた他のカスペルスキー製品の動作中に発生したイベントの情報を受信できます。イベントに関する情報は管理サーバーデータベースに保存されます。この情報は外部 SIEM システムにエクスポートできます。イベント情報を外部 SIEM システムにエクスポートすると、SIEM システムの管理者は、管理対象デバイスまたは管理グループで発生したセキュリティシステムイベントに迅速に対処できます。

イベント種別

Kaspersky Security Center には、次のイベント種別があります：

- 一般イベント：管理対象となるカスペルスキー製品すべてで共通して発生するイベントです。一般イベントの例としては「ウイルスアウトブレイク」があります。一般イベントでは、構文と形式が厳密に定義されています。一般イベントは、レポートやダッシュボードなどで使用されます。
- 管理対象のカスペルスキー製品それぞれに固有のイベント：管理対象となるカスペルスキーの各製品には、独自のイベントのセットがあります。

イベントソース

イベントは、次の製品で生成される可能性があります：

- Kaspersky Security Center のコンポーネント：
  - 管理サーバー
  - ネットワークエージェント
  - iOS MDM サーバー
- 管理対象のカスペルスキー製品

  管理対象のカスペルスキー製品によって生成されるイベントの詳細は、該当する製品のドキュメントを参照してください。

製品によって生成されるイベントの完全なリストは、アプリケーションポリシーの［**イベントの設定**］タブで確認できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示できます。

イベントの重要度

各イベントには固有の重要度があります。発生した状況に応じて、イベントには様々な重要度が割り当てることができます。イベントの重要度には次の 4 つがあります：

- *緊急イベント*は、データの損失、誤動作、または重大なエラーを招きかねない重大な問題が発生したことを示すイベントです。
- *機能エラー*は、アプリケーションの動作中または手順の実行中に重大な問題、エラー、または誤動作の発生を示すイベントです。
- *警告*は、必ずしも重大ではなくても、将来問題が発生する可能性があることを示すイベントです。こうしたイベントの発生後、データや機能を失わずにアプリケーションを復元できるのであれば、ほとんどのイベントは警告を意味します。
- *情報*イベントは、操作が適切に完了したこと、アプリケーションが適切に動作していること、手順が完了したことを伝えるために発生するイベントです。

各イベントには保管期間が定義されており、保管期間中、ユーザーは Kaspersky Security Center でイベントを表示または変更することができます。一部のイベントは既定により、管理サーバーデータベースに保管されません。保管期間がゼロと定義されているためです。管理サーバーデータベースに 1 日以上保管されるイベントだけを外部システムにエクスポートできます。

イベントのエクスポートについて

イベントのエクスポートは、組織および技術レベルでセキュリティ問題に対処し、セキュリティ監視サービスを提供し、各種ソリューションからの情報を統合できる、一元化されたシステム内で使用できます。これらは SIEM システムで、ネットワークのハードウェアとアプリケーション、またはセキュリティオペレーションセンター（SOC）によって生成されたセキュリティアラートとイベントをリアルタイムで分析します。

これらのシステムは、ネットワーク、セキュリティ、サーバー、データベース、アプリケーションなど多くのソースからのデータを受信します。SIEM システムは、重要なイベントを見逃すことがないように、監視対象データを統合する機能も提供します。さらに、緊急のセキュリティ問題を管理者に通知するために、相互に関連するイベントとアラートの分析を自動的に実行します。アラートはダッシュボードから発することも、メールなどのサードパーティのチャネルから送信することもできます。

Kaspersky Security Center から外部 SIEM システムにイベントをエクスポートするプロセスには、イベントの送信元である Kaspersky Security Center とイベントのレシーバである SIEM システムの 2 つが関係します。イベントを正常にエクスポートするには、SIEM システムと Kaspersky Security Center 管理コンソールの両方で設定する必要があります。どちらを先に設定してもかまいません。Kaspersky Security Center 管理コンソールからのイベントの送信を設定してから、SIEM システムによるイベントの受信を設定することも、逆の順序で設定することもできます。

Kaspersky Security Center からのイベントの送信方法

Kaspersky Security Center から外部システムにイベントを送信する方法は 3 つあります：

- Syslog 形式を使用して任意の SIEM システムにイベントを送信

  Syslog プロトコルを使用すると、Kaspersky Security Center 管理サーバーおよび管理対象デバイスにインストールされたカスペルスキー製品で発生したイベントはすべてリレーできます。Syslog プロトコルは、標準メッセージロギングプロトコルです。任意の SIEM システムへのイベントのエクスポートに使用可能です。

  この目的のために、SIEM システムに転送するイベントをマークする必要があります。イベントは、管理コンソールまたは Kaspersky Security Center Web コンソールでマークできます。マークされたイベントのみが SIEM システムに転送されます。何もマークしなかった場合、イベントは転送されません。

- CEF 形式と LEEF 形式を使用して、QRadar システム、Splunk システム、ArcSight システムにイベントを送信

  CEF プロトコルと LEEF プロトコルを使用すると、一般イベントをエクスポートできます。CEF プロトコルと LEEF プロトコル経由でイベントをエクスポートする場合、エクスポートする特定のイベントを選択することはできません。代わりに、一般イベントがすべてエクスポートされます。Syslog プロトコルとは異なり、CEF プロトコルと LEEF プロトコルは汎用的なプロトコルではありません。CEF プロトコルと LEEF プロトコルは、対応する一部の SIEM システム（QRadar、Splunk、ArcSight）用です。そのため、これらの形式のいずれかを使用してイベントをエクスポートする場合は、必要なパーサーを SIEM システム内で使用します。

- Kaspersky Security Center のデータベースから直接、任意の SIEM システムにエクスポート

  このイベントのエクスポート方法では、SQL クエリを使用して、データベースのパブリックビューから直接イベントを受信できます。クエリの結果は XML ファイルに保存されるため、外部システムへの入力データとして使用できます。パブリックビューにあるイベントだけをデータベースから直接エクスポートできます。

SIEM システムによるイベントの受信

SIEM システムは、Kaspersky Security Center からイベントを受信して適切に解析する必要があります。これらの目的に対応できるように、SIEM システムを適切に設定する必要があります。設定は、利用する具体的な SIEM システムによります。ただし、レシーバとパーサーの設定など、すべての SIEM システムの設定で一般的なステップがいくつかあります。

SIEM システムでのイベントのエクスポートの設定について

Kaspersky Security Center から外部 SIEM システムにイベントをエクスポートするプロセスには、イベントの送信元である Kaspersky Security Center とイベントのレシーバである SIEM システムの 2 つが関係します。イベントのエクスポートは、SIEM システムと Kaspersky Security Center 管理コンソールの両方で設定する必要があります。

SIEM システムで指定する設定は、使用している個々のシステムにより異なります。一般に、すべての SIEM システムでレシーバを設定する必要があり、受信イベントを解析するためのメッセージパーサーを任意で設定します。

レシーバの設定

Kaspersky Security Center から送信されたイベントを受信するには、SIEM システムでレシーバを設定する必要があります。一般に、SIEM システムで次の設定を指定する必要があります：

- **エクスポートのプロトコルまたは入力の種別**

  これはメッセージ転送プロトコルで、TCP/IP または UDP のいずれかになります。このプロトコルは、Kaspersky Security Center で指定したプロトコルと同じにする必要があります。

- **ポート**

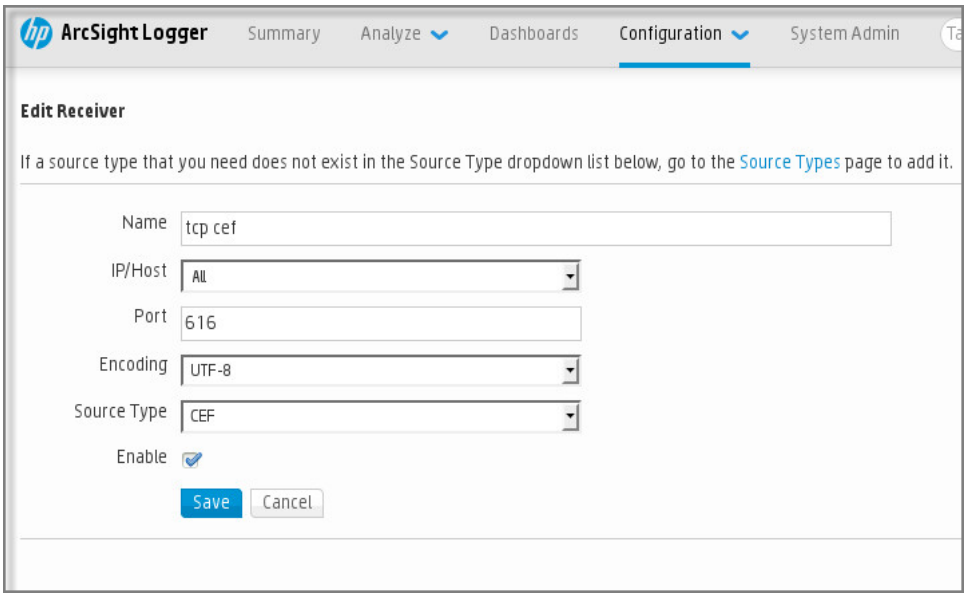
  Kaspersky Security Center に接続するポート番号。このポートは、Kaspersky Security Center で指定したポートと同じにする必要があります。

- **メッセージのプロトコルまたはソースの種別**

  SIEM システムへのイベントのエクスポートに使われるプロトコル。標準プロトコルの Syslog、CEF、または LEEF のいずれかを指定できます。SIEM システムは、指定のプロトコルに従ってメッセージパーサーを選択します。

使用する SIEM システムによっては、受信者の設定を一部追加で指定する必要があります。

次の図は、ArcSight の受信者のセットアップ画面を示します。



ArcSight でのレシーバのセットアップ

メッセージパーサー

エクスポートされたイベントはメッセージとして SIEM システムに渡されます。SIEM システムでイベントに関する情報が利用できるように、これらのメッセージを適切に解析する必要があります。メッセージパーサーは SIEM システムの一部です。イベントの ID、深刻度、説明、パラメータなど関連フィールドにメッセージの内容を分けるために使用します。メッセージの内容を分けることで、SIEM システムは Kaspersky Security Center から受信したイベントを処理して、SIEM システムデータベースに保管することができます。

Syslog 形式で SIEM システムにエクスポートするイベントのマーキング

イベントの自動エクスポートを有効にしたら、外部 SIEM システムにエクスポートするイベントを選択する必要があります。

次の条件のいずれかに基づいて、外部システムへの Syslog 形式でのイベントのエクスポートを設定できます：

- 一般的なイベントのマーキング。イベントの設定または管理サーバーの設定でエクスポートするイベントをポリシー内でマークすると、特定のポリシーで管理されているすべてのアプリケーションで発生した選択済みのイベントが SIEM システムに送信されます。エクスポートされたイベントがポリシー内で選択されている場合、このポリシーで管理されている個別アプリケーションの当該イベントを再定義することはできません。

- 管理対象アプリケーションのイベントのマーキング。管理対象デバイスにインストールされた管理対象アプリケーションへエクスポートするイベントをマークすると、そのアプリケーションで発生したイベントのみが SIEM システムに送信されます。

Syslog 形式で SIEM システムにエクスポートするイベントのマーキングについて

イベントの自動エクスポートを有効にしたら、外部 SIEM システムにエクスポートするイベントを選択する必要があります。

次の条件のいずれかに基づいて、外部システムへの Syslog 形式でのイベントのエクスポートを設定できます：

- 一般的なイベントのマーキング。イベントの設定または管理サーバーの設定でエクスポートするイベントをポリシー内でマークすると、特定のポリシーで管理されているすべてのアプリケーションで発生した選択済みのイベントが SIEM システムに送信されます。エクスポートされたイベントがポリシー内で選択されている場合、このポリシーで管理されている個別アプリケーションの当該イベントを再定義することはできません。

- 管理対象アプリケーションのイベントのマーキング。管理対象デバイスにインストールされた管理対象アプリケーションへエクスポートするイベントをマークすると、そのアプリケーションで発生したイベントのみが SIEM システムに送信されます。

Syslog 形式でエクスポートするカスペルスキー製品のイベントのマーキング

管理対象デバイスにインストールされた特定の管理対象アプリケーションで発生したイベントをエクスポートする場合は、エクスポートするイベントをそのアプリケーションのポリシーでマークします。この場合、マークされたイベントが、ポリシーの範囲に含まれるすべてのデバイスからエクスポートされます。

特定の管理対象アプリケーションからエクスポートするイベントをマークするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. イベントをマークするアプリケーションのポリシーをクリックします。
   ポリシーの設定ウィンドウが表示されます。
3. ［**イベントの設定**］セクションに移動します。
4. SIEM にエクスポートするイベントに隣接するチェックボックスをオンにします。
5. ［**Syslog を使用しての SIEM システムへのエクスポート用にマークする**］をクリックします。

   SIEM システムにエクスポートするイベントは、イベントのリンクをクリックして開く［**イベント登録**］セクションでマーキングすることもできます。

6. チェックマーク（✓）がイベントまたは SIEM システムにエクスポートするためにマーキングしたイベントの［**Syslog**］列に表示されます。
7. ［**保存**］をクリックします。

管理対象アプリケーションからマークされたイベントを、SIEM システムへエクスポーされる準備ができています。

特定の管理デバイスのために、SIEM システムへエクスポートするイベントをマークできます。以前エクスポートしたイベントがアプリケーションのポリシーでマークされた場合、管理対象デバイスのためにマークされたイベントを再定義することはできません。

管理対象デバイスにエクスポートするイベントをマークするには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、必要なデバイスの名前のリンクをクリックします。
   選択したデバイスのプロパティウィンドウが表示されます。
3. ［**アプリケーション**］セクションに移動します。
4. アプリケーションのリストで、必要なアプリケーションの名前のリンクをクリックします。
5. ［**イベントの設定**］セクションに移動します。
6. SIEM にエクスポートするレイベントに隣接するチェックボックスをオンにします。
7. ［**Syslog を使用しての SIEM システムへのエクスポート用にマークする**］をクリックします。

   SIEM システムにエクスポートするイベントは、イベントのリンクをクリックして開く［**イベント登録**］セクションでマークすることもできます。

8. チェックマーク（✓）がイベントまたは SIEM システムにエクスポートするためにマーキングしたイベントの［**Syslog**］列に表示されます。

これで、SIEM システムへのエクスポートが設定済みの場合は、マーキングされたイベントが管理サーバーから SIEM システムへ送信されるようになりました。

Syslog 形式でエクスポートする一般的なイベントのマーキング

Syslog 形式を使用して、管理サーバーが SIEM システムにエクスポートする一般的なイベントをマーキングすることができます。

SIEM システムにエクスポートする一般的なイベントをマークするには：

1. 次のいずれかの手順を実行します：
   - メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   - メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動し、ポリシーのリンクをクリックします。
2. 表示されたウィンドウで、［**イベントの設定**］タブを選択します。
3. ［**Syslog を使用しての SIEM システムへのエクスポート用にマークする**］をクリックします。

   SIEM システムにエクスポートするイベントは、イベントのリンクをクリックして開く［**イベント登録**］セクションでマーキングすることもできます。

4. チェックマーク（✓）がイベントまたは SIEM システムにエクスポートするためにマーキングしたイベントの［**Syslog**］列に表示されます。

これで、SIEM システムへのエクスポートが設定済みの場合は、マーキングされたイベントが管理サーバーから SIEM システムへ送信されるようになりました。

CEF 形式および LEEF 形式を使用したイベントのエクスポート

CEF プロトコルと LEEF プロトコルを使用すると、一般イベントおよびカスペルスキー製品から管理サーバーに送信されたイベントを SIEM システムにエクスポートできます。エクスポートするイベントのセットは事前定義されており、エクスポートするイベントを選択することはできません。

使用している SIEM システムを基にエクスポート形式を選択します。次の表は、SIEM システムおよび対応するエクスポート形式を示します。

SIEM システムへのイベントのエクスポートに使用する形式

SIEM システム	エクスポート形式
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF（ログイベント拡張フォーマット） - IBM Security QRadar SIEM 用にカスタマイズされたイベント形式。QRadar は LEEF イベントを統合、識別、処理できます。LEEF イベントは UTF-8 文字コードを使用する必要があります。LEEF プロトコルの詳細については、IBM Knowledge Center を参照してください。

- CEF（Common Event Format） - 様々なセキュリティとネットワークのデバイス、アプリケーションからのセキュリティ関連情報の相互運用性を改善するオープンログ管理標準。CEF により、共通のイベントログ形式を使用できるため、データを容易に統合して集約し、企業用管理システムで分析できます。CEF イベントは UTF-8 文字コードを使用する必要があります。

自動エクスポートを使用する場合、Kaspersky Security Center から SIEM システムに一般イベントが送信されます。イベントの自動エクスポートは、有効にすると即座に開始されます。このセクションでは、イベントの自動エクスポートを有効にする方法について詳細に説明します。

Syslog 形式を使用したイベントのエクスポートについて

Syslog 形式を使用すると、管理サーバー、管理対象デバイスにインストールされた他のカスペルスキー製品で発生したイベントを SIEM システムにエクスポートできます。

Syslog は標準メッセージロギングプロトコルです。メッセージを生成するソフトウェア、メッセージを保管するシステム、メッセージを報告、分析するソフトウェアを分けることができます。各メッセージには、メッセージを生成したソフトウェアの種別を示す機能コードのラベルが付けられ、重要度が割り当てられます。

Syslog 形式は、インターネット技術タスクフォース（インターネット標準）によって公開されている RFC（Request for Comments）の文書で定義されています。Kaspersky Security Center から外部システムへのイベントのエクスポートには、RFC 5424 標準が使用されます。

Kaspersky Security Center で、Syslog 形式を使用して外部システムにイベントがエクスポートされるように設定できます。

エクスポートのプロセスは次の 2 つのステップで構成されます：

1. イベントの自動エクスポートの有効化。このステップでは、イベントを SIEM システムに送信するように Kaspersky Security Center を設定します。自動エクスポートを有効にすると、Kaspersky Security Center は即座にイベントの送信を開始します。

2. 外部システムにエクスポートするイベントの選択。このステップでは、SIEM システムにエクスポートするイベントを選択します。

イベントを SIEM システムにエクスポートするための Kaspersky Security Center の設定

SIEM システムにイベントをエクスポートするには、Kaspersky Security Center Web コンソールでエクスポートのプロセスを設定する必要があります。

Kaspersky Security Center Web コンソールで SIEM システムへのエクスポートを設定するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**SIEM へエクスポート**］セクションを選択します。

3. ［**設定**］をクリックします。

   ［**エクスポート設定**］セクションが開きます。

4. ［**エクスポート設定**］セクションで設定を指定します：

   - **SIEM システムサーバーアドレス**

     現在使用している SIEM システムがインストールされているサーバーの IP アドレスです。SIEM システム設定でこの値を確認してください。

   - **SIEM システムのポート**

     Kaspersky Security Center と SIEM システムサーバー間の接続を確立するために使用するポート番号。Kaspersky Security Center の設定と SIEM システムのレシーバ設定でこの値を指定します。

   - **プロトコル**

メッセージを SIEM システムに送信するために使用するプロトコルを選択します。TCP/IP、UDP、TCP プロトコルのいずれかを選択できます。

TLS over TCP プロトコルを選択した場合は、次の TLS 設定を指定します：

- **サーバー認証**

  ［**サーバー認証**］フィールドでは、**信頼する証明書**または **SHA フィンガープリント**を選択できます：

  - **信頼できる証明書**：信頼できる証明書認証局（CA）からルート証明書を含む完全な証明書チェーンを受け取り、そのファイルを Kaspersky Security Center にアップロードすることができます。Kaspersky Security Center は、SIEM システムサーバーの証明書チェーンも CA によって署名されているかどうかを確認します。

    信頼できる証明書を追加するには、［**CA 証明書を参照**］をクリックして、証明書をアップロードします。

  - **SHA フィンガープリント**：Kaspersky Security Center で、SIEM システムの完全な証明書チェーン（ルート証明書を含む）の SHA1 サムプリントを指定できます。SHA1 サムプリントを追加するには、［**サムプリント**］フィールドでサムプリントを入力し、［**追加**］をクリックします。

  ［**クライアント認証を追加する**］を使用して、Kaspersky Security Center を認証する証明書を生成することができます。このようにして、Kaspersky Security Center が発行した自己署名証明書を使用します。この場合、SIEM システムサーバーの認証に、信頼できる証明書と SHA フィンガープリントの両方を使用することができます。

- **サブジェクト名 / サブジェクト代替名を追加する**

  サブジェクト名は、証明書を受け取るドメインの名前です。SIEM システムサーバーのドメイン名が SIEM システムサーバー証明書のサブジェクト名と一致しない場合、Kaspersky Security Center は SIEM システムサーバーに接続できません。しかし、SIEM システムサーバーは証明書内で名前が変更された場合にドメイン名を変更することがあります。この場合、サブジェクト名を［**サブジェクト名 / サブジェクト代替名を追加する**］で指定することができます。指定されたサブジェクト名のいずれかが SIEM システム証明書のサブジェクト名と一致する場合、Kaspersky Security Center は SIEM システムサーバー証明書を検証します。

- **クライアント認証を追加する**

  クライアント認証用に、自身の証明書を挿入するか、Kaspersky Security Center で生成することができます。

  - **証明書を挿入する**:CA など、任意の発行元から受け取った証明書を使用できます。次のいずれかの証明書タイプを使用して、証明書とその秘密鍵を指定する必要があります：

    - **X.509 証明書 PEM**：［**証明書のファイル**］フィールドに証明書のファイルをアップロードし、［**鍵のファイル**］フィールドに秘密鍵のファイルをアップロードします。両方のファイルは相互に依存せず、ファイルを読み込む順序は重要ではありません。両方のファイルがアップロードされたら、秘密鍵をデコードするためのパスワードを［**パスワードまたは証明書の検証**］で指定します。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

    - **X.509 証明書 PKCS12**：証明書と秘密鍵を含む単一のファイルを［**証明書のファイル**］フィールドにアップロードします。ファイルをアップロードしたら、秘密鍵をデコードするためのパスワードを［**パスワードまたは証明書の検証**］で指定します。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

- **鍵を生成する**：Kaspersky Security Center で自己署名証明書を生成できます。Kaspersky Security Center は生成された自己署名証明書を保存し、証明書の公開部分または SHA-1 フィンガープリントを SIEM システムに渡すことができます。

- **データ形式**

  SIEM システムの要件に応じて、システムログ、CEF または LEEF 形式を選択できます。

システムログデータ形式を選択した場合は、以下を指定する必要があります。

- **最大メッセージサイズ（バイト）**

  SIEM システムにリレーされた1つのメッセージの最大サイズ（バイト）を指定します。各イベントは1つのメッセージでリレーされます。メッセージの実際の長さが指定の値を上回る場合、メッセージは切り捨てられて、データが失われる可能性があります。既定のサイズは 2048 バイトです。［**プロトコル**］でシステムログ形式を選択した場合にだけ、このフィールドを使用できます。

5. 必要に応じて、管理サーバーデータベースからアーカイブイベントをエクスポートし、アーカイブイベントのエクスポートを開始する日付を設定できます：

   a. ［**エクスポートの開始日を設定**］をクリックします。

   b. 開いたセクションで、［**システムイベントのエクスポートの開始日**］フィールドに開始日を指定します。

   c. ［**OK**］をクリックします。

6. スイッチを［**SIEM システムデータースへのイベントの自動エクスポートが［有効］です**］に切り替えます。

7. SIEM システム接続が正常に設定されていることを確認するには、［**接続の確認**］をクリックします。

   接続のステータスが表示されます。

8. ［**保存**］をクリックします。

SIEM システムへのエクスポートが設定されました。

データベースからのイベントの直接エクスポート

Kaspersky Security Center インターフェイスを使わなくても、Kaspersky Security Center のデータベースから直接イベントを取得できます。パブリックビューに対して直接クエリを実行してイベントデータを取得することも、既存のパブリックビューを基に独自のビューを作成して、必要なデータを取得するようにアドレス指定することもできます。

パブリックビュー

Kaspersky Security Center のデータベースには、パブリックビューの便利なセットをご用意しています。これらのパブリックビューの詳細は、klakdb.chm のドキュメントを参照してください。

v_akpub_ev_event パブリックビューには、データベース内のイベントパラメータを表す一連のフィールドが含まれています。klakdb.chm ドキュメントには、デバイス、アプリケーション、ユーザーなど、他の Kaspersky Security Center のエンティティに対応するパブリックビューに関する情報も含まれています。この情報はクエリに使用できます。

このセクションでは、klsql2 ユーティリティを使って SQL クエリを作成する手順について説明し、クエリの例を示します。

SQL クエリまたはデータベースビューを作成する時には、データベースと連携する他のプログラムも使用できます。Kaspersky Security Center のデータベースへの接続に必要なインスタンス名やデータベース名などのパラメータの表示方法についても、該当セクションを参照してください。

klsql2 ユーティリティを使用した SQL クエリの作成

この記事では、klsql2 ユーティリティをダウンロードして使用する方法、このユーティリティを使用して SQL クエリを作成する方法について説明します。

klsql2 ユーティリティを使用するには：

1. Kaspersky Security Center のインストールフォルダーから klsql2 ユーティリティを配置します。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。Kaspersky Security Center の古いバージョン向けの klsql2 ユーティリティバージョンは使用しないでください。

2. 任意のテキストエディターで src.sql ファイルを作成し、そのファイルをユーティリティと同じフォルダーに配置します。

3. 必要な SQL クエリを src.sql ファイルに入力して、ファイルを保存します。

4. Kaspersky Security Center 管理サーバーがインストールされたデバイスで、次のコマンドをコマンドラインに入力して、src.sql ファイルから SQL クエリを実行し、結果を result.xml ファイルに保存します：
   ```
   klsql2 -i src.sql -u <ユーザー名> -p <パスワード> -o result.xml
   ```
   <ユーザー名>と<パスワード>は、定義データベースにアクセスできるユーザーアカウントの資格情報です。

5. 必要に応じて、データベースにアクセスできるユーザーアカウントのログインとパスワードを入力してください。

6. 新しく作成されたファイル result.xml を開いて、SQL クエリ結果を確認します。

ファイル src.sql を編集して、パブリックビューに対する任意の SQL クエリを作成することができます。次に、コマンドラインから SQL クエリを実行して、結果をファイルに保存します。

klsql2 ユーティリティでの SQL クエリの例

このセクションでは、klsql2 ユーティリティによって作成された SQL クエリの例を示します。

次の例では、過去 7 日間にデバイスで発生したイベントを取得し、発生した順にイベントを表示します。イベントは新しい順から表示されます。

例：
```
SELECT
e.nId, /* イベントの識別子 */
```

```
    e.tmRiseTime, /* イベントが発生した時間 */
    e.strEventType, /* イベント種別の内部名 */
    e.wstrEventTypeDisplayName, /* イベント種別の表示名 */
    e.wstrDescription, /* イベントについて表示される説明 */
    e.wstrGroupName, /* デバイスが配置されているグループの名前 */
    h.wstrDisplayName, /* イベントが発生したデバイスの表示名 */
    CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
    CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
    CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
    CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* イベントが発生したデバイスの IP アドレス */
    FROM v_akpub_ev_event e
    INNER JOIN v_akpub_host h ON h.nId=e.nHostId
    WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
    ORDER BY e.tmRiseTime DESC
```

Kaspersky Security Center データベース名の表示

SQL Server、MySQL、MariaDB のいずれかのデータベース管理ツールで Kaspersky Security Center のデータベースにアクセスする場合は、SQL スクリプトエディターから接続できるようにその定義データベースの名前を調べる必要があります。

Kaspersky Security Center のデータベースの名前を表示するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（ ）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**現在のデータベースの詳細**］セクションを選択します。

   データベース名は［**データベース名**］フィールドに指定されます。このデータベース名を使用して、SQL クエリ内のデータベースのアドレスを指定します。

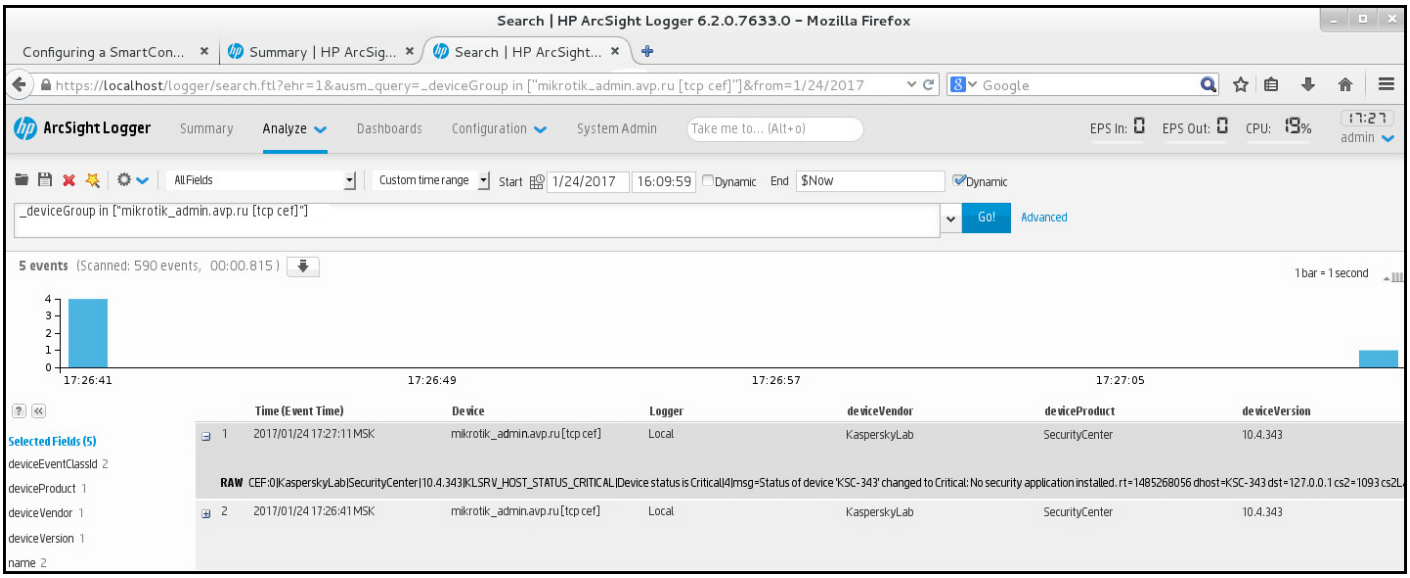
エクスポート結果の表示

イベントのエクスポート手順が正常に完了するようにコントロールすることができます。それには、イベントのエクスポートとともにメッセージが SIEM システムで受信されているかどうかを確認します。

Kaspersky Security Center から送信されたイベントが SIEM システムで受信され、適切に解析されている場合、設定は両者で適切に行われています。イベントが受信されない場合は、Kaspersky Security Center で指定した設定を SIEM システムの設定と比べて確認してください。

次の図は、ArcSight にエクスポートされたイベントを示します。たとえば、最初のイベントは重大な管理サーバーイベントです：「*デバイスのステータスが「緊急」です。*」

エクスポートされたイベントの SIEM システムでの表示は、使用している SIEM システムによって異なります。



イベントの例

クラウド環境での Kaspersky Security Center Web コンソールの操作

このセクションでは、Amazon Web Services、Microsoft Azure、Google Cloud などのクラウド環境での Kaspersky Security Center の導入とメンテナンスに関わる Kaspersky Security Center Web コンソールの機能について説明します。

クラウド環境での動作には、専用のライセンスが必要です。専用のライセンスがない場合、クラウドデバイスに関係するインターフェイス要素は表示されません。

Kaspersky Security Center Web コンソールのクラウド環境設定

クラウド環境設定ウィザードを使用して Kaspersky Security Center を構成する場合に必要な項目は次の通りです：

- クラウド環境用の特定の資格情報：
  - クラウドセグメントをポーリングする権限が付与された IAM ロールまたはクラウドセグメントをポーリングする権限が付与された IAM ユーザーアカウント（Amazon Web Services で使用する場合）
  - Azure アプリケーション ID パスワードとサブスクリプション（Microsoft Azure で使用する場合）
  - Google クライアントのメールアドレス、プロジェクト ID、秘密鍵（Google Cloud で使用する場合）
- インストールパッケージ：
  - Windows 用のネットワークエージェント
  - Linux 用のネットワークエージェント
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux の Web プラグイン

- 次のうち少なくとも1つ：
  - Kaspersky Endpoint Security for Windows のインストールパッケージと Web プラグイン（推奨）
  - Kaspersky Security for Windows Server のインストールパッケージと Web プラグイン

使用準備済みイメージから Kaspersky Security Center を導入する場合、管理コンソールを介して管理サーバーへの最初の接続時に、クラウド環境設定ウィザードが自動的に開始されます。また、ウィザードはいつでも手動で起動できます。

クラウド環境設定ウィザードを手動で起動するには：

メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**クラウド環境の設定**］の順に移動します。

ウィザードが起動します。

クラウド環境の設定の平均作業時間は約 15 分です。

ステップ1：必要なプラグインとインストールパッケージのチェック

以下にリストされている必要な Web プラグインとインストールパッケージがすべてある場合、この手順は表示されません。

クラウド環境の構成には、次のコンポーネントが必要です：

- インストールパッケージ：
  - Windows 用のネットワークエージェント
  - Linux 用のネットワークエージェント
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux の Web プラグイン
- 次のうち少なくとも1つ：
  - Kaspersky Endpoint Security for Windows のインストールパッケージと Web プラグイン（推奨）
  - Kaspersky Security for Windows Server のインストールパッケージと Web プラグイン

    Kaspersky Security for Windows Server の代わりに、Kaspersky Endpoint Security for Windows を使用することを推奨します。

Kaspersky Security Center は、既にあるコンポーネントを自動的に検出し、不足しているコンポーネントのみをリスト表示します。［**ダウンロードするアプリケーションを選択**］をクリックし、必要なプラグインとインストールパッケージを選択して、一覧表示されたコンポーネントをダウンロードします。コンポーネントのダウンロード後、［**更新**］を使用して不足しているコンポーネントのリストを更新できます。

ステップ 2：製品のライセンス管理

BYOL AMI を使用していて、Kaspersky Security for Virtualization のライセンスまたは Kaspersky Hybrid Cloud Security のライセンスで製品をアクティベーションしていない場合にのみ、このステップは表示されます。

ライセンスを指定し、［**次へ**］をクリックして先に進みます。

指定したライセンスが管理サーバーの保管領域に追加されます。

再びウィザードを実行しても、このステップは表示されません。

ステップ 3：クラウド環境と認証の選択

このセクションでは、Kaspersky Security Center のバージョン 12.1 以降でのみ利用できる機能について説明しています。

次の設定を指定します：

- **クラウド環境**

  Kaspersky Security Center を導入するクラウド環境を選択します：AWS、Azure、または Google Cloud。

  複数のクラウド環境を使用する場合は、1 つの環境を選択してもう一度ウィザードを実行します。

- **接続名**

  接続の名前を入力します。名前を 256 文字以上にすることはできません。Unicode 文字のみを使用できます。

  この名前はクラウドデバイスの管理グループの名前としても使用されます。

  複数のクラウド環境を使用する予定の場合は、たとえば「Azure Segment」「AWS Segment」「Google Segment」のように、環境の名前を接続名に含めることを検討してください。

認証情報を入力し、指定したクラウド環境での認証を受信します。

AWS

AWS をクラウドセグメントの種別として選択した場合、クラウドセグメントをさらにポーリングするには、IAM ロールまたは AWS IAM アクセスキーが必要です。

- **EC2 インスタンスに割り当てられた AWS IAM ロール**

  IAM ロール、および管理サーバーに必要な権限がある場合は、このオプションを選択します。

- **AWS IAM ユーザー**

  AWS IAM アクセスキーがある場合は、このオプションを選択します。キーデータを入力します：

  - **アクセスキーの ID**

    IAM アクセスキーの ID（英数字の並び）：IAM ユーザーアカウント作成時に受け取ったキーの ID です。

    このフィールドは、IAM ロールではなく AWS IAM アクセスキーを認証のために選択した場合に使用できます。

  - **秘密鍵**

    IAM ユーザーアカウント作成時にアクセスキーの ID と一緒に受け取った秘密鍵です。

    秘密鍵の文字はアスタリスクで表示されます。秘密鍵を入力し始めると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを必要な間だけ押し続けます。

    このフィールドは、IAM ロールではなく AWS IAM アクセスキーを認証のために選択した場合に使用できます。

    入力した文字を表示するには、［**表示**］を押し続けます。

Azure

Azure をクラウドセグメントの種別として選択した場合は、クラウドセグメントの今後のポーリングに使用する接続について、以下の設定を指定します：

- **Azure アプリケーション ID**

  Azure ポータルで作成したアプリケーション ID です。

  ポーリングやその他の目的で使用する Azure アプリケーション ID を 1 つだけ指定できます。別の Azure セグメントでポーリングを実行する場合は、既存の Azure 接続を事前に削除する必要があります。

- **Azure サブスクリプション ID**

  Azure ポータルで作成したサブスクリプションです。

- **Azure アプリケーションパスワード**

  アプリケーション ID の作成時に取得したアプリケーション ID のパスワードです。

  パスワードの文字はアスタリスクで表示されます。パスワードの入力を開始すると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを押し続けます。

  入力した文字を表示するには、［**表示**］を押し続けます。

- **Azure ストレージアカウント名**

  Kaspersky Security Center で使用するために作成した Azure ストレージアカウントの名前です。

- **Azure ストレージのアクセスキー**

  パスワード（アクセスキー）は Kaspersky Security Center で使用する Azure ストレージアカウントを作成した時に取得したものです。

  キーは、Azure ストレージアカウントの概要セクションのアクセスキーに関するサブセクションで確認できます。

  入力した文字を表示するには、［**表示**］を押し続けます。

Google Cloud

Google Cloud をクラウドセグメントの種別として選択した場合は、クラウドセグメントの今後のポーリングに使用する接続について、以下の設定を指定します：

- **クライアントメールアドレス**

  クライアントのメールアドレスは、Google Cloud でプロジェクトの登録に使用したメールアドレスです。

- **プロジェクト ID**

  プロジェクト ID は、Google Cloud でプロジェクトの登録時に取得した ID です。

- **秘密鍵**

  秘密鍵は、Google Cloud でプロジェクトの登録時に秘密鍵として取得した文字列です。間違えないように、この文字列をコピーして貼り付けることを検討してください。

  入力した文字を表示するには、［**表示**］を押し続けます。

この指定した接続は本製品の設定に保存されます。

クラウド環境設定ウィザードでは、1セグメントのみ指定可能です。後で追加の接続を指定して、他のクラウドセグメントを管理することもできます。

［**次へ**］をクリックして先に進みます。

ステップ 4：セグメントのポーリング、クラウドとの同期設定および次に実行する処理の選択

このステップでは、クラウドセグメントのポーリングが開始され、クラウドデバイス専用の管理グループが自動的に作成されます。ポーリング中に検出されたデバイスはこのグループに配置されます。クラウドセグメントのポーリングスケジュールがが設定されます（既定では 5 分ごとです。後で設定を変更できます）。

未割り当てデバイスを自動的に移動する［**クラウドと同期**］ルールも作成されます。以降、クラウドネットワークがスキャンされるたびに、検出された仮想デバイスは［**管理対象デバイス**］の［**クラウド**］グループ内の対応するサブグループに移動されます。

次の設定を定義します：

- **管理グループをクラウドの階層構造と同期**

  このオプションをオンにすると、［**クラウド**］グループが自動的に［**管理対象デバイス**］グループ内に作成され、クラウドデバイスの検索が開始されます。クラウドネットワークの各スキャンによって検出されたインスタンスと仮想マシンは、クラウドグループ内に配置されます。このグループ内の管理サブグループの構造は、クラウドセグメントの構造に対応します（AWS では、アベイラビリティーゾーンとプレイスメントグループは構造に反映されません。Azure では、サブネットは構造に反映されません）。クラウド環境のインスタンスとして識別されていないデバイスは**未割り当てデバイス**グループに分類されます。このグループ構造を使用して、インストールタスクをグループ化してアンチウイルス製品をインスタンスにインストールし、グループごとに異なるポリシーを設定することができます。

  このチェックボックスをオフにしても、**クラウド**グループは作成され、デバイスの検索も開始されます。ただし、クラウドセグメントの構造に対応するサブグループはグループ内で作成されません。検出されたすべてのインスタンスは**クラウド**管理グループに属しているため、1つのリストに表示されます。同期を必要とする Kaspersky Security Center を使用している場合、［**クラウドと同期**］ルールのプロパティを編集し、このルールを強制的に実行することもできます。このルールを強制的に適用すると、クラウドセグメントの構造と一致するようにクラウドグループ内のサブグループの構造が変更されます。

  既定では、このオプションはオフです。

- **保護の導入**

  このオプションをオンにすると、セキュリティ製品をインスタンスにインストールするためのタスクをウィザードで作成します。ウィザードが終了すると、製品導入ウィザードが自動的にクラウドセグメント内のデバイス上で起動するため、ユーザーはネットワークエージェントとセキュリティ製品をこれらのデバイスにインストールできます。

  Kaspersky Security Center にはこれらの導入時に利用できるネイティブツールが用意されています。EC2 インスタンスまたは Azure 仮想マシンにアプリケーションにインストールに必要な権限が付与されていない場合、**リモートインストール**タスクを手動で構成し、必要な権限が付与されたアカウントを指定できます。この場合、AWS API または Azure API を使用して検出されたデバイスではリモートインストールタスクを利用できません。このタスクは Active Directory、Windows ドメイン、IP アドレス範囲のいずれかのポーリングを使用して検出されたデバイスで利用できます。

  このオプションをオフにすると、製品導入ウィザードは起動せず、セキュリティ製品をインスタンスにインストールするタスクは作成されません。これらの操作は両方とも、後で手動で実行することができます。

［保護の導入］オプションを選択すると、［**デバイスの再起動**］セクションが使用可能になります。このセクションでは、対象デバイスのオペレーティングシステムがいつ再起動するかを選択する必要があります。アプリケーションのインストール中に、デバイスのオペレーティングシステムを再起動する場合の処理を選択します：

- **再起動しない**

  このオプションをオンにすると、セキュリティ製品のインストール後にデバイスが再起動されません。

- **再起動**

  このオプションをオンにすると、セキュリティ製品のインストール後にデバイスが再起動されます。

［**次へ**］をクリックして先に進みます。

Google Cloud では、製品の導入は Kaspersky Security Center ネイティブツールを使用してのみ行うことができます。Google Cloud を選択した場合、［**保護の導入**］は使用できません。

ステップ 5：ポリシーとタスクを作成するアプリケーションの選択

この手順は、 Kaspersky Endpoint Security for Windows と Kaspersky Security for Windows Server の両方のインストールパッケージとプラグインがある場合にのみ表示されます。これらのアプリケーションの 1 つのみのプラグインとインストールパッケージがある場合、この手順はスキップされ、Kaspersky Security Center は既存のアプリケーションのポリシーとタスクを作成します。

ポリシーとタスクを作成するアプリケーションを選択します：

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

ステップ 6：Kaspersky Security Center の Kaspersky Security Network の設定

Kaspersky Security Center の動作に関する情報を Kaspersky Security Network（KSN）ナレッジベースに転送する設定を指定します。次のいずれかのオプションをオンにします：

- **Kaspersky Security Network への参加に同意する**

  Kaspersky Security Center とクライアントデバイスにインストールされている管理対象製品は、自動的に動作情報を Kaspersky Security Network に送信します。Kaspersky Security Network への参加により、ウイルスなどの脅威に関する情報を含んだデータベースのアップデートをより迅速に入手できるため、セキュリティへの緊急の脅威にすぐに対応できます。

- **Kaspersky Security Network への参加に同意しない**

  Kaspersky Security Center と管理対象製品は、Kaspersky Security Network に対して情報を提供しません。

  このオプションをオンにすると、Kaspersky Security Network の使用がオフになります。

カスペルスキーは、Kaspersky Security Network への参加を推奨しています。

管理対象アプリケーション向けの KSN の使用に同意するかどうかの選択も表示されます。Kaspersky Security Network の使用に同意する場合、管理対象アプリケーションからカスペルスキーへデータが送信されます。Kaspersky Security Network の使用に同意しない場合、管理対象アプリケーションはカスペルスキーへデータを送信しません。（アプリケーションのポリシーで後から設定を変更できます。）

［**次へ**］をクリックして先に進みます。

ステップ 7： 保護の初期設定の作成

作成されたポリシーとタスクのリストを確認できます。

ポリシーとタスクの作成が完了するのを待ってから、［**次へ**］をクリックして進みます。ウィザードの最後のページで、［**終了**］をクリックして終了します。

Kaspersky Security Center Web コンソールを使用したネットワークセグメントのポーリング

AWS API ツール、Azure API ツールまたは Google API ツールを使用した、クラウドセグメントに対する定期的なポーリングによって、ネットワーク構造とそのネットワーク内のデバイスに関する情報が管理サーバーで受信されます。Kaspersky Security Center は、この情報を使用して、［未割り当てデバイス］フォルダーと［管理対象デバイス］フォルダーの内容を更新します。デバイスが管理グループに自動的に移動するように設定している場合、検出されたデバイスは管理グループに含まれます。

管理サーバーにクラウドセグメントのポーリングを許可するには、対応する権限を IAM ロールまたは IAM ユーザーアカウント（AWS の場合）、アプリケーション ID とパスワード（Azure の場合）、あるいは Google クライアントのメール、Google プロジェクト ID および秘密鍵によって付与する必要があります。

各クラウドセグメント用に接続を追加したり削除したりできます。また、各クラウドセグメントのポーリングスケジュールを設定することもできます。

クラウドセグメントのポーリングに使用する接続を追加する

利用可能な接続のリストにクラウドセグメントのポーリングに使用する接続を追加するには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**クラウド**］の順に移動します。
2. 表示されたウィンドウで［**プロパティ**］をクリックします。
3. 表示されたウィンドウの［**設定**］で、［**追加**］をクリックします。
   ［**クラウドセグメントの設定**］ウィンドウが表示されます。
4. クラウドセグメントのポーリングに使用する接続について、クラウド環境の名前を指定します：
   - **クラウド環境**

     Kaspersky Security Center を導入するクラウド環境を選択します：AWS、Azure、または Google Cloud。

     複数のクラウド環境を使用する場合は、1 つの環境を選択してもう一度ウィザードを実行します。

   - **接続名**

     接続の名前を入力します。名前を 256 文字以上にすることはできません。Unicode 文字のみを使用できます。

     この名前はクラウドデバイスの管理グループの名前としても使用されます。

     複数のクラウド環境を使用する予定の場合は、たとえば「Azure Segment」「AWS Segment」「Google Segment」のように、環境の名前を接続名に含めることを検討してください。
5. 認証情報を入力し、指定したクラウド環境での認証を受信します。

- AWS を選択した場合は、次の設定を指定してください：
  - **AWS IAM ロールを使用**

    既に AWS サービスで使用する管理サーバー用 IAM ロールを作成している場合、このオプションを選択します。

  - **AWS IAM ユーザーアカウントの資格情報**

    必要な権限がある IAM ユーザーアカウントがある場合、このオプションを選択し、キーの ID と秘密鍵を入力します。

    ［AWS IAM ユーザーアカウントの資格情報］を指定した場合は、以下を指定します：

    - **アクセスキーの ID**

      IAM アクセスキーの ID（英数字の並び）：IAM ユーザーアカウント作成時に受け取ったキーの ID です。

      このフィールドは、IAM ロールではなく AWS IAM アクセスキーを認証のために選択した場合に使用できます。

    - **秘密鍵**

      IAM ユーザーアカウント作成時にアクセスキーの ID と一緒に受け取った秘密鍵です。

      秘密鍵の文字はアスタリスクで表示されます。秘密鍵を入力し始めると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを必要な間だけ押し続けます。

      このフィールドは、IAM ロールではなく AWS IAM アクセスキーを認証のために選択した場合に使用できます。

    入力した文字を表示するには、［**表示**］を押し続けます。

- Azure を選択した場合は、次の設定を指定してください：
  - **Azure アプリケーション ID**

    Azure ポータルで作成したアプリケーション ID です。

    ポーリングやその他の目的で使用する Azure アプリケーション ID を 1 つだけ指定できます。別の Azure セグメントでポーリングを実行する場合は、既存の Azure 接続を事前に削除する必要があります。

  - **Azure サブスクリプション ID**

    Azure ポータルで作成したサブスクリプションです。

  - **Azure アプリケーションパスワード**

アプリケーション ID の作成時に取得したアプリケーション ID のパスワードです。

パスワードの文字はアスタリスクで表示されます。パスワードの入力を開始すると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを押し続けます。

入力した文字を表示するには、［**表示**］を押し続けます。

- **Azure ストレージアカウント名**

  Kaspersky Security Center で使用するために作成した Azure ストレージアカウントの名前です。

- **Azure ストレージのアクセスキー**

  パスワード（アクセスキー）は Kaspersky Security Center で使用する Azure ストレージアカウントを作成した時に取得したものです。

  キーは、Azure ストレージアカウントの概要セクションのアクセスキーに関するサブセクションで確認できます。

  入力した文字を表示するには、［**表示**］を押し続けます。

Google Cloud を選択した場合は、次の設定を指定してください：

- **クライアントメールアドレス**

  クライアントのメールアドレスは、Google Cloud でプロジェクトの登録に使用したメールアドレスです。

- **プロジェクト ID**

  プロジェクト ID は、Google Cloud でプロジェクトの登録時に取得した ID です。

- **秘密鍵**

  秘密鍵は、Google Cloud でプロジェクトの登録時に秘密鍵として取得した文字列です。間違えないように、この文字列をコピーして貼り付けることを検討してください。

  入力した文字を表示するには、［**表示**］を押し続けます。

6. 必要に応じて、［**ポーリングのスケジュールを設定する**］をクリックし、既定の設定を変更します。

この接続は本製品の設定に保存されます。

追加したクラウドセグメントの初回ポーリング後、このセグメントに対応するサブグループが［**管理対象デバイス**］の［**クラウド**］管理グループに表示されます。

誤った資格情報を指定した場合、クラウドセグメントのポーリング中、インスタンスは検出されず、新しいサブグループは［**管理対象デバイス**］の［**クラウド**］管理グループに表示されません。

クラウドセグメントのポーリングに使用した接続を削除する

特定のクラウドセグメントをポーリングする必要がなくなった場合、利用可能な接続リストから、そのセグメントに対応する接続を削除できます。また、クラウドセグメントをポーリングするための権限が別の認証情報を持つ IAM ユーザーに移された場合にも、接続を削除できます。

接続を削除するには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**クラウド**］の順に移動します。
2. 表示されたウィンドウで［**プロパティ**］をクリックします。
3. 表示された［**設定**］ウィンドウで、削除するセグメントの名前をクリックします。
4. ［**削除**］をクリックします。
5. 表示されたウィンドウで、［OK］をクリックして処理を確定します。

接続が削除されます。この接続と対応しているクラウドセグメント内のデバイスが、管理グループから自動的に削除されます。

Kaspersky Security Center Web コンソールを使用したポーリングスケジュールの設定

クラウドセグメントのポーリングは、スケジュールに従って実行されます。ポーリングの頻度が設定可能です。

ポーリング頻度は、クラウド環境の設定で自動的に 5 分に設定されています。この値はいつでも変更でき、別のスケジュールを設定することができます。ポーリングの実行を 5 分間隔より多い頻度に設定しないでください。AWS API 操作にエラーが生じる可能性があります。

クラウドセグメントのポーリングスケジュールを設定するには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**クラウド**］の順に移動します。
2. 表示されたウィンドウで［**プロパティ**］をクリックします。
3. 表示された［**設定**］ウィンドウで、ポーリングスケジュールを設定するセグメントの名前をクリックします。
   ［**クラウドセグメントの設定**］ウィンドウが表示されます。
4. ［**クラウドセグメントの設定**］ウィンドウで、［**ポーリングのスケジュールを設定する**］をクリックします。
   ［**スケジュール**］ウィンドウが表示されます。
5. ［**スケジュール**］ウィンドウで、次の設定を指定します：
   - **実行予定**
     ポーリングスケジュールのオプション：
     - **N 日ごと**

指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。
既定では、現在のシステム日時から、1日ごとにポーリングが実行されます。

- N分ごと

  指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。
  既定では、現在のシステム時刻から、5分ごとにポーリングが実行されます。

- 曜日ごと

  指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。
  既定では、毎週金曜日の午後6時にポーリングが実行されます。

- 毎月、選択した週の指定日

  毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。
  既定では、月内のいかなる日付も選択されておらず、開始時刻は午後6時です。

- **開始までの間隔**

  Nに相当する分または日数を指定します。

- **開始時刻**

  初回のポーリングを開始する時間を指定します。

- **未実行のタスクを実行する**

  ポーリングの実行がスケジュールされていた時刻に管理サーバーがオフまたは接続できなかった場合は、管理サーバーがオンになった時に即座にポーリングを実行させるか、ポーリングの次回のスケジュールまで待機するかを選択できます。

  このオプションをオンにすると、管理サーバーがオンになるとすぐにポーリングを開始します。

  このオプションをオフにすると、管理サーバーはポーリングの次回のスケジュールまでポーリングの実行を待機します。

  既定では、このオプションはオンです。

6. 変更を保存します。

セグメントのポーリングスケジュールが設定され保存されます。

Kaspersky Security Center Web コンソールを使用したクラウドセグメントのポーリング結果の表示

クラウドセグメントのポーリング結果を確認できます。管理サーバーの管理対象であるクラウドデバイスのリストを表示して確認します。

クラウドセグメントのポーリング結果を表示するには：

メインメニューで、［**検出と製品の導入**］→［**検出**］→［**クラウド**］の順に移動します。

ポーリングが可能なクラウドセグメントが表示されます。

Kaspersky Security Center Web コンソールを使用したクラウドデバイスのプロパティの表示

各クラウドデバイスのプロパティを表示できます。

クラウドデバイスのプロパティを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
2. プロパティを表示するデバイスの名前をクリックします：
   プロパティウィンドウの［**全般**］セクションが表示されます。
3. 特定のクラウドデバイスのプロパティを表示する場合は、［**システム**］セクションをプロパティウィンドウで選択します。
   デバイスのクラウドプラットフォームに応じたプロパティが表示されます。
   AWS のデバイスでは、次のプロパティが表示されます：
   - **API を使用して検出されたデバイス**（値：**AWS**）
   - **クラウドのリージョン**
   - **クラウドの VPC**
   - **クラウドのアベイラビリティーゾーン**
   - **クラウドのサブネット**
   - **クラウドのプレイスメントグループ**（AWS API を使用して検出された Amazon EC2 インスタンスの場合のみ。それ以外の場合、この項目は表示されません）

   Azure のデバイスでは、次のプロパティが表示されます：
   - **API を使用して検出されたデバイス**（値：**Microsoft Azure**）
   - **クラウドのリージョン**
   - **クラウドのサブネット**

   Google Cloud のデバイスでは、次のプロパティが表示されます：
   - **API を使用して検出されたデバイス**（値：**Google Cloud**）

- **クラウドのリージョン**
- **クラウドの VPC**
- **クラウドのアベイラビリティーゾーン**
- **クラウドのサブネット**

クラウドとの同期：移動ルールの設定

クラウド環境の設定の操作中に、［クラウドと同期］ルールが自動的に作成されます。このルールにより、各ポーリング中に見つかったデバイスが［未割り当てデバイス］グループから［管理対象デバイス］の［クラウド］グループに自動的に移動されるため、デバイスを一元管理することが可能になります。既定では、ルールは作成後にアクティブになります。ルールはいつでも無効にしたり、実行したりすることができます。

［クラウドと同期］ルールのプロパティを変更する、またはルールを実行するには：

1. メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**移動ルール**］の順に選択します。
   移動ルールのリストが開きます。
2. 移動ルールのリストで、［**クラウドと同期**］を選択します。
   ルールのプロパティウィンドウが開きます。
3. 必要に応じて、［**クラウドセグメント**］タブの［**ルールの条件**］タブで次の設定を指定します：

- **デバイスがクラウドセグメント内にある**

  選択したクラウドセグメント内にあるデバイスにのみルールが適用されるようになります。オフにすると、検出されたすべてのデバイスにルールが適用されます。

  既定では、このオプションがオンです。

- **子オブジェクトも含む**

  選択されたセグメント内およびネストされたすべてのクラウドサブセクション内の全デバイスにルールが適用されるようになります。オフにすると、ルートセグメント内にあるデバイスにのみルールが適用されます。

  既定では、このオプションがオンです。

- **デバイスをネストされたオブジェクトから対応するサブグループに移動する**

  このオプションをオンにすると、ネストされたオブジェクトのデバイスがその構造に対応するサブグループに自動的に移動します。

  このオプションをオフにすると、ネストされたオブジェクトのデバイスがクラウドサブグループのルートに移動し、ルートより下の分岐は行われません。

  既定では、このオプションはオンです。

- **新しく検出されたデバイスの配置階層に対応するサブグループを作成する**

このオプションをオンにすると、デバイスが含まれるセクションに対応するサブグループが［**管理対象デバイス**］の［**クラウド**］グループの階層構造にない場合は、Kaspersky Security Center で対応するサブグループが作成されます。たとえば、デバイスの検索中に新しいサブネットが検出された場合、同じ名前のグループが［**管理対象デバイス**］の［**クラウド**］グループの下に新規に作成されます。

このオプションをオフにすると、Kaspersky Security Center で新しいサブグループは作成されません。たとえば、ネットワークのポーリング中に新しいサブネットが検出された場合、［**管理対象デバイス**］の［**クラウド**］グループにサブネットと同じ名前のグループが新規に作成されることはなく、サブネットに含まれていたデバイスは［**管理対象デバイス**］の［**クラウド**］グループに移動されます。

既定では、このオプションはオンです。

- **クラウドセグメントで何も検出されなかったサブグループを削除する**

  このチェックボックスをオンにすると、既存のクラウドオブジェクトのセクションに対応していないすべてのサブグループがクラウドグループから削除されます。

  このオプションをオフにすると、既存のクラウドオブジェクトのセクションに対応しないサブグループもすべて保持されます。

  既定では、このオプションはオンです。

［**管理グループをクラウドの階層構造と同期**］をクラウド環境の設定を使用してオンにすると、［**クラウドと同期**］ルールが［**新しく検出されたデバイスの配置階層に対応するサブグループを作成する**］および［**クラウドセグメントで何も検出されなかったサブグループを削除する**］がオンな状態で作成されます。

［**管理グループをクラウドの階層構造と同期**］を有効にしなかった場合、［**クラウドと同期**］ルールが、これらのオプションが無効な（クリアされた）状態で作成されます。お使いの Kaspersky Security Center で、［**管理対象デバイス**］の［**クラウド**］サブグループ内にあるサブグループの構造とクラウドセグメントの構造が一致する必要がある場合、［**新しく検出されたデバイスの配置階層に対応するサブグループを作成する**］と［**クラウドセグメントで何も検出されなかったサブグループを削除する**］を有効にして、ルールを実行します。

4. ［**API を使用して検出されたデバイス**］から、次のいずれかの値を選択します：

   - ［**いいえ**］。デバイスは AWS API、Azure API、Google API のいずれでも検知できません。これはデバイスがクラウド環境外にあるか、クラウド環境内にあるが何らかの理由により API では検出できないことを意味します。
   - **AWS**：AWS API を使用して検出されたデバイスで、これはデバイスが間違いなく AWS クラウド環境にあることを意味します。
   - **Azure**：Azure API を使用して検出されたデバイスで、これはデバイスが間違いなく Azure クラウド環境にあることを意味します。
   - **Google Cloud**:Google API を使用して検出されたデバイスで、これはデバイスが間違いなく Google クラウド環境にあることを意味します。
   - 値なし：この基準は適用できません。

5. 必要に応じて、他のセクションで他のルールのプロパティを設定します。

移動ルールが設定されます。

Azure 仮想マシンへの製品のリモートインストール

Microsoft Azure 仮想マシンに製品をインストールするには、有効なライセンスが必要です。

Kaspersky Security Center では次の使用シナリオがサポートされます。

- クライアントデバイスが Azure API によって検出され、製品のインストールも API によって実行される。Azure API を使用すると、次のアプリケーションのみをインストールできます：
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- クライアントデバイスが Azure API によって検出され、製品のインストールはディストリビューションポイントによって実行されるか、ディストリビューションポイントがない場合は、スタンドアロンインストールパッケージを使用して手動で実行される。この方法では、Kaspersky Security Center でサポートされている任意の製品をインストールできます。

Azure 仮想マシンで製品のリモートインストールタスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。
3. ウィザードの指示に従います：
   a. ［**アプリケーションのリモートインストール**］をタスク種別として選択します。
   b. ［**インストールパッケージ**］ページで、［**Microsoft Azure API によるリモートインストール**］を選択します。
   c. デバイスにアクセスするアカウントを選択する際は、既存の Azure アカウントを使用するか、［**追加**］をクリックして Azure アカウントの資格情報を入力します：
      - **Azure アカウント名**

        指定する資格情報の任意の名前を入力します。タスクを実行するアカウントのリストにこの名前が表示されます。

      - **Azure アプリケーション ID**

        Azure ポータルで作成したアプリケーション ID です。

        ポーリングやその他の目的で使用する Azure アプリケーション ID を 1 つだけ指定できます。別の Azure セグメントでポーリングを実行する場合は、既存の Azure 接続を事前に削除する必要があります。

      - **Azure アプリケーションパスワード**

アプリケーション ID の作成時に取得したアプリケーション ID のパスワードです。

パスワードの文字はアスタリスクで表示されます。パスワードの入力を開始すると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを押し続けます。

d. ［**管理対象デバイス**］の［**クラウド**］グループから目的のデバイスを選択します。

ウィザードが完了すると、アプリケーションのリモートインストール用のタスクがタスクのリストに表示されます。

管理サーバーデータのバックアップタスクをクラウドの DBMS を使用して作成

バックアップタスクは管理サーバーのタスクです。クラウド環境にある DBMS（AWS　または Azure）を使用する場合はバックアップタスクを作成します。

管理サーバーのデータバックアップタスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。
3. ウィザードの最初のページで、［**アプリケーション**］リストから［**Kaspersky Security Center 15.1**］を選択し、［**タスク種別**］リストから［**管理サーバーデータのバックアップ**］を選択します。
4. ウィザードの対応するページで、次の情報を指定します：
   - AWS のデータベースを使用している場合：
     - **S3 バケット名**

       バックアップ用に作成した S3 バケットの名前です。

     - **アクセスキーの ID**

       S3 バケットストレージインスタンスを使用するために IAM ユーザーアカウントを作成した時に受け取ったキーの ID（英数字の並び）です。

       このフィールドは、S3 バケット上の RDS データベースを選択した場合に使用可能になります。

     - **秘密鍵**

IAM ユーザーアカウント作成時にアクセスキーの ID と一緒に受け取った秘密鍵です。

秘密鍵の文字はアスタリスクで表示されます。秘密鍵を入力し始めると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを必要な間だけ押し続けます。

このフィールドは、IAM ロールではなく AWS IAM アクセスキーを認証のために選択した場合に使用できます。

- Microsoft Azure のデータベースを使用している場合：
  - **Azure ストレージアカウント名**

    Kaspersky Security Center で使用するために作成した Azure ストレージアカウントの名前です。

  - **Azure サブスクリプション ID**

    Azure ポータルで作成したサブスクリプションです。

  - **Azure パスワード**

    アプリケーション ID の作成時に取得したアプリケーション ID のパスワードです。

    パスワードの文字はアスタリスクで表示されます。パスワードの入力を開始すると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを押し続けます。

  - **Azure アプリケーション ID**

    Azure ポータルで作成したアプリケーション ID です。

    ポーリングやその他の目的で使用する Azure アプリケーション ID を 1 つだけ指定できます。別の Azure セグメントでポーリングを実行する場合は、既存の Azure 接続を事前に削除する必要があります。

  - **Azure SQL サーバー名**

    この名前とリソースグループは Azure SQL サーバーのプロパティで確認できます。

  - **Azure SQL サーバーリソースグループ**

    この名前とリソースグループは Azure SQL サーバーのプロパティで確認できます。

  - **Azure ストレージのアクセスキー**

    情報はストレージアカウントのプロパティの［アクセスキー］セクションで確認できます。いずれのキー（key1 または key2）も使用できます。

タスクが作成され、タスクリストに表示されます。［**タスクの作成が完了したらタスクの詳細を表示する**］を有効にすると、既定のタスク設定をタスクの作成後にすぐに変更できます。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

クライアントデバイスのリモート診断

Windows ベースと Linux ベースのクライアントデバイス上での次の操作のリモート実行についてリモート診断を使用できます：

- トレースの有効化と無効化、トレースレベルの変更、トレースファイルのダウンロード
- システム情報とアプリケーション設定のダウンロード
- イベントログのダウンロード
- アプリケーションのダンプファイルの生成
- 診断の開始および診断レポートのダウンロード
- アプリケーションの起動、停止、再起動

クライアントデバイスからダウンロードしたイベントログと診断レポートを、管理者自身による問題のトラブルシューティングに活用できます。また、テクニカルサポートにお問い合わせいただいた場合、テクニカルサポートの担当者がより詳細な分析を行うために、トレースファイル、ダンプファイル、イベントログ、診断レポートをクライアントデバイスからダウンロードするように求められる場合もあります。

リモート診断ウィンドウを開く

Windows ベースと Linux ベースのクライアントデバイスのリモート診断を実行するには、リモート診断ウィンドウを開く必要があります。

リモート診断ウィンドウを開くには：

1. リモート診断ウィンドウを開くデバイスを選択するには、次のいずれかを実行します：
   - デバイスが管理グループに属している場合は、メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
   - デバイスが未割り当てデバイスグループに属している場合は、メインメニューで、［**検出と製品の導入**］→［**未割り当てデバイス**］の順に移動します。
2. 目的のデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**詳細**］タブをクリックします。
4. 表示されたウィンドウで、［**リモート診断**］をクリックします。
   クライアントデバイスの［**リモート診断**］ウィンドウが開きます。管理サーバーとクライアントデバイス間の接続が確立されていない場合、エラーメッセージが表示されます。

あるいは、Linux ベースのクライアントデバイスに関するすべての診断情報を一度に取得する必要がある場合は、このデバイスで collect.sh スクリプトを実行できます。

アプリケーションのトレースの有効化と無効化

Xperf トレースを含む、アプリケーションのトレースを有効または無効にできます。

トレースの有効化および無効化

リモートデバイスでのトレースを有効または無効にするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。
   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。
3. アプリケーションリストで、トレースを有効または無効にするアプリケーションを選択します。
   リモート診断オプションのリストが表示されます。
4. トレースを有効にする場合：
   a. ［**トレース**］セクションで［**トレースを有効化**］をクリックします。
   b. ［**トレースレベルを変更**］ウィンドウで表示される設定の既定値は変更しないことを推奨します。設定値の編集が必要な場合は、テクニカルサポート担当者が必要な変更をご案内します。次の設定を使用できます：
      - **トレースレベル**
        トレースレベルでは、トレースファイルに含める情報の詳細度を指定できます。
      - **ローテーションありトレース**
        トレース情報を上書きし、トレースファイルのサイズが過剰に大きくなるの防止します。トレース情報を保存するために使用できるファイルの最大数と、各ファイルの最大サイズを指定します。トレースファイルの数が指定した最大数と同じになり、書き込み中のファイルのサイズが指定した最大サイズに達すると、新しいトレースファイルを作成できるように最も古いトレースファイルが削除されます。

        ローテーションありトレースは、Kaspersky Endpoint Security でのみ使用可能です。
   c. ［**保存**］をクリックします。

選択したアプリケーションのトレースが有効になります。場合によっては、トレースを有効にするには、セキュリティ製品とタスクを再起動しなければならないことがあります。

Linux ベースのクライアントデバイスでは、ネットワークエージェントコンポーネントのアップデーターのトレースは、ネットワークエージェント設定によって規制されます。したがって、Linux を実行しているクライアントデバイスでは、このコンポーネントに対して［**トレースを有効化**］および［**トレースレベルを変更**］がオフになっています。

5. 選択したアプリケーションのトレースを無効にする場合は、［**トレースを無効化**］をクリックします。
   選択したアプリケーションのトレースが無効になります。

Xperf トレースの有効化

Kaspersky Endpoint Security では、テクニカルサポート担当者がシステムのパフォーマンス情報の Xperf トレースを有効にするようにお願いする場合があります。

Xperf トレースを有効にして設定するか、無効にするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。
   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。
3. アプリケーションのリストから Kaspersky Endpoint Security for Windows を選択します。
   Kaspersky Endpoint Security for Windows のリモート診断オプションのリストが表示されます。
4. ［**Xperf トレース**］セクションで［**Xperf トレースを有効化**］をクリックします。
   Xperf トレースが既に有効になっている場合、［**Xperf トレースを無効化**］が代わりに表示されます。Kaspersky Endpoint Security for Windows の Xperf トレースを無効にする場合は、このボタンをクリックしてください。
5. ［**Xperf トレースのレベルを変更**］ウィンドウが開くので、テクニカルサポート担当者からの依頼内容に応じて、次の操作を実行してください：
   a. 次のいずれかのトレースレベルを選択します：
      - **低レベル**

        この種別のトレースファイルには、システムに関する最小限の量の情報が含まれています。
        既定では、このオプションがオンです。

      - **高レベル**

        この種別のトレースファイルには*低レベル*のトレースファイルより詳細な情報が含まれています。*低レベル*のトレースファイルではパフォーマンスを十分に評価できない場合などに、テクニカルサポートの担当者から提出を求められることがあります。*高レベル*のトレースファイルには、ハードウェア、オペレーティングシステム、プロセスとアプリケーションの開始と終了のリスト、パフォーマンスの評価に使用されたイベント、Windows システム評価ツールからのイベントなどに関する情報を含む技術情報が含まれます。

   b. 次のいずれかの Xperf トレース種別を選択します：
      - **基本**

        Kaspersky Endpoint Security の動作中にトレース情報が取得されます。
        既定では、このオプションがオンです。

- **再起動時**

  管理対象デバイスでのオペレーティングシステムの起動時にトレース情報を受信します。このトレース種別は、デバイスが起動してから Kaspersky Endpoint Security が起動するまでの間にシステムパフォーマンスに影響を与える問題が発生している場合に使用すると効果的です。

［**ローテーションファイルのサイズ（MB）**］を有効にし、トレースファイルのサイズが過剰に大きくなるのを防止するように依頼される場合もあります。続いて、トレースファイルの最大サイズを設定します。ファイルが指定した最大サイズに達すると、最も古いトレース情報が削除され、新しい情報が上書きされます。

c. ローテーションするファイルサイズを定義します。

d. ［**保存**］をクリックします。

Xperf トレースが有効になり設定されます。

6. Kaspersky Endpoint Security for Windows の Xperf トレースを無効にする場合は、［**Xperf トレース**］セクションの［**Xperf トレースを無効化**］をクリックしてください。

Xperf トレースが無効になります。

アプリケーションのトレースファイルのダウンロード

アプリケーションのトレースファイルをダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。

   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。
3. アプリケーションのリストで、トレースファイルをダウンロードするアプリケーションを選択します。
4. ［**トレース**］セクションで、［**トレースファイル**］をクリックします。

   トレースファイルのリストが表示された［**デバイスのトレースログ**］ウィンドウが開きます。
5. ダウンロードするファイルをトレースファイルのリストから選択します。
6. 次のいずれかの手順を実行します：

   - ［**ダウンロード**］をクリックして、選択したファイルをダウンロードします。ダウンロードするファイルを 1 つまたは複数選択できます。
   - 選択したファイルの一部をダウンロード：

     a. ［**一部をダウンロード**］をクリックします。

     複数のファイルの一部を同時にダウンロードすることはできません。複数のトレースファイルを選択すると、［**一部をダウンロード**］がオフになります。

     b. ウィンドウが開いたら、名前を指定し、必要に応じてダウンロードするファイルの部分を指定します。

Linux ベースのデバイスの場合、ファイル部分名の編集は使用できません。

c. ［**ダウンロード**］をクリックします。

選択したファイル、またはその一部が指定の場所にダウンロードされます。

トレースファイルの削除

不要になったトレースファイルを削除することができます。

トレースファイルを削除するには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. 表示された［モート診断］ウィンドウで、［**イベントログ**］タブを選択します。
3. ［**トレースファイル**］セクションで、削除するトレースファイルに応じて［**Windows Update ログ**］または［**リモートインストールログ**］をクリックします。

［**Windows Update ログ**］は、Windows ベースのクライアントデバイスでのみ使用できます。

トレースファイルのリストが表示された［**デバイスのトレースログ**］ウィンドウが開きます。

4. 削除するファイルをトレースファイルのリストから1つまたは複数選択します。
5. ［**削除**］をクリックします。

選択したトレースファイルが削除されます。

アプリケーション設定のダウンロード

クライアントデバイスからアプリケーション設定をダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。
3. ［**アプリケーション設定**］セクションで［**ダウンロード**］をクリックして、クライアントデバイスにインストールされたアプリケーションの設定に関する情報をダウンロードします。

情報を含む ZIP アーカイブが指定された場所にダウンロードされます。

イベントログのダウンロード

リモートデバイスからイベントログをダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。

2. ［リモート診断］ウィンドウの［**イベントログ**］タブで、［**全デバイスのログ**］をクリックします。

3. ［**全デバイスのログ**］ウィンドウで、関連するログを1つまたは複数選択します。

4. 次のいずれかの手順を実行します：

- ［**ファイル全体をダウンロード**］をクリックして、選択したログをダウンロードします。
- 選択したログの一部をダウンロード：

a. ［**一部をダウンロード**］をクリックします。
複数のログの一部を同時にダウンロードすることはできません。複数のイベントログを選択すると、［**一部をダウンロード**］がオフになります。

b. ウィンドウが開いたら、名前を指定し、必要に応じてダウンロードするログの部分を指定します。
Linux ベースのデバイスの場合、ログ部分名の編集は使用できません。

c. ［**ダウンロード**］をクリックします。

選択したイベントログ、またはその一部が指定の場所にダウンロードされます。

アプリケーションの起動、停止、再起動

クライアントデバイス上でアプリケーションを起動、停止、再起動することができます。

アプリケーションを起動、停止、再起動するには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。

2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。
［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。

3. アプリケーションのリストで、起動、停止、または再起動するアプリケーションを選択します。

4. 次のいずれかのボタンをクリックして処理を選択します：

- **アプリケーションの停止**
アプリケーションが現在実行されていないと、このボタンは使用できません。
- **アプリケーションの再開**
アプリケーションが現在実行されていないと、このボタンは使用できません。
- **アプリケーションの開始**
アプリケーションの実行が現在停止されていないと、このボタンは使用できません。

選択した処理に応じて、必要なアプリケーションがクライアントデバイス上で起動、停止、再起動します。

ネットワークエージェントを再起動すると、デバイスと管理サーバーとの現在の接続が失われることを伝えるメッセージが表示されます。

Kaspersky Security Center ネットワークエージェントのリモート診断を実行し、結果をダウンロードする

リモートデバイスで Kaspersky Security Center ネットワークエージェントの診断を開始し、結果をダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。

   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。
3. アプリケーションのリストで、［**Kaspersky Security Center ネットワークエージェント**］を選択します。

   リモート診断オプションのリストが表示されます。
4. ［**診断レポート**］セクションで［**診断を実行**］をクリックします。

   リモート診断が開始され、診断レポートが生成されます。診断が完了すると、［**診断レポートをダウンロード**］が使用可能になります。
5. ［**診断レポートをダウンロード**］をクリックしてレポートをダウンロードします。

レポートが指定した場所にダウンロードされます。

クライアントデバイスでのアプリケーションの実行

場合によっては、テクニカルサポートの担当者の指示に従って、クライアントデバイス上でアプリケーションを実行する必要があります。そのデバイスにアプリケーションをインストールする必要はありません。

クライアントデバイス上でアプリケーションを実行するには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. ［リモート診断］ウィンドウで［**リモートでアプリケーションを実行**］タブを選択します。
3. ［**アプリケーションファイル**］セクションで、［**参照**］をクリックして、クライアントデバイス上で実行するアプリケーションを含む ZIP アーカイブを選択します。

   > ZIP アーカイブにはユーティリテフォルダーが含まれている必要があります。このフォルダーには、リモートデバイスで実行する実行ファイルが含まれています。

   必要に応じて、実行ファイル名とコマンドラインの引数を指定できます。これを行うには、**リモートデバイス上で実行されるアーカイブ内の実行ファイル**と［**コマンドラインの引数**］フィールドに入力します。
4. ［**アップロードして実行**］をクリックして、クライアントデバイス上で指定したアプリケーションを実行します。
5. カスペルスキーのサポート担当者の指示に従ってください。

アプリケーションのダンプファイルの生成

アプリケーションダンプファイルを使用すると、ある時点でクライアントデバイスで実行されているアプリケーションのパラメータを表示できます。このファイルには、アプリケーション用にロードされたモジュールに関する情報も含まれています。

Linux ベースのデバイスからのダンプファイルの取得はサポートされていません。

リモート診断を通じてダンプファイルを取得するには、kldumper ユーティリティを使用します。このユーティリティは、テクニカルサポートの専門家の要求に応じて、カスペルスキー製品のプロセスのダンプファイルを取得するように設計されています。kldumper ユーティリティの使用要件に関する詳細情報は、Kaspersky Security Center ナレッジベースに記載されています。

アプリケーションのダンプファイルを生成するには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. ［リモート診断］ウィンドウで［**リモートでアプリケーションを実行**］タブを選択します。
3. ［**ダンプファイルの生成**］セクションで、ダンプファイルを生成するアプリケーションの実行ファイルを指定します。
4. ［**ダンプファイルをダウンロード**］をクリックします。

   指定されたアプリケーションのダンプファイルを含むアーカイブがダウンロードされます。

   指定されたアプリケーションがクライアントデバイス上で実行されていない場合、ダウンロードされたアーカイブに含まれる「結果」フォルダーは空になります。

   指定されたアプリケーションが実行中であるにもかかわらず、ダウンロードがエラーで失敗したり、ダウンロードしたアーカイブに含まれる［結果］フォルダーが空の場合は、Kaspersky Security Center ナレッジベースを参照してください。

Linux ベースのクライアントデバイスでのリモート診断の実行

Kaspersky Security Center を使用すると、クライアントデバイスから基本的な診断情報をダウンロードできます。あるいは、カスペルスキーの collect.sh スクリプトを使用して、Linux ベースのデバイスに関する診断情報を取得することもできます。このスクリプトは、診断が必要な Linux ベースのクライアントデバイス上で実行され、診断情報、このデバイスのシステム情報、アプリケーションのトレースファイル、デバイスログ、および緊急終了したアプリケーションのダンプファイルを含むファイルを生成します。

collect.sh スクリプトを使用して、Linux ベースのクライアントデバイスに関するすべての診断情報を一度に取得することを推奨します。Kaspersky Security Center を通じて診断情報をリモートでダウンロードする場合は、リモート診断インターフェイスのすべてのセクションを実行する必要があります。また、Linux ベースのデバイスの診断情報は完全には取得されない可能性があります。

生成された診断情報を含むファイルをカスペルスキーテクニカルサポートに送信する必要がある場合は、ファイルを送信する前にすべての機密情報を削除してください。

collect.sh スクリプトを使用して Linux ベースのクライアントデバイスから診断情報をダウンロードするには、次の手順を実行します：

1. collect.sh スクリプトをダウンロードする アーカイブ collect.tar.gz に含まれています。
2. ダウンロードしたアーカイブを、診断する必要がある Linux ベースのクライアントデバイスにコピーします。
3. 次のコマンドを実行して、アーカイブ collect.tar.gz を解凍します：

   ```
   # tar -xzf collect.tar.gz
   ```

4. 次のコマンドを実行して、スクリプトの実行権限を指定します：

   ```
   # chmod +x collect.sh
   ```

5. 管理者権限を持つアカウントを使用して、collect.sh スクリプトを実行します：

   ```
   # ./collect.sh
   ```

診断情報を含むファイルが生成され、フォルダー /tmp/$HOST_NAME-collect.tar.gz に保存されます。

隔離とバックアップからのファイルのダウンロードと削除

このセクションでは、Kaspersky Security Center Web コンソールでファイルをダウンロードする方法、および隔離とバックアップからファイルを削除する方法について説明します。

隔離とバックアップからのファイルのダウンロード

次の 2 つの条件のいずれかが満たされた場合にのみ、隔離とバックアップからファイルをダウンロードできます：［**管理サーバーから切断しない**］がオンになっているか、接続ゲートウェイが使用されている。いずれの条件も満たさない場合は、ダウンロードできません。

隔離またはバックアップにあるファイルのコピーをハードディスクに保存するには：

1. 次のいずれかの手順を実行します：
   - Quarantineからファイルのコピーを保存するには、メインメニューで、［**操作**］→［**リポジトリ**］→［**隔離**］の順に移動します。
   - バックアップからファイルのコピーを保存するには、メインメニューで、［**操作**］→［**リポジトリ**］→［**バックアップ**］の順に移動します。
2. 表示されるウィンドウで、ダウンロードするファイルを選択し、［**ダウンロード**］をクリックします。

ダウンロードが開始されます。クライアントデバイスで隔離に配置されたファイルのコピーが、指定したフォルダーに保存されます。

隔離、バックアップ、またはアクティブな脅威リポジトリからのオブジェクトの削除について

クライアントデバイスにインストールされているカスペルスキーのセキュリティ製品がオブジェクトを隔離、バックアップ、またはアクティブな脅威リポジトリに配置すると、追加されたオブジェクトに関する情報が［**隔離**］、［**バックアップ**］、または Kaspersky Security Center の［**アクティブな脅威**］セクションに送信されます。これらのセクションのいずれかを開いた際に、リストからオブジェクトを選択して［**削除**］ボタンをクリックすると、Kaspersky Security Center は次のいずれかのアクションまたは両方の処理を実行します：

- 選択したオブジェクトをリストから削除する
- 選択したオブジェクトをリポジトリから削除する

実行する処理は、選択したオブジェクトをリポジトリに配置したカスペルスキー製品によって定義されます。カスペルスキー製品は、［**エントリを追加したアプリケーション**］フィールドで指定されています。実行する処理の詳細については、カスペルスキー製品のマニュアルを参照してください。

Kaspersky Security Center Web コンソールインターフェースの言語の変更

Kaspersky Security Center Web コンソールインターフェイスの言語を選択できます。

インターフェイス言語を変更するには：

1. メインメニューで、［**設定**］→［**言語**］の順にクリックします。
2. サポートされているローカリゼーション言語のいずれかを選択します。

API リファレンスガイド

この Kaspersky Security Center OpenAPI リファレンスガイドは、次のタスクを支援する目的で作成されています：

- 自動化とカスタマイズ。管理コンソールを使用して、手動で扱う必要がないタスクを自動化できます。管理コンソールでサポートされていないシナリオの実装も可能です。たとえば、管理者として Kaspersky Security Center OpenAPI を使用し、管理グループ構造の作成を支援するスクリプトを作成、実行することで、その構造の最新の状態を維持できます。

- カスタム開発。たとえば、クライアント用に操作を制限した代替の MMC ベースの管理コンソールを開発できます。

OpenAPI リファレンスガイドでは、画面右側の検索フィールドを使用して必要な情報を検索できます。

OPENAPI リファレンスガイド（英語）

スクリプトのサンプル

OpenAPI リファレンスガイドには、次の表に示す Python スクリプトのサンプルが含まれています。これらのサンプルは、OpenAPI メソッドを呼び出して、ネットワークを保護するための様々なタスクを自動的に実行する方法を示しています。たとえば、「プライマリ」と「セカンダリ」の階層の作成、Kaspersky Security Centerでのタスクの実行、ディストリビューションポイントの割り当てなどの方法です。サンプルをそのまま実行することも、サンプルを基に独自のスクリプトを作成することもできます。

OpenAPI メソッドを呼び出してスクリプトを実行するには：

1. KlAkOAPI.tar.gz アーカイブをダウンロードします。このアーカイブには、KlAkOAPI パッケージとサンプルが含まれています（アーカイブまたは OpenAPI リファレンスガイドからコピーできます）。KlAkOAPI.tar.gz アーカイブは、Kaspersky Security Center のインストールフォルダーにもあります。

2. 管理サーバーがインストールされているデバイス上の KlAkOAPI.tar.gz アーカイブから KlAkOAPI パッケージをインストールします。

   OpenAPI メソッドを呼び出し、サンプルや独自のスクリプトを実行するのは、管理サーバーと KlAkOAPI パッケージがインストールされているデバイスでのみ実行できます。

ユーザーシナリオと Kaspersky Security Center OpenAPI メソッドのサンプルの一致

サンプル	サンプルの目的	シナリオ
KlAkParams のログ記録	`KlAkParams` データ構造を使用してデータを抽出、処理できます。サンプルには、このデータ構造の使用方法を示しています。 サンプル出力は、様々な方法で表示される場合があります。データを取得して HTTP メソッドを送信したり、自分のコードで使用したりできます。	監視とレポート
プライマリ / セカンダリ階層の作成と削除（英語）	管理サーバーをセカンダリ管理サーバーとして追加し、プライマリとセカンダリの階層を確立できます。または、セカンダリ管理サーバーを階層から切断することもできます。	• 管理サーバーの階層の作成：セカンダリ管理サーバーの追加 • 管理サーバーの階層の削除
Active Directory 単位に基づく構造のグループ階層の作成	Active Directory 単位をポーリングして、検出されたデバイスグループの階層を形成できます。	管理グループの作成

キャッシュされた Active Directory 単位に基づく構造のグループ階層の作成	以前にポーリングされた Active Directory 単位に基づいて、管理対象デバイスグループの階層を形成できます。最後のポーリング後に新しいデバイスが Active Directory に表示された場合、それらは保存されたポーリング結果に含まれていないため、グループに追加されません。	管理グループの作成
接続ゲートウェイを使用してネットワークリストファイルを指定したデバイスにダウンロード	接続ゲートウェイを使用して、必要なデバイスでネットワークエージェントに接続できます。次に、ネットワークリストを含むファイルをデバイスにダウンロードします。	ディストリビューションポイントと接続ゲートウェイの調整
プライマリ管理サーバーリポジトリに保存されたライセンスのセカンダリ管理サーバーへのインストール	プライマリ管理サーバーに接続し、そこから必要なライセンスをダウンロードして、このライセンスを階層内のすべてのセカンダリ管理サーバーに送信できます。	管理対象アプリケーションのライセンスの管理
有効なユーザー権限のレポートの作成	様々なレポートを作成できます。たとえば、このサンプルを使用して、有効なユーザー権限のレポートを生成できます。このレポートでは、ユーザーのグループと役割に応じて、ユーザーが持つ権限について説明します。 レポートは、HTML、PDF、Excel 形式でダウンロードできます。	レポートの生成と表示
デバイスでのタスクの開始	接続ゲートウェイを使用して、必要なデバイスでネットワークエージェントに接続できます。次に必要なタスクを実行します。	タスクの手動での開始
Active Directory のサイトおよびサービスに基づいた IP サブネットの作成（英語）	使用する Active Directory 単位に基づいて IP サブネットを作成できます。 サンプルは、指定された IP 範囲のポーリングを開始し、検出されたサブネットを削除して、新しいサブネットとの競合を回避します。したがって、サブネットの保存が重要なネットワークでは、このサンプルを実行しないでください。 ポーリング後、サンプルは Active Directory を参照し、その中のすべてのデバイスを調査して、IP サブネットを作成します。これを実行するために、サンプルはすべてのデバイスのマスクと IP アドレスを使用します。	ネットワーク保護の設定
デバイスのディストリビューションポイントのグループへの登録（英語）	管理対象デバイスをディストリビューションポイント（以前はアップデートエージェントと呼ばれていました）として割り当てることができます。	定義データベースとカスペルスキー製品のアップデート
すべてのグループの列挙（英語）	管理グループに対して、様々な処理を実行できます。サンプルでは、次の実行方法を例示しています： • ［管理対象デバイス］ルートグループの識別子の取得 • グループ階層の移動 • グループの完全な拡張階層を、名前とネスト構造とともに取得	管理サーバーの設定
タスクの列挙、タスクの統計のクエリ、タスクの実行（英語）	参照可能な情報は次の通りです： • タスクの進捗履歴 • 現在のタスクステータス • 様々なステータスのタスクの数 タスクの実行も可能です。既定では、サンプルは統計の出力後にタスクを実行します。	タスク実行の監視
タスクの作成と実行（英語）	タスクを作成できます。サンプルにある次のタスクパラメータを指定します： • 種別 • 実行方法 • 名前 • タスクが使用されるデバイスグループ 既定では、サンプルは「メッセージを表示する」種別のタスクを作成します。このタスクは、管理サーバーのすべての管理対象デバイスに対して実行できます。必要に応じて、タスクパラメータを独自に指定できます。	タスクの作成
ライセンスの列挙（英語）	管理サーバーが管理するデバイスにインストールされたカスペルスキー製品の、現在のライセンスがすべてリストされた一覧を取得できます。リストには、全ライセンスの詳細データ（名前、種別、有効期限日など）が含まれています。	使用中のライセンスに関する情報の表示

内部ユーザーの作成および検索（英語）	さらなる作業のためにアカウントを作成できます。	管理サーバーを開始するアカウントの選択
カスタムカテゴリの作成（英語）	必要なパラメータとともに、アプリケーションカテゴリを作成できます。	コンテンツが手動で追加されるアプリケーションカテゴリの作成
SrvView を使用したユーザーの列挙（英語）	SrvView クラスを使用して、管理サーバーからの詳細な情報をリクエストできます。たとえば、このサンプルを使用してユーザーのリストを取得できます。	ユーザーアカウントの管理

OpenAPI 経由で Kaspersky Security Center と連携するアプリケーション

一部のアプリケーションは、OpenAPI 経由で Kaspersky Security Center と連携します。Kaspersky Anti Targeted Attack Platform または Kaspersky Security for Virtualization などがこのようなアプリケーションに含まれます。また、OpenAPI に基づいて開発されたカスタムクライアントアプリケーションであることもあります。

OpenAPI 経由で Kaspersky Security Center と連携するアプリケーションは管理サービスに接続します。管理サーバーへの接続用に IP アドレスの許可リストを設定している場合は、Kaspersky Security Center の OpenAPI を使用するアプリケーションをインストールしているデバイスの IP アドレスを追加してください。使用しているアプリケーションが OpenAPI によって動作しているかどうかについては、そのアプリケーションのヘルプを参照してください。

導入と設定に関する推奨事項

このセクションでは、Kaspersky Security Center の導入方法と使用方法について説明します。

アプリケーションの導入、設定、および使用方法についての推奨事項を確認いただけます。また、アプリケーションの操作に関する一般的な問題を解決する方法についても説明しています。

Kaspersky Security Center を導入するにあたって

組織のネットワークに Kaspersky Security Center コンポーネントを導入する計画がある場合は、プロジェクトのサイズと範囲を考慮する必要があります。特に、次の要素を重視してください：

- デバイスの合計数
- MSP クライアントの数

1 台の管理サーバーで最大 100,000 台のデバイスをサポートできます。組織ネットワーク上に合計で 100,000 台を超えるデバイスが存在する場合は、サービスプロバイダー側で複数の管理サーバーを導入し、階層化して一元的に管理する必要があります

1 台の管理サーバーで最大 500 の仮想サーバーを作成できます。このため、MSP クライアント 500 ごとに管理サーバー 1 台が必要です。

導入計画段階では、管理サーバーに対して特別な X.509 証明書を割り当てることを検討する必要があります。管理サーバーに対する X.509 証明書の割り当てが有効になるのは、次の場合です（部分的なリスト）：

- SSL Termination プロキシを使用して、セキュアソケットレイヤー（SSL）トラフィックをスキャンする場合
- 証明書で必要な値を指定する場合
- 証明書で必要な暗号化強度を指定する場合

管理サーバーへのインターネットアクセス

クライアントネットワーク上のデバイスにインターネット経由での管理サーバーへのアクセスを許可するためには、次の管理サーバーのポートを使用できるようにする必要があります：

- 13000 TCP — クライアントネットワークに導入されたネットワークエージェントを接続するための管理サーバーの TLS ポート
- 8061 TCP — 管理コンソールツールを使用したスタンドアロンパッケージの公開用 HTTPS ポート
- 8060 TCP — 管理コンソールツールを使用したスタンドアロンパッケージの公開用 HTTP ポート
- 13292 TCP — 管理が必要なモバイルデバイスがある場合のみ必要とされる TLS ポート

Kaspersky Security Center Web コンソールを使用して、ネットワーク管理の基本オプションをクライアントに提供する必要がある場合は、Kaspersky Security Center Web コンソールのポート 8080 TCP（HTTPS ポート）を開く必要があります。

Kaspersky Security Center 標準設定

1台または複数台の管理サーバーを MSP のサーバーに導入します。管理サーバーの数は、使用可能なハードウェア、MSP クライアントの合計数、または管理対象デバイスの合計数に基づき選択可能です。

1台の管理サーバーで最大 100,000 台のデバイスをサポートできます。導入後に管理対象デバイスを増やす可能性がある場合は、1台の管理サーバーに接続するデバイスの数を少なくしておきます。

1台の管理サーバーで最大 500 の仮想サーバーを作成できます。このため、MSP クライアント 500 ごとに管理サーバー1台が必要です。

複数台のサーバーを使用する場合は、1つの階層に統合してください。管理サーバーの階層を使用することによりポリシーとタスクが重複するのを防ぎ、管理対象デバイスの全セットを1台の管理サーバーで管理している場合と同様に処理できます。つまり、デバイスの検索、デバイス選択の構築、レポートの作成などの処理です。

MSP クライアントに対応する各仮想サーバー上で、ディストリビューションポイントを1台または複数台、割り当てる必要があります。MSP クライアントと管理サーバーがインターネットを経由して接続されている場合は、ディストリビューションポイントで、*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを作成しておくことが有用な場合があります。これにより、管理サーバーからではなくカスペルスキーのサーバーから直接アップデートをダウンロードできるようになります。

MSP クライアントネットワーク内のデバイスの一部がインターネットに直接アクセスできない場合、ディストリビューションポイントをゲートウェイモード接続に切り替える必要があります。この場合、MSP クライアントネットワーク上のデバイスのネットワークエージェントは、直接ではなくゲートウェイを介して管理サーバーに接続され、緊密に同期します。

ほとんどの場合、管理サーバーは MSP クライアントネットワークをポーリングできないため、ディストリビューションポイントに対してこの機能をオンにしておくことが有用な場合があります。

管理サーバーは、MSP クライアントネットワーク上で NAT よりも内側にある管理対象デバイスに対して、ポート 15000 UDP に通知を送信することはできません。この問題を解決するために、ディストリビューションポイントとして動作しているデバイスのプロパティで、管理サーバーへの常時接続モードを有効にしておき、ゲートウェイモードで接続するのが便利です（［**管理サーバーから切断しない**］）。連続接続モードは、ディストリビューションポイントの合計数が 300 を超えていない場合に使用可能です。

ディストリビューションポイントの概要

ネットワークエージェントがインストールされたデバイスはディストリビューションポイントとして使用できます。このモードでは、ネットワークエージェントは、次の機能を実行できます：

- アップデートの配信（アップデートは、管理サーバーまたはカスペルスキーのサーバーから取得します）。後者の場合、ディストリビューションポイントとして機能するデバイスに対して*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを作成する必要があります。
- その他のデバイスへのソフトウェアのインストール（ネットワークエージェントの初期導入を含む）。
- 新しいデバイスを検出したり既存のデバイスの情報を更新するために、ネットワークを検索します。ディストリビューションポイントは管理サーバーと同じ方法でデバイスを検出できます。

組織ネットワークにディストリビューションポイントを導入する目的は、次の通りです：

- アップデート元として機能させる場合、管理サーバーの負荷を減らします。

- インターネットのトラフィックを最適化します。この場合、MSP クライアントネットワーク上にある各デバイスがアップデート時にカスペルスキーのサーバーまたは管理サーバーにアクセスする必要がないためです。

- 管理サーバーに、MSP クライアントネットワークの NAT の背後（管理サーバーを基準にして）にあるデバイスへのアクセスを提供し、管理サーバーが次の処理を実行できるようにします：

  - IPv4 または IPv6 ネットワークの UDP を経由したデバイスへの通知の送信

  - IPv4 または IPv6 ネットワークの検索

  - 初期導入の実行

  - プッシュサーバーとしての動作

1つの管理グループに対して、1つのディストリビューションポイントが割り当てられます。この場合、ディストリビューションポイントの範囲には、管理グループとそのすべてのサブグループ内にあるすべてのデバイスが含まれます。ただし、ディストリビューションポイントとして動作しているデバイスは、割り当てられている管理グループに含まれていなくてもかまいません。

ディストリビューションポイントを接続ゲートウェイとして動作させることができます。この場合、ディストリビューションポイントの範囲内のデバイスは、管理サーバーと直接接続されずゲートウェイを介して接続されます。このモードは、ネットワークエージェントをインストールしたデバイスと管理サーバー間を直接には接続できない場合に有効です。

ディストリビューションポイントとして動作するデバイスについては、あらゆる不正なアクセスに対して、物理的な保護も含めて保護する必要があります。

管理サーバーの階層構造

1台の MSP で、複数台の管理サーバーを稼働させる場合があります。複数台の別の管理サーバーを管理するのは不便であるため、1つの階層を適用することができます。2 台の管理サーバーのプライマリおよびセカンダリ設定には、次のオプションがあります：

- セカンダリ管理サーバーは、プライマリ管理サーバーからポリシーとタスクを継承することにより、設定の重複を防ぎます。

- プライマリ管理サーバーのデバイスには、セカンダリ管理サーバーのデバイスを含めることができます。

- プライマリ管理サーバーのレポートには、セカンダリ管理サーバーのデータ（詳細情報を含む）を含めることができます。

プライマリ管理サーバーは、上記のオプションの範囲内で非仮想セカンダリ管理サーバーからのみデータを受信します。この制限は、プライマリ管理サーバーと定義データベースを共有する仮想管理サーバーには適用されません。

仮想管理サーバー

物理管理サーバーに基づいて、複数台の仮想管理サーバーを作成できます。これは、セカンダリ管理サーバーと類似したものです。仮想管理サーバーモデルは、アクセス制御リスト（ACL）に基づいた任意のアクセスモデルと比較した場合、機能性が高く、高度の分離性を実現しています。ポリシーとタスクが存在する割り当て済みデバイスの管理グループ専用の構造に加えて、各仮想管理サーバーにも未割り当てデバイスのグループ、レポート、抽出されたデバイスとイベント、インストールパッケージ、移動ルールなどがあります。各 MSP クライアントを最大限に分離するため、使用する機能に仮想管理サーバーを選択することを推奨します。さらに、各 MSP クライアントに仮想管理サーバーを作成すると、Kaspersky Security Center Web コンソールを介して、クライアントにネットワーク管理の基本オプションを提供することができます。

仮想管理サーバーはセカンダリ管理サーバーと非常に類似していますが、次の相違点があります：

- 仮想管理サーバーには、多数のグローバル設定と独自の TCP ポートが備えられていません。
- 仮想管理サーバーには、セカンダリ管理サーバーはありません。
- 仮想管理サーバーには、他の仮想管理サーバーはありません。
- 物理管理サーバーには、すべての仮想管理サーバーの管理対象デバイスに関するデバイス、グループ、およびオブジェクトが表示されます（隔離中の項目、アプリケーションレジストリなど）。
- 仮想管理サーバーがスキャンできるのは、ディストリビューションポイントが接続されているネットワークのみです。

Kaspersky Endpoint Security for Android によるモバイルデバイスの管理

Kaspersky Endpoint Security for Android™ がインストールされているモバイルデバイス（以降、KES デバイスと表記）は、管理サーバーによって管理されます。Kaspersky Security Center は、KES デバイスを管理するために次の機能をサポートしています：

- モバイルデバイスをクライアントデバイスとして処理：
  - 管理グループに所属
  - 監視（ステータス、イベント、レポートの表示など）
  - Kaspersky Endpoint Security for Android のローカル設定の変更とポリシーの割り当て
- 一元管理モードでのコマンドの送信
- リモートによるモバイルアプリパッケージのインストール

管理サーバーは、KES デバイスを TLS、TCP ポート 13292 を使用して管理します。

導入と初期セットアップ

Kaspersky Security Center は配信アプリケーションです。Kaspersky Security Center には次のアプリケーションが含まれます：

- 管理サーバー - 組織のデバイスを管理し、DBMS にデータを格納するためのコアコンポーネント。

- 管理コンソール - 管理者用の基本ツール。管理コンソールは管理サーバーに同梱されていますが、管理者が1台または複数台のデバイスに個別にインストールすることもできます。
- Kaspersky Security Center Web コンソールは、基本操作向けに設計された管理サーバー用 Web インターフェイスです。このコンポーネントはシステム要件を満たす任意のデバイスにインストールできます。
- ネットワークエージェント - デバイスにインストールされているセキュリティ製品の管理、およびそのデバイスに関する情報の取得を実行。組織のデバイスには、ネットワークエージェントがインストールされています。

組織ネットワークに Kaspersky Security Center を導入するには、次の作業を実行します：

- 管理サーバーのインストール
- Kaspersky Security Center Web コンソールのインストール
- 管理者のデバイスへの管理コンソールのインストール
- 企業のデバイスへのネットワークエージェントとセキュリティ製品のインストール

管理サーバーのインストールに関する推奨事項

このセクションでは、管理サーバーをインストールする際の推奨事項について説明します。また、管理サーバーデバイスの共有フォルダーを使用して、クライアントデバイスにネットワークエージェントを導入する方法についても説明します。

フェールオーバークラスターに管理サーバーサービス用のアカウントを作成する

既定では、インストーラーが自動的に管理サーバーのサービス用非特権アカウントを作成します。一般的なデバイスに管理サーバーをインストールする場合には、この動作を活用するのが最も便利です。

ただし、フェールオーバークラスターに管理サーバーをインストールする際には、別の方法で行います：

1. 管理サーバーのサービス用非特権ドメインアカウントを作成し、そのアカウントを KLAdmins という名前のグローバルドメインセキュリティグループに所属させます。
2. 管理サーバーのインストーラーで、サービス用に作成したドメインアカウントを指定します。

DBMS の選択

管理サーバーで使用するデータベース管理システム（DBMS）を選択する場合は、管理サーバーが対応できるデバイス数を考慮する必要があります。

次の表に、有効な DBMS オプションとその使用上の推奨事項と制限事項を示します。

DBMS に関する推奨事項と制限事項

DBMS	推奨事項と制限事項

SQL Server Express Edition 2016 以降	10,000 台未満のデバイスに対して単一の管理サーバーを実行する場合は、この DBMS を使用してください。 ソフトウェアインベントリタスクを無効にし、（Kaspersky Endpoint Security ポリシーの設定で）起動したアプリケーション上の管理サーバーの通知を無効にすることを推奨します。 定義データベースのオーバーフローを防ぐために、イベントリポジトリ内のイベントの最大数を制限できます。 詳細については、データベースの容量の計算トピックを参照してください。 管理サーバーと別のアプリケーションで同時に SQL Server Express Edition DBMS を使用することは厳重に禁じられています。 Microsoft SQL Express データベースは、［**Windows Update の同期の実行**］タスクではサポートされていません。
Express を除く 2016 以降のローカル SQL Server Edition	制限なし。
Express を除く 2016 以降のリモート SQL Server Edition	両方のデバイスが同じ Windows® ドメインにある場合のみ有効。ドメインが異なる場合は、両方のデバイス間で双方向の信頼された接続を確立する必要があります。
ローカルまたはリモートの MySQL 5.5、5.6、5.7（MySQL バージョン 5.5.1、5.5.2、5.5.3、5.5.4、5.5.5 はサポートされません）	10,000 台未満のデバイスに対して単一の管理サーバーを実行する場合は、この DBMS を使用してください。 ソフトウェアインベントリタスクを無効にし、（Kaspersky Endpoint Security ポリシーの設定で）起動したアプリケーション上の管理サーバーの通知を無効にすることを推奨します。詳細については、データベースの容量の計算トピックを参照してください。
ローカルまたはリモート MySQL 8.0.20 以降	50,000 台未満のデバイスに対して単一の管理サーバーを実行する場合は、この DBMS を使用してください。 ソフトウェアインベントリタスクを無効にし、（Kaspersky Endpoint Security ポリシーの設定で）起動したアプリケーション上の管理サーバーの通知を無効にすることを推奨します。詳細については、データベースの容量の計算トピックを参照してください。
ローカルまたはリモートの MariaDB（サポートされているバージョンを参照）	20,000 台未満のデバイスに対して単一の管理サーバーを実行する場合は、この DBMS を使用してください。 ソフトウェアインベントリタスクを無効にし、（Kaspersky Endpoint Security ポリシーの設定で）起動したアプリケーション上の管理サーバーの通知を無効にすることを推奨します。詳細については、データベースの容量の計算トピックを参照してください。
PostgreSQL、Postgres Pro（サポートされているバージョンを参照）	50,000 台未満のデバイスに対して単一の管理サーバーを実行する場合は、これらのいずれの DBMS を使用してください。 ソフトウェアインベントリタスクを無効にし、（Kaspersky Endpoint Security ポリシーの設定で）起動したアプリケーション上の管理サーバーの通知を無効にすることを推奨します。詳細については、データベースの容量の計算トピックを参照してください。

PostgreSQL、MariaDB、または MySQL DBMS を使用する場合、［**イベント**］タブには、選択したクライアントデバイスのイベントの不完全なリストが表示されることがあります。これは、DBMS が非常に大量のイベントを保存する場合に発生します。次のいずれかを実行すると、表示されるイベントの数を増やすことができます：

- 不要なイベントを削除します。
- 不要なイベントの保存期間を短縮します。

デバイスの管理サーバーに記録されたイベントの完全なリストを表示するには、レポートを使用します。

SQL Server 2019 を DBMS として使用しており、累積パッチ CU12 以降をインストールしていない場合、Kaspersky Security Center をインストールした後に次の手順を実行する必要があります：

1. SQL Management Studio を使用して、SQL Server に接続します。
2. 次のコマンドを実行します（データベース名に別の名前を選択し、「KAV」の代わりに使用する場合）：

```
USE KAV
GO
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. SQL Server 2019 サービスを再起動します。

再起動しないと、SQL Server 2019 の使用時に「There is insufficient system memory in resource pool 'internal' to run this query」などのエラーが発生する場合があります。

管理サーバーのアドレスの指定

管理サーバーのインストール時には、管理サーバーの外部アドレスを指定する必要があります。このアドレスは、ネットワークエージェントのインストールパッケージを作成する際の既定のアドレスとして使用されます。外部アドレスを指定すると、管理コンソールツールを使用して管理サーバーホストのアドレスを変更できるようになります。この場合、作成済みのネットワークエージェントのインストールパッケージでは、アドレスは自動的には変更されません。

クライアント組織のネットワークでの保護の設定

管理サーバーのインストールが完了すると管理コンソールが起動し、関連するウィザードを使用して初期セットアップを実行するよう要求されます。クイックスタートウィザードの実行中に、ルート管理グループに次のポリシーとタスクが作成されます：

- Kaspersky Endpoint Security のポリシー
- Kaspersky Endpoint Security をアップデートするグループタスク
- Kaspersky Endpoint Security がインストールされたデバイスをスキャンするグループタスク
- ネットワークエージェントのポリシー
- 脆弱性スキャンタスク（ネットワークエージェントのタスク）
- アップデートのインストールと脆弱性修正タスク（ネットワークエージェントのタスク）

ポリシーとタスクは既定の設定値で作成されますが、組織が最適ではないまたは許容できない状態であることが示されます。この場合、作成したオブジェクトのプロパティを確認し、必要な場合は手動で変更します。

このセクションでは、ポリシー、タスク、および管理サーバーのその他の設定の手動設定、ディストリビューションポイント、管理グループ構造とタスクの階層の構築や、その他の設定について説明します。

Kaspersky Endpoint Security ポリシーの手動セットアップ

このセクションでは、クイックスタートウィザードで作成される、Kaspersky Endpoint Security ポリシーの設定方法に関する推奨事項を説明します。ポリシーのプロパティウィンドウで設定を実行できます。

設定を編集する際には、ワークステーションでその値を使用できるように、関連する設定の上にあるロックアイコンをクリックする必要があることに注意してください。

［先進の脅威対策］セクションでのポリシーの設定

このセクションに記載されている設定の詳細な説明は、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

［**先進の脅威対策**］セクションで、Kaspersky Endpoint Security for Windows の Kaspersky Security Network の使用を設定できます。ふるまい検知、脆弱性攻撃ブロック、ホスト侵入防止、修復エンジンなどの Kaspersky Endpoint Security for Windows モジュールを設定することもできます。

［**Kaspersky Security Network**］サブセクションで、［**KSN プロキシを使用する**］を有効にすることを推奨します。このオプションを使用することで、ネットワーク上でトラフィックを再分配し、最適化できます。［**KSN プロキシを使用する**］がオフになっている場合は、KSN サーバーの直接使用を有効にできます。

［脅威対策］セクションでのポリシーの設定

このセクションに記載されている設定の詳細な説明については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

ポリシープロパティウィンドウの［**脅威対策**］セクションで、［**ファイアウォール**］および［**ファイル脅威対策**］のサブセクションに追加の設定を指定することを推奨します。

［**ファイアウォール**］サブセクションには、クライアントデバイス上のアプリケーションのネットワークアクティビティを制御できる設定が含まれています。クライアントデバイスは、パブリック、ローカル、信頼済みのいずれかのステータスが割り当てられているネットワークを使用します。ネットワークステータスに応じて、Kaspersky Endpoint Security はデバイスでのネットワークアクティビティを許可または拒否できます。組織に新しいネットワークを追加する時は、適切なネットワークステータスを割り当てる必要があります。たとえば、クライアントデバイスがノート PC の場合、ノート PC は常にローカルネットワークに接続されているとは限らないため、このデバイスではパブリックネットワークまたは信頼できるネットワークを使用することを推奨します。［**ファイアウォール**］サブセクションで、組織で使用するネットワークにステータスを正しく割り当てたことを確認できます。

ネットワークのリストを確認するには：

1. ポリシーのプロパティで、［**脅威対策**］→［**ファイアウォール**］の順に選択します。
2. ［**使用可能なネットワーク**］セクションで、［**設定**］をクリックします。
3. 表示される［**ファイアウォール**］ウィンドウで、［**ネットワーク**］タブに移動してネットワークのリストを表示します。

［**ファイル脅威対策**］サブセクションで、ネットワークドライブのスキャンを無効にできます。ネットワークドライブのスキャンを行うと、ネットワークドライブに大幅な負荷がかかることがあります。ファイルサーバーで間接スキャンを実行するのが有効です。

ネットワークドライブのスキャンを無効にするには：

1. ポリシーのプロパティで、［**脅威対策**］→［**ファイル脅威対策**］の順に選択します。
2. ［**セキュリティレベル**］セクションで、［**設定**］をクリックします。
3. ［**ファイル脅威対策**］ウィンドウが開いたら、［**全般**］タブで［**すべてのネットワークドライブ**］をオフにします。

［全般設定］セクションでのポリシーの設定

このセクションに記載されている設定の詳細な説明は、Kaspersky Endpoint Security のヘルプを参照してください。

以下で、詳細なセットアップ操作について説明します。この操作は、Kaspersky Endpoint Security のポリシーのプロパティウィンドウの［**全般設定**］セクションで実行してください。

［全般設定］セクション、［レポートと保管領域］サブセクション

［**管理サーバーへのデータ転送**］セクションで、［**起動されたアプリケーションの情報**］をオンにしてください。このチェックボックスをオンにすると、管理サーバー定義データベースに、ネットワーク接続されたデバイス上にあるすべてのバージョンのソフトウェアモジュールに関する情報が保存されます。この情報は、Kaspersky Security Center データベース内に大量のディスク容量を必要とする場合があります（数十ギガバイト）。このため、トップレベルのポリシーで［**起動されたアプリケーションの情報**］がオンになっている場合は、オフにする必要があります。

［全般設定］セクション、［インターフェイス］サブセクション

組織ネットワーク内で管理コンソールを使用した一元管理モードで脅威対策による保護を管理する必要がある場合は、ワークステーションの Kaspersky Endpoint Security ユーザーインターフェイスの表示を無効にして（［**ユーザーインターフェイス**］セクションの［**アプリケーションインターフェイスを表示する**］をオフにする）、ワークステーションでパスワードによる保護を有効にする必要があります（［**パスワードによる保護**］セクションの［**パスワードによる保護を有効にする**］をオンにする）。

［イベントの設定］セクションでのポリシーの設定

［**イベントの設定**］セクションで、管理サーバーに関する次の項目以外のすべてのイベントを保存しないように設定する必要があります：

- ［**緊急イベント**］タブ：
  - コンピューター起動時の自動起動が無効です
  - アクセスが拒否されました
  - アプリケーションの起動が禁止されました
  - 駆除できません
  - ライセンス違反です
  - 暗号化モジュールを読み込めません
  - 2 つのタスクを同時に開始できません
  - アクティブな脅威が検知されました。特別な駆除を開始してください
  - ネットワーク攻撃が検知されました

- アップデートされていないコンポーネントがあります
- アクティベーションエラー
- ポータブルモードの有効化中にエラーが発生しました
- Kaspersky Security Center との対話中にエラーが発生しました
- ポータブルモードの無効化中にエラーが発生しました
- アプリケーション機能の変更中にエラーが発生しました
- ファイル暗号化 / 復号化ルールの適用中にエラーが発生しました
- ポリシーを適用できません
- プロセスが終了しました
- ネットワーク動作がブロックされました

- ［**機能エラー**］タブ：タスク設定が無効です。設定は適用されません
- ［**警告**］タブ：
  - セルフディフェンスが無効です
  - 予備のライセンスが正しくありません
  - ユーザーが暗号化ポリシーを拒否しました
- ［**情報**］タブ：アプリケーションの起動がテストモードでブロックされています

Kaspersky Endpoint Security のグループアップデートタスクの手動セットアップ

このサブセクションの情報が適用されるのは、Kaspersky Security Center 10 Maintenance Release 1 以降のバージョンのみです。

管理サーバーがアップデート元として動作する場合、Kaspersky Endpoint Security 10 以降のバージョンの最適かつ推奨されるスケジュールオプションは、［**新しいアップデートがリポジトリにダウンロードされ次第**］と［**タスクの開始を自動的かつランダムに遅延させる**］です。

Kaspersky Endpoint Security バージョン 8 のグループアップデートタスクの場合は、タスクを実行するまでの時間を明示的に指定し（1 時間以上）、［**タスクの開始を自動的かつランダムに遅延させる**］をオンにします。

カスペルスキーのサーバーからリポジトリにダウンロードをアップデートするローカルタスクが各ディストリビューションポイントで作成される場合、Kaspersky Endpoint Security グループのアップデートタスクに合わせて定期スケジュールを組むことが最適かつ推奨されます。この場合、ランダム化の間隔を 1 時間に設定する必要があります。

Kaspersky Endpoint Security がインストールされたデバイスのスキャン用グループタスクの手動セットアップ

クイックスタートウィザードにより、デバイススキャン用のグループタスクが作成されます。既定では、このタスクは**金曜日の午後 7 時に実行**するよう設定されており、［**未実行のタスクを実行する**］がオフになっています。

つまり、組織内のデバイスが、たとえば、金曜日の午後 6 時 30 分にシャットダウンされる場合、そのデバイスのスキャンタスクは一切実行されません。組織で採用されている職場のルールに基づいて、このタスクに対する最も効率的なスケジュールをセットアップする必要があります。

脆弱性とアプリケーションのアップデートの検索タスクのスケジュール設定

クイックスタートウィザードにより、ネットワークエージェントでの*脆弱性とアプリケーションのアップデートの検索*タスクが作成されます。既定では、このタスクは**火曜日の午後 7 時に実行**するよう設定されており、［**未実行のタスクを実行する**］がオンになっています。

組織で採用されている職場のルールによりこの時刻にすべてのデバイスをシャットダウンするように定められている場合は、デバイスが再度電源オンになる時刻、つまり水曜日の朝以降に、*脆弱性とアプリケーションのアップデートの検索*タスクが実行されます。脆弱性スキャン時には CPU とディスクサブシステムの負荷が増大するため、このように業務時間中に処理が実行されてしまうことが問題となる可能性があります。組織で採用されている職場のルールに基づいて、このタスクに対する最も効率的なスケジュールをセットアップする必要があります。

アップデートのインストールと脆弱性の修正用グループタスクの手動セットアップ

クイックスタートウィザードにより、ネットワークエージェントのアップデートのインストールと脆弱性の修正用のグループタスクが作成されます。既定では、このタスクの実行時間は毎日午前1時に設定されており、［**未実行のタスクを実行する**］がオフになっています。

組織の職場のルールにより夜間はデバイスをシャットダウンするように定められている場合、アップデートのインストールは一切実行されません。組織で採用されている職場のルールに基づいて、脆弱性スキャンタスクに対する最も効率的なスケジュールをセットアップする必要があります。また、アップデートのインストール時には、デバイスの再起動を要求される場合があることにも注意してください。

管理グループの構造の構築とディストリビューションポイントの割り当て

Kaspersky Security Center の管理グループ構造では、次の機能が実行されます：

- ポリシー範囲の設定

関連する一連の設定をデバイスに適用する別の方法は、ポリシーのプロファイルを使用することです。この場合、ポリシーの範囲は、タグ、Active Directory 組織単位内のデバイスの場所、Active Directory セキュリティグループの所属などによって設定されます。

- グループタスク範囲の設定

  管理グループの階層に基づいていない、グループタスク範囲の定義方法が存在します。これは、デバイス選択用のタスクと特定のデバイス用のタスクを使用することです。

- デバイス、仮想管理サーバー、およびセカンダリ管理サーバーへのアクセス権限の設定

- ディストリビューションポイントの割り当て

管理グループ構造を構築する際には、ディストリビューションポイントを最適に割り当てるために、組織ネットワークのトポロジーを考慮する必要があります。ディストリビューションポイントを最適に分散配置すると、組織ネットワークのトラフィック量を軽減できます。

組織の構造と MSP クライアントによって導入されたネットワークトポロジーに応じて、管理グループ構造に次の標準設定を適用できます：

- 単一のオフィス

- 複数の小規模な離れているオフィス

MSP クライアントの標準設定：単一のオフィス

標準の「単一のオフィス」設定では、すべてのデバイスが組織ネットワーク内に置かれているため、お互いを「見る」ことができます。組織ネットワークは、いくつかの部分に区切られ（ネットワークまたはネットワークセグメント）、狭い帯域幅によって連結されるかたちで構成されている場合があります。

管理グループの構造は、次の方法で構築することが可能です：

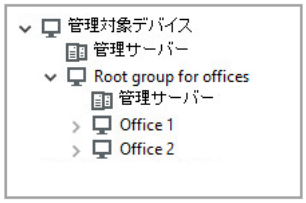
- ネットワークトポロジーを考慮に入れて管理グループの構造を構築します。管理グループの構造が、厳密にネットワークトポロジーを反映していなくても問題ありません。ネットワークが区切られた各部分と特定の管理グループの間に一致があれば十分です。ディストリビューションポイントの自動割り当てを使用するか、または手動で割り当てることができます。

- ネットワークトポロジーを考慮に入れずに管理グループの構造を構築します。この場合は、ディストリビューションポイントの自動割り当てを無効にしてから、ディストリビューションポイントとして動作する 1 台以上のデバイスをネットワークの区切られた各部分のルート管理グループ（たとえば、**管理対象デバイス**グループ）に対して割り当てる必要があります。ディストリビューションポイントは、すべて同じレベルに置かれ、組織ネットワーク内のすべてのデバイスを包含する同じ範囲を対象とします。この場合、各ネットワークエージェントは、最短経路のディストリビューションポイントに接続します。ディストリビューションポイントへの経路は、tracert ユーティリティによって追跡できます。

MSP クライアントの標準設定：複数の小規模なリモートオフィス

この標準設定は、インターネットを介して本社と通信する可能性のある多数の小規模なリモートオフィス向けの設定です。各リモートオフィスは NAT を介するようにその背後に配置されています。つまり、2 つのオフィスはお互いに分離されているため、お互いに接続することはできません。

管理グループ構造内で設定を反映させる必要があります。つまり、各リモートオフィスに対して、個別の管理グループを作成する必要があります（下の図のグループ［**Office 1**］と［**Office 2**］）。



管理グループ構造に含まれているリモートオフィス

1つのオフィスに対応する各管理グループに対して、1つまたは複数個のディストリビューションポイントを割り当てる必要があります。ディストリビューションポイントは、空きディスク容量が十分なリモートオフィスにあるデバイスである必要があります。たとえば、［**Office 1**］グループに導入されているデバイスは、［**Office 1**］管理グループに割り当てられているディストリビューションポイントにアクセスできます。

ノート PC を持ち運んでオフィス間を移動するユーザーが存在する場合は、各リモートオフィスで 2 台以上のデバイス（既存のディストリビューションポイントに加えて）を選択し、それらのデバイスをトップレベルの管理グループ（上の図の［**Root group for offices**］）用のディストリビューションポイントとして動作するように割り当てる必要があります。

例：［**Office 1**］管理グループ内にノート PC を導入しましたが、［**Office 2**］管理グループに対応するオフィスにマシンを持って移動するとします。ノート PC を移動させると、ネットワークエージェントは［**Office 1**］グループに割り当てられているネットワークエージェントへのアクセスを試行しますが、これらのディストリビューションポイントは使用不可の状態です。次に、ネットワークエージェントは、［**Root group for offices**］に割り当てられているディストリビューションポイントへのアクセスの試行を開始します。リモートオフィスはお互いに分離されているため、［**Root group for offices**］管理グループに割り当てられているディストリビューションポイントへのアクセスの試行は、ネットワークエージェントが［**Office 2**］グループ内にあるディストリビューションポイントへのアクセスを試行した際にのみ正常に実行されます。つまり、ノート PC は最初のオフィスに対応する管理グループ内に残りますが、ディストリビューションポイントについては移動後のオフィスに存在するディストリビューションポイントを使用します。

ポリシーのプロファイルを使用した、ポリシーの階層

このセクションでは、管理グループ内のデバイスにポリシーを適用する方法について説明します。また、ポリシープロファイルについても説明します。

ポリシーの階層

Kaspersky Security Center では、複数のデバイスに対して単一の一連の設定を定義するためにポリシーを使用します。たとえば、管理グループ G で定義されているアプリケーション P のポリシー範囲には、グループ G とそのすべてのサブグループの、アプリケーション P がインストールされた管理対象デバイスが含まれます。ただし、プロパティで［**親グループから継承する**］がオフになっているサブグループを除きます。

ポリシーは、設定の横にロックアイコン（）がある点で、ローカル設定とは異なります。ポリシープロパティの設定（または設定のグループ）がロックされている場合は、効率的な設定を作成する際に最初にこの設定（または、設定のグループ）を使用し、次に下位のポリシーに対して設定または設定のグループを記述する必要があります。

デバイスに対して効率的な設定を作成する際の説明は次の通りです。ロックされていない設定値をすべてポリシーから取得し、その値をローカル設定値で上書きします。これにより、生成されたコレクションがポリシーから取得したロック済みの設定値により上書きされます。

同じアプリケーションのポリシーは、管理グループの階層を介してお互いに影響を与えます。上位のポリシーのロック済みの設定は、下位のポリシーの同じ設定を上書きします。

モバイルユーザーに対しては、特別なポリシーが存在します。このポリシーは、デバイスがモバイルユーザーモードに切り替わった際に有効になります。モバイルユーザーポリシーが管理グループの階層を介して他のポリシーに影響することはありません。

Kaspersky Security Center の今後のバージョンでは、モバイルユーザーポリシーはサポートされなくなります。モバイルユーザーポリシーに代わって、ポリシーのプロファイルが使用されます。

ポリシーのプロファイル

多数の環境において、デバイスにポリシーを適用する方法が管理グループの階層を使用するだけというのは適切ではありません。複数の管理グループで 1 つまたは 2 つの設定値が異なる単一ポリシーで複数のインスタンスを作成し、将来これらのポリシーの内容を同期させることが必要になる場合があります。

このような問題を回避するために、Kaspersky Security Center は*ポリシープロファイル*をサポートしています。ポリシーのプロファイルには、ポリシー設定のサブセットが指定されています。このサブセットはポリシーとともに対象デバイスに配信され、*プロファイルの有効化条件*と呼ばれる特定の条件下でポリシーを補完する機能を果たします。プロファイルに含まれるのは、クライアントデバイス（コンピューターまたはモバイルデバイス）でアクティブな「基本」ポリシーとは異なる設定のみです。プロファイルを有効にすると、プロファイルが有効になる前にデバイスで有効になっていたポリシー設定が修正されます。こうした設定により、プロファイルで指定された値が得られます。

現在、ポリシーのプロファイルに適用されている制限事項は次の通りです：

- ポリシーには最大 100 個のプロファイルを含めることができます。
- ポリシーのプロファイルにその他のプロファイルを含めることはできません。
- ポリシーのプロファイルに通知の設定を含めることはできません。

プロファイルの内容

ポリシーのプロファイルには、次の構成要素が含まれています：

- 名前：同じ名前のプロファイルは、共通のルールが含まれる管理グループの階層によって相互に影響します。
- ポリシー設定のサブセット：すべての設定が含まれているポリシーとは異なり、プロファイルには実際に必要な設定のみが含まれています（ロック済みの設定）。
- アクティベーション条件：デバイスのプロパティを使用した論理式。プロファイルが有効になる（ポリシーを補完する）のは、プロファイルの有効化条件に該当する場合のみです。その他の場合はすべて、プロファイルは非アクティブで無視されます。論理式には、次のデバイスプロパティを含めることができます：
  - モバイルユーザーモードのステータス
  - ネットワーク環境のプロパティ：ネットワークエージェント接続の有効なルールの名前
  - 指定したタグがデバイスに存在するかどうか
  - Active Directory 単位におけるデバイスの場所：明示的（デバイスはまさに指定した OU 内にある）、または暗黙的（デバイスは OU 内にある。ただし、任意のネストレベルで指定した OU 内にある）

- デバイスが属している Active Directory セキュリティグループ（明示的または暗黙的）
- デバイス所有者が属している Active Directory セキュリティグループ（明示的または暗黙的）

- プロファイルを無効にする：無効化されたプロファイルは常に無視され、それぞれの有効化条件は検証されません。
- プロファイルの優先度：異なるプロファイルの有効化条件は独立しているため、複数のプロファイルを同時に有効化することができます。アクティブなプロファイルに重複しない一連の設定が含まれている場合、問題は発生しません。ただし、2 つのアクティブなプロファイルで同じ設定の値が異なる場合は、不明確さが発生します。この不明確さを回避するために、プロファイルの優先度が使用されます。不明確な変数の値は、優先度が高い方（プロファイルのリスト内での位置付けが高い方）のプロファイルから取得されます。

ポリシーが階層を介してお互いに影響を与え合う場合のプロファイルの動作

名前が同じプロファイルは、ポリシー統合ルールに従って統合されます。上位のポリシーのプロファイルは、下位のポリシーのプロファイルよりも優先度が高くなっています。上位のポリシーで設定の編集がブロックされている（ロック状態）場合、下位のポリシーでは上位のポリシーのプロファイルの有効化条件が使用されます。一方、上位のポリシーで設定の編集が許可されている場合は、下位のポリシーのプロファイルの有効化条件が使用されます。

ポリシーのプロファイルの有効化条件には［**オフラインのデバイス**］プロパティが含まれているため、プロファイルではサポートされていないモバイルユーザー用のポリシー機能は完全に置き換えられます。

モバイルユーザー用のポリシーにはプロファイルが含まれていることがありますが、そのプロファイルがアクティブ化されるのは、デバイスがモバイルユーザーモードに切り替えられた後だけです。

タスク

Kaspersky Security Center は、様々な*タスク*を作成して実行することにより、デバイス上にインストールされたカスペルスキー製品を管理します。アプリケーションのインストール、起動、停止、ファイルのスキャン、定義データベースやソフトウェアモジュールのアップデート、アプリケーションでのその他のタスクを実行するには、タスクが必要です。

アプリケーションのタスクを作成できるのは、そのアプリケーション用の管理プラグインがインストールされている場合に限られます。

タスクは管理サーバー上とデバイス上で実行できます。

次のタスクは管理サーバーで実行されます：

- レポートの自動配信
- 管理サーバーのリポジトリへのアップデートのダウンロード
- 管理サーバーデータのバックアップ
- データベースのメンテナンス
- Windows Update の同期の実行
- 基準となるデバイスの OS イメージに基づいたインストールパッケージの作成

次の種別のタスクはデバイスで実行されます：

- *ローカルタスク* - 特定の1台のデバイスで実行されるタスク

  ローカルタスクを変更するには、管理者が管理コンソールツールを使用するか、またはリモートデバイスのユーザーが実行します（たとえば、セキュリティ製品のインターフェイスを使用）。管理対象デバイスの管理者とユーザーが同時にローカルタスクを変更する場合、管理者が行う変更内容の方が優先度が高いため有効になります。

- *グループタスク* - 特定のグループに属するすべてのデバイスで実行されるタスク

  タスクのプロパティで特別な設定を行わない限り、グループタスクは選択したグループのすべてのサブグループに影響します。さらに、グループタスクは該当するグループまたはそのサブグループのいずれかに導入されている、セカンダリおよび仮想管理サーバーに接続されているデバイスにも適用されます（オプション設定による）。

- *グローバルタスク* - 管理グループに含まれるかどうかに関係なく、特定のデバイスで実行されるタスク

アプリケーションごとに、任意の数のグループタスク、グローバルタスク、ローカルタスクを作成できます。

タスクの設定に変更を加え、タスクの進行状況を表示し、タスクをコピー、エクスポート、インポート、および削除できます。

タスクは、そのタスクを作成した対象のアプリケーションが実行中である場合のみ、デバイス上で開始されます。

タスクの実行結果は、管理サーバー上の Microsoft Windows のイベントログと Kaspersky Security Center のイベントログに一元的に保存されます。また、各デバイスのローカルにも保存されます。

タスクの設定には個人データを使用しないでください。たとえば、ドメイン管理者パスワードを指定することは避けてください。

デバイス移動ルール

*デバイス移動ルール*を使用して、MSP クライアントに対応する仮想サーバーでの管理グループへのデバイス割り当てを自動化することを推奨します。デバイス移動ルールは、3 つのメイン部分から構成されます。それは、名前、実行条件（デバイス属性を使用した論理式）、および対象管理グループです。デバイス属性がルールの実行条件を満たしている場合は、このルールによりデバイスが対象管理グループに移動されます。

デバイス移動ルールにはすべて優先度が設定されています。管理サーバーは優先度の昇順に従って、デバイス属性が各ルールの実行条件を満たしているかどうかを確認します。デバイス属性がルールの実行条件を満たしている場合、そのデバイスは対象グループに移動され、このデバイスに対するルール処理が完了します。デバイス属性が複数のルールの条件を満たしている場合、そのデバイスは優先度が最も高いルールの対象グループに移動されます（つまり、ルールのリスト内で最高ランク）。

デバイス移動ルールは暗黙的に作成できます。たとえば、インストールパッケージまたはリモートインストールタスクのプロパティで、ネットワークエージェントをデバイスにインストールした後にそのデバイス移動先の管理グループを指定できます。さらに、移動ルールのリスト内で Kaspersky Security Center の管理者が、デバイス移動ルールを明示的に作成できます。このリストは、管理コンソールの［**未割り当てデバイス**］グループのプロパティ内に置かれています。

既定では、デバイス移動ルールは、管理グループに対してデバイスを最初にワンタイムで割り当てることを目的としています。このルールにより、［**未割り当てデバイス**］グループから一度だけデバイスが移動されます。デバイスがこのルールによって一度移動されている場合は、デバイスを手動で［**未割り当てデバイス**］グループに戻したとしても、このデバイスが再度移動されることはありません。これは移動ルールを適用する際に推奨される方法です。

一部の管理グループに割り当て済みであるデバイスを移動できます。これを実行するには、ルールのプロパティで［**どの管理グループにも属していないデバイスのみ移動する**］をオフにします。

一部の管理グループに割り当て済みのデバイスに対して移動ルールを適用すると、管理サーバーの負荷が大幅に増大します。

単一のデバイスに繰り返し適用される移動ルールを作成することができます。

単一のデバイスをあるグループから別のグループに繰り返し移動させないでください（たとえば、該当するデバイスに特別なポリシーを適用するために、特別なグループタスクを実行するか、または特定のディストリビューションポイントを使用してデバイスをアップデートする）。

このような処理は、管理サーバーとネットワークのトラフィックの負荷を極端に増大させるため、サポートされていません。また、Kaspersky Security Center の操作原理と競合する可能性もあります（特に、アクセス権限、イベント、レポートの分野において）。ポリシーのプロファイル、デバイス抽出のタスク、標準シナリオに従ったネットワークエージェントの割り当てなどを使用して、別のソリューションを見つける必要があります。

ソフトウェアのカテゴリ分け

アプリケーションの実行状態を監視する主なツールは、*カスペルスキーのカテゴリ*です（以下、*KL カテゴリ*と表記）。KL カテゴリを使用することで、Kaspersky Security Center 管理者によるソフトウェアのカテゴリ分けのサポートを簡略化でき、管理対象デバイスへのトラフィックを最小化できます。

アプリケーションカテゴリは、既存の KL カテゴリのいずれかには分類できないアプリケーションに対してのみ作成する必要があります（たとえば、カスタムメイドソフトウェア用）。また、アプリケーションカテゴリは、アプリケーションのインストールパッケージ（MSI）またはインストールパッケージの置かれているフォルダーに基づいて作成されます。

KL カテゴリによりカテゴリ化されていない大規模セットのソフトウェアが提供されている場合は、自動的に更新されるカテゴリを作成するのが便利です。実行ファイルのチェックサムは、配布パッケージを含むフォルダーが変更されるたびに、自動的にこのカテゴリに追加されます。

My Documents、%windir%、%ProgramFiles%、および %ProgramFiles(x86)% フォルダーに対して、ソフトウェアの自動アップデートカテゴリを作成しないでください。これらのフォルダーにあるファイルのプールは頻繁に変更する必要がありますが、これにより管理サーバーの負荷とネットワークのトラフィックが増大します。この場合、一連のソフトウェアを格納する専用フォルダーを作成し、このフォルダーに定期的に新しい項目を追加する必要があります。

マルチテナントアプリケーションの概要

Kaspersky Security Center を使用することで、サービスプロバイダーの管理者とテナント管理者はマルチテナントをサポートするカスペルスキー製品を利用できます。サービスプロバイダーのインフラストラクチャにマルチテナントのカスペルスキー製品がインストールされると、それぞれのテナントはカスペルスキー製品の利用を開始できます。

それぞれのテナントに対してタスクとポリシーを個別に適用するには、Kaspersky Security Center でテナントごとに専用の仮想管理サーバーを作成する必要があります。それぞれのテナントで実行しているマルチテナントの製品のタスクとポリシーは、すべて、対応する仮想管理サーバーの管理対象デバイス管理グループに対して作成する必要があります。プライマリ管理サーバーの管理グループに対して作成したタスクは、テナントに属するデバイスには影響しません。

サービスプロバイダーの管理者とテナントの管理者が異なる点として、テナントの管理者はそのテナントのデバイスを対象としたタスクとポリシーのみを作成したり表示できます。また、サービスプロバイダーの管理者とテナントの管理者では、利用できるタスクとポリシーが異なります。テナント管理者は、一部のタスクとポリシーの設定を利用できません。

1つのテナント内で管理グループの階層がある場合、マルチテナントの製品のポリシーは、下位の管理グループだけでなく上位の管理グループにも継承され、該当するテナント内のすべてのクライアントデバイスに反映されます。

管理サーバーの設定のバックアップと復元

管理サーバーとそのデータベースの設定のバックアップは、バックアップタスクと klbackup ユーティリティを使用して実行されます。バックアップコピーには、証明書、管理対象デバイスのドライブ暗号化用のプライマリキー、様々なライセンス情報、および内容、タスク、ポリシーのすべてを含む管理グループ構造など、管理サーバーに関係するすべての主要な設定とオブジェクトが含まれています。バックアップコピーを使用すると、数十分から数時間で可能な限り迅速に管理サーバーの操作を復元できます。

バックアップコピーが使用できない場合は、障害が発生して証明書や管理サーバーの設定がすべて失われてしまうことがあります。この場合は、Kaspersky Security Center を最初から再設定し、組織ネットワークで再度ネットワークエージェントの初期導入を実行する必要があります。管理対象デバイスのドライブ暗号化用のプライマリキーもすべて失われ、Kaspersky Endpoint Security がインストールされたデバイスの暗号化されたデータも失われてしまう危険性があります。そのため、必ず標準的なバックアップタスクを実行し、管理サーバーを定期的にバックアップしてください。

クイックスタートウィザードは、管理サーバー設定のバックアップタスクを作成し、このタスクが毎日午前 4 時に実行されるように設定します。既定では、バックアップコピーはフォルダー %ALLUSERSPROFILE%\Application Data\KasperskySC に保存されます。

別のデバイスにインストールされている Microsoft SQL Server のインスタンスが DBMS として使用されている場合は、バックアップコピーを格納するフォルダーとして UNC パスを指定し、バックアップタスクを変更する必要があります。この場合、管理サーバーサービスと SQL Server サービスの両方による書き込みが使用できます。この要件は、Microsoft SQL Server DBMS のバックアップ特別機能から導かれます。

Microsoft SQL Server のローカルインスタンスが DBMS として使用されている場合は、専用メディアにバックアップコピーを保存して、管理サーバーとともに損傷から保護することを推奨します。

バックアップコピーには重要なデータが含まれているため、バックアップタスクと klbackup ユーティリティではバックアップコピーがパスワードにより保護されます。既定では、作成されるバックアップタスクのパスワードは空白です。このため、バックアップタスクのプロパティでパスワードを設定する必要があります。この要件を無視すると、管理サーバー証明書のすべての鍵、ライセンスの鍵、および管理対象デバイスのドライブ暗号化用のプライマリキーが暗号化されないままになります。

定期的なバックアップの他に、管理サーバーのアップグレードのインストールやパッチ適用などの重要な変更を加える前にも、必ずバックアップコピーを作成する必要があります。

Microsoft SQL Server を DBMS として使用すると、バックアップコピーのサイズを最小限に抑えることができます。これを行うには、SQL Server 設定で［**バックアップを圧縮する**］をオンにします。

バックアップコピーからの復元を実行するには、インストール済みで、バックアップコピーを作成したのと同じバージョン（またはそれ以降）の管理サーバーの操作可能なインスタンスでユーティリティ klbackup を使用します。

復元を実行する対象の管理サーバーのインスタンスでは、同じ種別（たとえば、同じ SQL Server または MariaDB）で同じかそれ以降のバージョンの DBMS を使用する必要があります。管理サーバーのバージョンは、同じ（同一またはそれ以降のパッチを適用）またはそれ以降にする必要があります。

このセクションでは、管理サーバーの設定とオブジェクトを復元する標準的な方法について説明します。

管理サーバーがインストールされているデバイスを操作できない

障害が発生しているため、管理サーバーをインストールしたデバイスが操作できない場合は、次の操作を実行してください：

- 新しい管理サーバーを同じアドレスで割り当てる：NetBIOS 名、FQDN、または固定 IP（ネットワークエージェント導入時の設定に応じて）。
- 同じ種別、同じ（またはそれ以降の）バージョンの DBMS を使用して、管理サーバーをインストールする。同じ（またはそれ以降の）パッチが適用された、同じバージョンまたはそれ以降のバージョンのサーバーをインストールする必要があります。インストール後は、ウィザードによる初期セットアップを実行しないでください。
- ［**スタート**］メニューで、klbackup ユーティリティによる復元を実行する。

管理サーバーまたはデータベースの設定が破損している

設定またはデータベースが破損しているため（たとえば、電力サージが原因）、管理サーバーが操作できない場合は、次の復元方法を使用してください：

1. 損傷を受けたデバイスでファイルシステムをスキャンする。
2. 操作できないバージョンの管理サーバーをアンインストールする。
3. 同じ種別、同じ（またはそれ以降の）バージョンの DBMS を使用して、管理サーバーを再インストールする。同じ（またはそれ以降の）パッチが適用された、同じバージョンまたはそれ以降のバージョンのサーバーをインストールする必要があります。インストール後は、ウィザードによる初期セットアップを実行しないでください。
4. ［**スタート**］メニューで、ユーティリティ klbackup による復元を実行する。

klbackup ユーティリティ以外の方法で管理サーバーを復元することは禁止されています。

サードパーティ製のソフトウェアを使用して管理サーバーの復元を試行した場合は、配信アプリケーション Kaspersky Security Center のノード上のデータが同期化されなくなり、その結果、本製品が正常に動作しなくなります。

ネットワークエージェントとセキュリティ製品の導入

組織内でデバイスを管理するには、各デバイスにネットワークエージェントをインストールする必要があります。組織用デバイスに配信された Kaspersky Security Center を導入すると、通常はそのデバイスでネットワークエージェントのインストールが開始されます。

Microsoft Windows XP では、ネットワークエージェントが次の動作を正常に実行できない可能性があります：カスペルスキーのサーバーからのアップデートの直接ダウンロード（ディストリビューションポイントとして動作している場合）、KSN プロキシサーバーとしての動作（ディストリビューションポイントとして動作している場合）、サードパーティ製品の脆弱性の検知（脆弱性とパッチ管理機能を使用している場合）

初期導入

デバイスに既にネットワークエージェントがインストールされている場合は、このネットワークエージェントを使用してデバイスにアプリケーションがリモートインストールされます。インストールするアプリケーションの配布パッケージは、管理者が定義したインストール設定とともに、ネットワークエージェントと管理サーバー間の通信チャネルを介して転送されます。配布パッケージを転送するには、転送配布用のノードを使用します。例：ディストリビューションポイント、マルチキャストによる配布など。ネットワークエージェントがインストール済みである管理対象デバイスへのアプリケーションのインストール方法に関する詳細は、このセクションの下を参照してください。

次のいずれかの手法を使用して、Windows を実行中のデバイスにネットワークエージェントの初期インストールを実行できます：

- アプリケーションをリモートインストールするためにサードパーティ製のツールを使用する。
- Windows のグループポリシー：Windows の標準的なグループポリシーの管理ツールを使用する。
- Kaspersky Security Center のリモートインストールタスクで、特別なオプションを強制的に使用する。
- Kaspersky Security Center が生成したスタンドアロンパッケージに対して、デバイスユーザーリンクを送信する。スタンドアロンパッケージは、選択したアプリケーションの配布パッケージを含む、設定が定義された実行モジュールです。
- デバイスで手動によりアプリケーションインストーラーを実行する。

Microsoft Windows 以外のプラットフォームでは、管理対象デバイスでネットワークエージェントの初期インストールを行う必要があります。これは既存のサードパーティ製のツールを介するか手動のいずれかの手段で、事前設定された配布パッケージを使用して、アーカイブをユーザーに送信することによって実施します。ネットワークエージェントを新しいバージョンにアップグレードする、または Windows 以外のプラットフォームに他のカスペルスキー製品をインストールするには、デバイス上にインストール済みのネットワークエージェントを使用してリモートインストールタスクを実行します。この場合、インストール方法は Microsoft Windows を実行しているデバイスの場合と同じです。

管理対象ネットワーク内に製品を導入するための方法と戦略を選択する際には、いくつかの要素について検討する必要があります（部分的なリスト）：

- 組織のネットワークの構成
- デバイスの合計数
- 管理対象ネットワーク上の Windows ドメインの存在、それらのドメイン内で Active Directory グループポリシーを変更する可能性
- カスペルスキー製品の初期導入が計画されているデバイスのローカル管理者権限のあるユーザーアカウントの認知（例：ローカル管理者権限のあるドメインユーザーアカウントの可用性、または、これらのデバイスの管理者権限がある一元管理されたローカルユーザーアカウントの存在）
- 管理サーバーと MSP クライアントネットワーク間の接続種別とネットワークチャネルの帯域、およびこれらのネットワーク内部のチャネルの帯域
- 導入開始時にリモートデバイスに適用されているセキュリティ設定（UAC および簡易ファイルの共有モードの使用など）

インストーラーを設定する

ネットワーク上へのカスペルスキー製品の導入を開始する前に、アプリケーションのインストール時に定義するインストール設定を指定する必要があります。ネットワークエージェントをインストールする際には、最低でも管理サーバーとプロキシ設定への接続に使用するアドレスを指定する必要があり、いくつかの詳細設定が必要になる場合もあります。選択したインストール方法に応じて、いくつかの方法で設定を定義できます。最も簡単な方法（選択したデバイスへの手動による対話式インストール）では、関連するすべての設定をインストーラーのユーザーインターフェイスを介して定義できます。このため一部のケースでは、ユーザーがインストーラーのインターフェイスに入力しなければならない設定情報（管理サーバーアドレスなど）とともにネットワークエージェント配布パッケージのリンクをユーザーに送信することによって、初期導入を行うことも可能です。

この方法の使用は推奨しません。ユーザーにとって不便であり、手動で設定を定義する時にエラーが生じるリスクが高いためです。また、デバイスグループのアプリケーションがサイレントインストールの場合、この方法は使用できません。一般には、管理者が一元管理モードで設定の値を指定する必要があります。この値は、スタンドアロンパッケージを作成する際に引き続き使用できます。スタンドアロンパッケージは自己解凍アーカイブで、管理者によって定義された設定を含む配布パッケージを含みます。スタンドアロンパッケージはリソースにあり、ここからエンドユーザーによるダウンロード（Kaspersky Security Center Web サーバーからなど）と、選択されたネットワーク接続デバイスのサイレントモードでのインストールの両方が可能です。

インストールパッケージ

最初に説明するアプリケーションのインストール設定を定義する主な方法は汎用性があり、Kaspersky Security Center のツールおよび多数のサードパーティ製のツールを使用した、すべてのインストール方法に適しています。この方法は、Kaspersky Security Center にアプリケーションのインストールパッケージを作成する処理から構成されています。

インストールパッケージを作成するには、次の方法を使用します：

- 含まれている*記述子*を基にして、指定した配布パッケージから自動的に作成（インストールと結果分析のルール、およびその他の情報を含む kud 拡張子のファイル）
- インストーラーの実行ファイル、または Microsoft Windows インストーラー（MSI）形式のインストーラーから作成（標準またはサポートされているアプリケーション用）

作成されたインストールパッケージは、サブフォルダーとファイルが格納されているフォルダーとして階層的に編成されます。インストールパッケージには元の配布パッケージの他に、編集可能な設定（インストールを完了するために必要なオペレーティングシステムの再起動を処理するための、インストーラーの設定とルールを含む）と小規模な予備モジュールが含まれています。

サポート対象に選択したアプリケーション固有のインストール設定値は、インストールパッケージの作成時に管理コンソールのユーザーインターフェイスで指定できます（さらなる設定は、既に作成済みのインストールパッケージのプロパティで可能です）。Kaspersky Security Center のツールを使用してアプリケーションをリモートインストールする際には、インストールパッケージをターゲットのデバイスに配布します。これで、アプリケーションのインストーラーを実行することにより、すべての管理者定義の設定がアプリケーションで使用できるようになります。カスペルスキー製品のインストールにサードパーティ製のツールを使用する際に必要になるのは、対象デバイスでインストールパッケージ全体（つまり、配布パッケージとその設定）を使用できるようにすることだけです。Kaspersky Security Center によってインストールパッケージが作成され、共有データフォルダーの専用サブフォルダーに保存されます。

インストールパッケージの設定では、特別な権限を持つアカウントを指定しないでください。

サードパーティ製のツールを使用して導入する前にカスペルスキー製品にこの設定方法を使用する方法は、「Microsoft Windows のグループポリシーを使用した導入」を参照してください。

Kaspersky Security Center のインストール直後には、自動的にいくつかのインストールパッケージが作成されます。これらのインストールパッケージはインストールの準備が完了しており、Microsoft Windows 用のネットワークエージェントパッケージとセキュリティ製品パッケージを含んでいます。

一部のケースでは、MSP クライアントネットワーク上でのアプリケーション導入時にインストールパッケージを使用する場合、MSP クライアントに対応する仮想サーバーでインストールパッケージを作成する必要が生じます。仮想サーバーでインストールパッケージを作成することで、MSP クライアントごとに異なるインストール設定を使用できるようになります。これはまず、ネットワークエージェントのインストールパッケージを取り扱う際に有用です。異なる MSP クライアントのネットワークに導入されたネットワークエージェントは、異なるアドレスを使用して管理者サーバーに接続するためです。実際に、ネットワークエージェントの接続先サーバーは、接続アドレスが決定します。

仮想管理サーバーでインストールパッケージをメイン動作モードにすると、仮想管理サーバー上で新しいインストールパッケージがすぐに作成される可能性があるだけでなく、プライマリ管理サーバーから仮想サーバーへインストールパッケージが配布されます。対応する管理サーバータスクを使用して、選択した（あるいはすべての）インストールパッケージを選択した仮想管理サーバー（選択された管理グループ内のすべてのサーバーを含む）に配布できます。また、新しい仮想管理サーバーの作成時に、プライマリ管理サーバーのインストールパッケージのリストを選択できます。選択したパッケージは、新たに作成された仮想管理サーバーへすぐに配布されます。

インストールパッケージが配布される際は、パッケージのコンテンツ全体がコピーされるわけではありません。配布対象のインストールパッケージに対応する仮想管理サーバーのファイルリポジトリで保存されるのは、その仮想サーバー固有の設定ファイルのみです。インストールパッケージの主要部分（インストール対象アプリケーションの配布パッケージを含む）は変更されないまま、プライマリ管理サーバーリポジトリのみに保存されます。これによりシステムのパフォーマンスが大幅に向上し、要求されるディスク容量を減らすことができます。仮想管理サーバーに配布されるインストールパッケージを取り扱う際（リモートインストールタスクの実行時や、スタンドアロンインストールパッケージの作成時など）に、プライマリ管理サーバーの元のインストールパッケージのデータが設定ファイルと「統合」され、これが仮想管理サーバー上の配布対象パッケージに対応したものになります。

アプリケーションのライセンスはインストールパッケージのプロパティ内で設定できますが、このライセンス配布方法は避けるのが適切です。フォルダー内のファイルへの読み取り権限が偶発的に取得される可能性が高いためです。この場合、ライセンスの自動配信またはライセンスのインストールタスクを使用する必要があります。

MSI プロパティと変換ファイル

Windows プラットフォームでインストールを設定する別の方法は、MSI プロパティと変換ファイルを定義することです。この方法は、Microsoft インストーラー形式のインストーラー用のサードパーティ製ツールを介したインストールの実施時と、標準的な Microsoft ツールまたは Windows グループポリシー用の他のサードパーティ製ツールを使用して Windows グループポリシーを介したインストールの実施時に使用できます。

アプリケーションのリモートインストールにおけるサードパーティ製のツールを使用した導入

組織でアプリケーションのリモートインストール用ツール（Microsoft System Center など）が使用可能な場合は、これらのツールを使用して初期導入を実行するのが便利です。

次の処理を実行する必要があります：

- 使用する導入ツールに最適なインストール設定方法を選択します。
- インストールパッケージの設定の変更（管理コンソールインターフェイスを使用）とインストールパッケージデータからのアプリケーション導入用として選択したサードパーティ製のツールの操作との間の同期メカニズムを定義します。

Kaspersky Security Center でのリモートインストールタスクに関する一般情報

Kaspersky Security Center は、リモートインストールタスクとして実装されるアプリケーションの各種リモートインストール方法を提供します。リモートインストールタスクは、特定のデバイスまたは選択したデバイスと指定した管理グループの両方に対して作成できます（このタスクは管理コンソールの［**タスク**］フォルダーに表示されます）。タスクを作成する際には、このタスク内にインストールする（ネットワークエージェントや別のアプリケーン用の）インストールパッケージを選択し、リモートインストール方法を定義するための特定の設定を指定することができます。

管理グループのタスクは、指定したグループに含まれるデバイスと、その管理グループ内のすべてのサブグループにあるすべてのデバイスの両方に影響を与えます。タスクは、対応する設定がそのタスク内で有効な場合、1つのグループまたはそのサブグループのいずれかに含まれるセカンダリ管理サーバーのデバイスに対応しています。

特定のデバイスに対するタスクでは、タスクが開始された時点での選択内容に従って、実行ごとにクライアントデバイスのリストが更新されます。選択内容に、セカンダリ管理サーバーに接続されているデバイスが含まれている場合は、そのデバイスでもタスクが実行されます。

セカンダリ管理サーバーに接続されているデバイスでリモートインストールタスクの操作を正常に実行するには、対応するセカンダリ管理サーバーに対して前もって配布タスクを実行し、タスクで使用するインストールパッケージを配布しておく必要があります。

Microsoft Windows のグループポリシーを使用した導入

次の条件を満たしている場合は、Microsoft Windows のグループポリシーを使用してネットワークの初期導入を実行してください：

- デバイスが Active Directory ドメインに属している。
- ドメインコントローラーへのアクセスは管理者権限で承認され、これにより Active Directory のグループポリシーの作成と修正ができます。
- 設定されたインストールパッケージは、ネットワークホスティング対象の管理対象デバイス（すべての対象デバイスによる読み取りに使用できる共有フォルダー）に移動できます。
- 対象デバイスへのネットワークエージェントの導入を開始する前に、導入スキームを使用して、対象デバイスの次回の定期的な再起動を待機できる（または、これらのデバイスに対して、Windows のグループポリシーを強制的に適用できる）。

この導入スキームは以下で構成されます：

- Microsoft インストーラー形式（MSI パッケージ）のアプリケーション配布パッケージは、共有フォルダー（対象デバイスの LocalSystem アカウントに読み取り権限が付与されているフォルダー）に置かれています。
- インストールオブジェクトは、Active Directory のグループポリシー内で配布パッケージ用として作成されます。
- インストール対象を設定するには、対象デバイスが含まれている、組織単位（OU）またはセキュリティグループを指定します。
- 対象デバイスの次回のドメインへのログイン時に（デバイスユーザーがシステムにログインする前）、必要なアプリケーションの有無を調べるために、インストールされているすべてのアプリケーションがチェックされます。アプリケーションが見つからない場合は、ポリシーで指定したリソースから配布パッケージがダウンロードされてインストールされます。

この導入スキームの利点は、オペレーティングシステムの読み込み時に、ユーザーがシステムにログインする前であっても、割り当て済みアプリケーションが対象デバイスにインストールされることです。十分な権限を付与されたユーザーがアプリケーションを削除した場合でも、次回のオペレーティングシステム起動時にアプリケーションが再インストールされます。一方、この導入スキームの欠点は、デバイスが再起動されるまで、グループポリシーに対して管理者が行った変更内容が有効にならないことです（別のツールが含まれていない場合）。

ネットワークエージェントとその他のアプリケーションは、それぞれのインストーラーが Windows インストーラー形式である場合、グループポリシーを使用して両方をインストールできます。

MSI パッケージからのネットワークエージェントのインストールはサイレントモードでのみ可能であり、MSI パッケージからの対話型インストールはサポートされていません。

さらに、この導入方法を選択する際は、Windows のグループポリシー適用後に、対象デバイスにコピーするファイルの元のファイルリソースの負荷についても評価する必要があります。また、設定されたインストールパッケージをリソースに送信する方法と、関連する設定変更内容を同期させる方法を選択する必要があります。

Kaspersky Security Center のリモートインストールタスクを使用した Microsoft Windows のポリシーの処理

この導入方法は、対象デバイスを含むドメインのコントローラーへのアクセスが管理サーバーデバイスから可能であり、対象デバイスから管理サーバーの共有フォルダー（インストールパッケージが保存されている）への読み取りアクセスが可能な場合のみ使用できます。上記の理由のため、この導入方法は MSP に適用されるとはみなされません。

Microsoft Windows のポリシーを使用した、アプリケーションのサポートされていないインストール

管理者は自分用に、Windows のグループポリシー内にインストールに必要なオブジェクトを作成できます。この場合、パッケージをスタンドアロンファイルサーバーにアップロードし、そのリンクを提供する必要があります。

可能なインストールシナリオは次の通りです：

- 管理者がインストールパッケージを作成し、管理コンソールでそのプロパティをセットアップします。次に、管理者はこのパッケージの EXEC サブフォルダー全体を、Kaspersky Security Center の共有フォルダーから組織の専用ファイルリソースのフォルダーにコピーします。グループポリシーオブジェクトにより、組織の専用ファイルリソースのサブフォルダーに格納されている、このパッケージの MSI ファイルへのリンクを指定します。

- 管理者がインターネットを介してアプリケーション配布パッケージ（ネットワークエージェント用も含む）をダウンロードし、そのパッケージを組織の専用ファイルリソースにアップロードします。グループポリシーオブジェクトにより、組織の専用ファイルリソースのサブフォルダーに格納されている、このパッケージの MSI ファイルへのリンクを指定します。インストール設定は、MSI プロパティを設定するか、または MST 変換ファイルを設定することによって定義されます。

Kaspersky Security Center のリモートインストールタスクを使用した強制的な導入

ネットワークエージェントやその他のアプリケーションの初期導入を実行するには、各デバイスにローカル管理者権限を持つユーザーアカウントがあることを前提として、Kaspersky Security Center のリモートインストールタスクを使用して、選択したインストールパッケージを強制的にインストールできます。

管理サーバーがデバイスに直接アクセスできない場合は、強制インストールを適用することもできます。たとえば、デバイスが分離されたネットワーク上に配置されている場合や、管理サーバーが DMZ にあり、デバイスがローカルネットワーク上に配置されている場合が考えられます。

初期導入の場合、ネットワークエージェントはインストールされません。そのため、リモートインストールタスクの設定では、ネットワークエージェントを使用してアプリケーションのインストールに必要なファイルの配布を選択することはできません。管理サーバーまたはディストリビューションポイントを介してオペレーティングシステムリソースを使用してファイルを配布することのみを選択できます。

管理サーバーサービスは、ターゲットデバイスに対する管理者権限を持つアカウントで実行する必要があります。または、リモートインストールタスクの設定で、admin$ 共有にアクセスできるアカウントを指定することもできます。

既定では、リモートインストールタスクは、管理サーバーが実行されているアカウントの資格情報を使用してデバイスに接続します。これは、リモートインストールタスクが実行されるアカウントではなく、admin$ 共有にアクセスするために使用されるアカウントであることを明確にすることが重要です。インストールは LocalSystem アカウントで実行されます。

対象デバイスを指定する方法として、明示的に指定する（リストを使用）、対象デバイスが属する Kaspersky Security Center の管理グループを選択する、または特定の基準に基づいてデバイスの抽出内容を作成するのいずれかを使用できます。インストールの開始時刻は、タスクのスケジュールによって定義されます。タスクのプロパティで［**未実行のタスクを実行する**］設定をオンにすると、対象デバイスの電源をオンにした直後または対象デバイスを対象管理グループに移動した際に、タスクを実行できます。

強制インストールは、インストールパッケージの対象デバイスへの送信、その後の各対象デバイスの admin$ リソースへのファイルコピー、これらのデバイス上でのサポートデバイスのリモート登録で構成されます。インストールパッケージの対象デバイスへの送信は、ネットワーク対話を保証する Kaspersky Security Center 機能を介して実施されます。この場合、次の条件を満たしている必要があります：

- 対象デバイスには、管理サーバー側またはディストリビューションポイント側からアクセスできます。
- ネットワーク上で、対象デバイスの名前解決が正常に機能しています。
- 対象デバイスで、管理共有（admin$）が有効のままである。
- 対象デバイスでは次のシステムサービスが実行されています：
  - サーバー（LanmanServer）
    既定では、このサービスは実行されています。
  - DCOM サーバープロセスランチャー（DcomLaunch）
  - RPC エンドポイントマッパー（RpcEptMapper）
  - リモートプロシージャコール（RpcSs）
- Windows ツールを介したリモートアクセスを可能にするために、対象デバイスでポート TCP 445 が開かれます。

  > TCP 139、UDP 137、および UDP 138 は古いプロトコルで使用されており、現在のアプリケーションには必要ありません。

  管理サーバーおよびディストリビューションポイントから対象デバイスへの接続には、ファイアウォールで動的な送信アクセスポートを許可する必要があります。
- ネットワークエージェントを導入する時、Active Directory ドメインポリシーのセキュリティ設定により、NTLM プロトコルの動作が可能になります。
- Microsoft Windows XP を実行している対象デバイスで、シンプルファイル共有モードが無効になっている。
- 対象デバイスでは、アクセス共有とセキュリティモデルは「*クラシック – ローカルユーザーはローカルユーザー自身として認証*」に設定されます。決して「*ゲストのみ – ローカルユーザーはゲストとして認証*」に設定できません。
- 対象デバイスをドメインに属させるか、または管理者権限を付与された統一アカウントを対象デバイスで前もって作成する。

Windows Server 2003 以降の Active Directory ドメインに参加していないデバイスにネットワークエージェントまたはその他のアプリケーションを正常に展開するには、そのデバイスでリモート UAC を無効にする必要があります。リモート UAC は、ネットワークエージェントやその他のアプリケーションの強制導入に必要な admin$ にローカル管理アカウントがアクセスできない原因の 1 つです。リモート UAC を無効にしても、ローカル UAC には影響しません。

まだいずれの Kaspersky Security Center の管理グループにも割り当てられていない新しいデバイスへのインストール時には、リモートインストールタスクのプロパティを開き、ネットワークエージェントのインストール後にデバイスの移動先の管理グループを指定できます。

グループタスクの作成時には、選択したグループ内のネストされたすべてのグループにあるすべてのデバイスに対して、各グループタスクが影響を与えることに注意してください。このため、サブグループ内でインストールタスクが重複しないようにする必要があります。

アプリケーションを強制インストールするためのタスクを作成する簡単な方法は、自動インストールです。この処理を実行するには、管理グループのプロパティを開いてから、インストールパッケージのリストを開き、このグループのデバイスにインストールする必要があるパッケージを選択しなければなりません。そうすると、このグループとそのすべてのサブグループ内にあるすべてのデバイスに、選択したインストールパッケージが自動的にインストールされます。パッケージのインストールに要する時間は、ネットワークのスループットとネットワーク接続されているデバイスの合計数に応じて異なります。

インストールパッケージを対象デバイスに配信する際に管理サーバーの負荷を軽減するには、インストールタスクでディストリビューションポイント経由のインストールを選択できます。ただし、このインストール方法では、ディストリビューションポイントとして動作しているデバイスの負荷が大幅に増大するのでご注意ください。したがって、ディストリビューションポイントの要件を満たすデバイスを選択することを推奨します。ディストリビューションポイントを使用する場合は、対象デバイスをホストする分離された各サブネットにディストリビューションポイントが存在することを確認する必要があります。

小容量チャネルを介して管理サーバーと通信するサブネット内のデバイスへのインストールを実行する際に、同じサブネット内のデバイス間で大容量チャネルが使用できる場合は、ディストリビューションポイントをローカルインストールのセンターとして使用することも役に立ちます。

%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit フォルダーのパーティションの空きディスク容量は、インストールされたアプリケーションの配布パッケージの合計サイズより何倍も大きな容量にする必要があります。

Kaspersky Security Center で作成された実行中のスタンドアロンパッケージ

上述のネットワークエージェントとその他のアプリケーションの初期導入方法は、適用される条件をすべて満たすことができないため、常に実装できるわけではありません。そのような場合は、Kaspersky Security Center で、管理者によって適切なインストール設定が行われているインストールパッケージを使用して、*スタンドアロンインストールパッケージ*と呼ばれる共通の実行ファイルを作成できます。スタンドアロンインストールパッケージは、妥当であると判断される場合（Web サーバーへの外部アクセスが対象デバイスのユーザー用に設定されている）、内部 Web サーバー（Kaspersky Security Center に含まれる）上、あるいは Kaspersky Security Center Web コンソールに含まれる排他的に導入された Web サーバー上のいずれかで公開されます。また、スタンドアロンパッケージは別の Web サーバーにコピーできます。

Kaspersky Security Center を使用して、現在使用されている Web サーバー上のスタンドアロンパッケージファイルのリンクを記載したメールメッセージを、特定のユーザーに送信できます。そうすることで、（対話モードで、またはサイレントインストールのキー「-s」を使用して）ファイルを実行するようユーザーに促すことができます。Web サーバーにアクセスできないデバイスのユーザーには、スタンドアロンインストールパッケージをメールメッセージに添付して送信できます。管理者は、スタンドアロンパッケージを外部デバイスにコピーし、関連のデバイスに配布し、後で実行することもできます。

スタンドアロンパッケージは、ネットワークエージェントパッケージ、別のアプリケーションのパッケージ（セキュリティ製品のパッケージなど）、またはその両方から作成できます。スタンドアロンパッケージをネットワークエージェントパッケージと別のアプリケーションから作成した場合、インストールはネットワークエージェントを使用して起動されます。

スタンドアロンパッケージをネットワークエージェントから作成する場合、ネットワークエージェントのインストールが完了した際に、新しいデバイス（管理グループのいずれにも割り当てられていないデバイス）が自動的に割り当てられる管理グループを指定できます。

スタンドアロンパッケージは、パッケージに含まれるアプリケーションのインストール結果が表示される対話モードで実行することも（既定）、サイレントモードで実行することもできます（キー「-s」を使用して実行した場合）。サイレントモードは、スクリプト（オペレーティングシステムイメージが導入された後に実行されるように設定されているスクリプトなど）からインストールする場合に使用できます。サイレントモードでは、インストール結果はプロセスのリターンコードから判断します。

アプリケーションの手動インストールのオプション

管理者や経験豊富なユーザーは、アプリケーションを対話モードにより手動でインストールできます。元の配布パッケージ、または元の配布パッケージから作成され、Kaspersky Security Center の共通フォルダーに保存されているインストールパッケージのいずれかを使用します。既定では、インストーラーは対話モードで実行され、必要な値をすべて入力するようユーザーに促します。ただし、キー「-s」を使用してインストールパッケージのルートからプロセス setup.exe を実行した場合は、インストーラーは、インストールパッケージの設定時に定義された設定を使用して、サイレントモードで実行されます。

> インストールパッケージのルートから setup.exe を実行した場合、まずパッケージが一時的なローカルフォルダーにコピーされ、その後、アプリケーションインストーラーがローカルフォルダーから実行されます。

ネットワークエージェントがインストールされたデバイスへのアプリケーションのリモートインストール

プライマリ管理サーバー（またはそのセカンダリ管理サーバーのいずれか）に接続された操作可能なネットワークエージェントがデバイスにインストールされた場合、このデバイスのネットワークエージェントのアップグレードや、ネットワークエージェント経由でサポートされる任意のアプリケーションのインストール、アップグレード、削除が可能です。

このオプションは、リモートインストールタスクのプロパティで［**ネットワークエージェントを使用する**］をオンにすることによって有効にすることができます。

このチェックボックスが選択されている場合、管理者によってインストール設定が定義されたインストールパッケージは、ネットワークエージェントと管理サーバー間の通信チャネルを経由して対象デバイスに送信されます。

管理サーバーの負荷を最適化し、管理サーバーとデバイス間のトラフィックを最小化するには、すべてのリモートネットワークまたはすべてのブロードキャストドメインで、ディストリビューションポイントを割り当てるのが適切な方法です（「ディストリビューションポイントについて」および「管理グループの構造の構築とディストリビューションポイントの割り当て」のセクションを参照）。この場合、インストールパッケージとインストーラーの設定は、ディストリビューションポイント経由で管理サーバーから対象デバイスに配布されます。

さらに、ディストリビューションポイントをインストールパッケージのブロードキャスト（マルチキャスト）配信に使用できるため、アプリケーション導入時のネットワークトラフィックを大幅に削減できます。

ネットワークエージェントと管理サーバー間の通信チャネルを経由してインストールパッケージを対象デバイスに送信する場合、送信の準備が整っているすべてのインストールパッケージは、%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer フォルダーにもキャッシュされます。複数の様々な種別の大規模インストールパッケージと、多数のディストリビューションポイントを使用する場合、このフォルダーのサイズは急増する可能性があります。

FTServer フォルダーからファイルを手動で削除することはできません。元のインストールパッケージが削除された場合、FTServer フォルダーから関連データが自動的に削除されます。

ディストリビューションポイント側で受信したデータはすべて、%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp フォルダーに保存されます。

$FTCITmp フォルダーからファイルを手動で削除することはできません。このフォルダーのデータを使用するタスクが完了すると、このフォルダーの中身は自動的に削除されます。

インストールパッケージは、管理サーバーとネットワークエージェント間の通信チャネルを経由して、ネットワーク送信用に最適化されたフォーマットで中間リポジトリから配布されるため、各インストールパッケージの元のフォルダーに保存されたインストールパッケージへの変更は許可されていません。そのような変更は、管理サーバーによって自動的に登録されません。インストールパッケージのファイルを手動で変更する必要がある場合は、管理コンソールでインストールパッケージの設定を編集しなければなりません（ただし、このようなシナリオは回避することが推奨されます）。管理コンソールでインストールパッケージの設定を編集すると、対象デバイスへの送信準備が整っているキャッシュ内のパッケージイメージが、管理サーバーによってアップグレードされてしまいます。

リモートインストールタスクに含まれるデバイス再起動を管理する

アプリケーションのリモートインストールを完了するには（特に Windows では）、通常はデバイスの再起動が必要です。

Kaspersky Security Center のリモートインストールタスクを使用する場合、新規タスクウィザード、または作成したタスクのプロパティウィンドウ（［**OS の再起動**］セクション）で、Windows デバイスに再起動が必要な際に実行する以下の操作を選択できます：

- **デバイスを再起動しない**：自動再起動は実行されません。インストールを完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、サーバーや、継続的な操作が不可欠なその他のデバイスのインストールタスクに適切です。

- **デバイスを再起動する**：インストールの完了に再起動が必要な場合は常に、デバイスは自動的に再起動されます。このオプションは、定期的に操作が一時停止（シャットダウンまたは再起動）されるデバイスのインストールタスクに有用です。

- **ユーザーに処理を確認する**：手動での再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。［**ユーザーに処理を確認する**］は、ユーザーにとって最も好都合な時間に再起動できることが要求されるワークステーションに最適です。

アンチウイルス製品のインストールパッケージでのデータベースアップデートの適合性

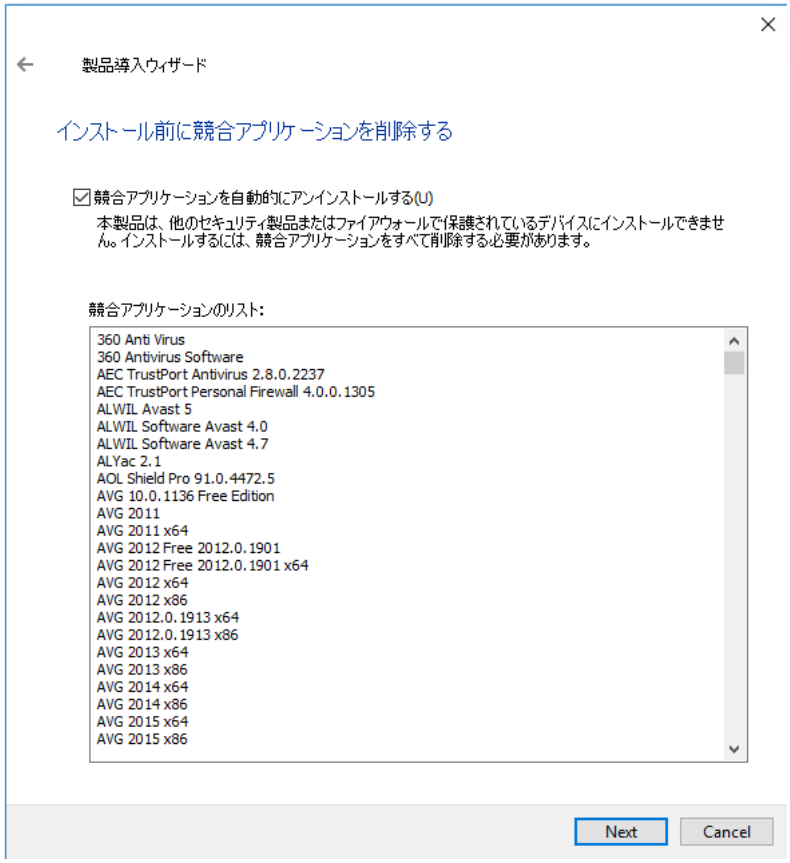
セキュリティ製品の配布パッケージと一緒に出荷された定義データベース（自動パッチのモジュールを含む）は、保護の導入を開始する前にアップデートすることが可能です。導入を開始する前に、（選択したインストールパッケージのコンテキストメニューで関連コマンドを使用するなどして）アプリケーションのインストールパッケージ内のデータベースをアップデートすることは有用です。そうすることで、対象デバイスへの保護製品の導入を完了するために必要な再起動の回数が低減されます。リモートインストールに、プライマリ管理サーバーから仮想サーバーへリレーされたインストールパッケージが関係する場合、プライマリ管理サーバー上の元のパッケージ内のデータベースをアップデートするだけで済みます。この場合、仮想サーバー上でリレーされたパッケージ内のデータベースはアップデート不要です。

サードパーティ製の競合セキュリティ製品の削除

カスペルスキーのセキュリティ製品を Kaspersky Security Center を使用してインストールする場合、インストールするアプリケーションと競合するサードパーティ製ソフトウェアを削除しなければならない場合があります。サードパーティアプリケーションを削除する方法は主に 2 つあります。

インストーラーを使用した競合アプリケーションの自動削除

インストーラーを実行すると、カスペルスキー製品と互換性がないアプリケーションのリストが表示されます。



リモートインストールウィザードに表示される、競合アプリケーションのリスト

Kaspersky Security Center が、競合アプリケーションを検出します。これにより、［**競合アプリケーションを自動的にアンインストールする**］をオンにしてインストールを続行できます。このチェックボックスをオフにして、競合アプリケーションをアンインストールしない場合、エラーが発生し、カスペルスキー製品がインストールされません。

競合アプリケーションの自動削除は、様々なインストールでサポートされています。

専用タスクを使用した競合アプリケーションの削除

競合アプリケーションを削除するには、*アプリケーションのリモートアンインストール*タスクを使用します。このタスクは、セキュリティ製品のインストールタスクの前にデバイスで実行する必要があります。たとえば、インストールタスクのスケジュール種別として［**他のタスクが完了次第**］を選択し、条件の対象となるタスクとして［*アプリケーションのリモートアンインストール*］を指定できます。

このアンインストール方法は、セキュリティ製品のインストーラーでは競合アプリケーションを適切に削除できない場合に有用です。

コマンドプロンプトを使用してパスワード保護されたネットワークエージェントを削除します

アンインストールパスワードを設定したネットワークエージェントをリモートでアンインストールするには、コマンドプロンプトを使用できます。

Kaspersky Security Center の管理下になくなったデバイスにインストールされた、パスワードで保護されたネットワークエージェントのパスワードを紛失または忘れた場合、klmover ユーティリティ、クリーナーツール（cleaner.exe）、またはコマンドプロンプトを使用してネットワークエージェントを削除することはできません。この場合、パスワードで保護されたネットワークエージェントがインストールされているデバイスにオペレーティングシステムを再インストールする必要があります。

コマンドプロンプトからネットワークエージェントをアンインストールするには：

1. アンインストールパスワードを 16 進コードに変換します。

   インターネットリソース、プログラミング環境、テキストエディター、またはその他の適切なツールを使用して、パスワードを 16 進コードに変換します。

   生成された 16 進コードを部分に分割するために使用される出力区切り文字が［`00`］に設定されていることを確認します。たとえば、16 進コード［`51 77 65 72 74 79`］は誤りですが、16 進コード［`5100770065007200740079 00`］は正しいです。

2. コマンドプロンプトに次のコマンドを入力し、**ENTER** を押します：

   `msiexec.exe /x{<製品コード>} /qn KLUNINSTPASSWD=<アンインストールパスワードの 16 進コード>`

   以下の表でネットワークエージェントの製品コードを見つけます。

ネットワークエージェント製品コード

ローカリゼーション	製品コード
アラビア語	{FA7BF140-F356-404A-BDA3-3EF0878D7C63}
ブルガリア語	{4DBF6741-FA51-4C14-AFD2-B7D9246995F6}
チェコ語	{478A6A0B-D177-4402-B703-808C05C56B13}
英語	{BCF4CF24-88AB-45E1-A6E6-40C8278A70C5}
フランス語	{2924BEDA-E0D7-4DAF-A224-50D2E0B12F5B}
ドイツ語	{2F383CB3-6D7C-449D-9874-164E49E1E0F5}
ハンガリー語	{8899A4D4-D678-49F8-AD96-0B784F58D355}
イタリア語	{DC3A3164-36B3-4FB4-B7BF-16A41C35A728}
日本語	{790C176F-7780-4C84-8B9C-455F5C0E61C5}

韓国語	{70812A40-973B-4DA1-96B9-C2011280CD99}
ポーランド語	{1A7B331A-ABBE-4230-995E-BCD99C5A18CF}
ポルトガル語	{0F05E4E5-5A89-482C-9A62-47CC58643788}
ルーマニア語	{FF802D76-E241-41D3-AAB4-DC7FBD659446}
ロシア語	{ED1C2D7E-5C7A-48D8-A697-57D1C080ABA7}
簡体字中国語	{FBD7C01E-49CB-4182-8714-9DB1EAE255CB}
スペイン語	{F03982CF-1C5C-4E12-9F9E-D36C35E62402}
スペイン語-mx	{29748B5F-D88A-4933-B614-1CCCD6EFB0B7}
繁体字中国語	{F6AD731A-36B4-4739-B1D4-70D6EDA35147}
トルコ語	{2475A66D-698B-4050-93FF-9B48EE82E2BA}

管理対象デバイスで関連する実行ファイルを実行するために、Kaspersky Security Center でアプリケーションのリモートインストール用ツールを使用する

新規パッケージウィザードを使用して、任意の実行ファイルを選択し、実行ファイルのコマンドラインの設定を定義できます。これを行うには、選択したファイルそのもの、またはこのファイルが保存されているフォルダー全体のいずれかを、インストールパッケージに追加します。次に、リモートインストールタスクを作成し、作成されたインストールパッケージを選択する必要があります。

タスクの実行中に、指定した実行ファイルが、定義したコマンドプロンプトの設定を使用して、対象デバイスで実行されます。

Microsoft Windows インストーラー（MSI）形式のインストーラーを使用する場合、Kaspersky Security Center では、標準ツールを使用してインストールの結果が分析されます。

脆弱性とパッチ管理が使用可能なライセンスがある場合、Kaspersky Security Center は、（社内の環境でサポートされるアプリケーションのインストールパッケージを作成する際に）インストールのルールと、アップデート可能な定義データベース内のインストール結果の分析も使用します。

そうでない場合は、実行ファイルの既定のタスクは、プロセスとすべての子プロセスの実行が完了するのを待ちます。実行中のプロセスがすべて完了すると、初期プロセスのリターンコードに依存せず、タスクは正常に終了します。このタスクのこのような動作を変更するには、タスクを作成する前に、新たに作成されたインストールパッケージのフォルダー内で Kaspersky Security Center が生成した kpd ファイルを手動で修正する必要があります。

実行中のプロセスの完了を待たないタスクでは、次のように、[SetupProcessResult] セクションで Wait 設定の値を 0 に設定します：

例：
```
[SetupProcessResult]
Wait=0
```

すべての子プロセスの完了を待たずに、Windows で実行中プロセスの完了のみを待つタスクでは、たとえば次のように、[SetupProcessResult] セクションで WaitJob 設定の値を 0 に設定します：

例：
```
[SetupProcessResult]
WaitJob=0
```

実行中のプロセスのリターンコードに応じて正常に終了する、またはエラーを返すタスクでは、たとえば次のように、[SetupProcessResult_SuccessCodes] セクションで正常なリターンコードを一覧表示します：

例：
[SetupProcessResult_SuccessCodes]
0=
3010=

この場合、一覧表示されたコード以外のコードではすべて、エラーが返されます。

タスク結果でタスクの正常終了やエラーのコメント文字を表示するには、たとえば次のように、[SetupProcessResult_SuccessCodes] および [SetupProcessResult_ErrorCodes] セクションで、プロセスのリターンコードに対応する簡単なエラーの説明を入力します：

例：
[SetupProcessResult_SuccessCodes]
0= インストールが正常に完了しました
3010= インストールを完了するには再起動が必要です
[SetupProcessResult_ErrorCodes]
1602= ユーザーによってインストールがキャンセルされました
1603= インストール中に致命的なエラーが発生しました

Kaspersky Security Center ツールを使用してデバイスの再起動を管理するには（操作の完了に再起動が必要な場合）、次のように、[SetupProcessResult_NeedReboot] セクションで、再起動が必要であることを示すプロセスのリターンコードを一覧表示します：

例：
[SetupProcessResult_NeedReboot]
3010=

製品導入を監視する

Kaspersky Security Center の導入を監視し、セキュリティ製品とネットワークエージェントが管理対象デバイスにインストールされていることを確認するには、［**製品の導入**］セクションのステータス信号を確認する必要があります。このステータス信号は、管理コンソールのメインウィンドウに表示される管理サーバーフォルダーの作業領域に配置されます。ステータス信号は、現在の製品導入ステータスを反映しています。ネットワークエージェントとセキュリティ製品がインストールされているデバイスの数が、ステータス信号の隣に表示されます。インストールタスクが実行中の場合は、ここで進捗状況を監視できます。インストールエラーが発生した場合は、ここにエラーの数が表示されます。リンクをクリックすると、エラーの詳細が表示されます。

［**管理対象デバイス**］フォルダーの作業領域の［**グループ**］タブにある導入状況の概要を使用することもできます。この表は、導入プロセスを反映しており、ネットワークエージェントがインストールされていないデバイス、ネットワークエージェントがインストールされているデバイス、またはネットワークエージェントとセキュリティ製品がインストールされているデバイスの数を表示します。

導入（または特定のインストールタスクの操作）の進捗状況の詳細を表示するには、該当のリモートインストールタスクの履歴ウィンドウを開きます（タスクを右クリックして、コンテキストメニューで［**履歴**］を選択）。ウィンドウには、2 つの一覧が表示されます。上の一覧には、デバイス上のタスクのステータスが表示され、下の一覧には、現在上の一覧で選択されているデバイスでのタスクイベントが表示されます。

導入エラーに関する情報は、管理サーバーの Kaspersky イベントログに追加されます。エラーに関する情報は、［**レポートと通知**］フォルダー、［**イベント**］サブフォルダー内で該当するイベントを選択する方法でも参照できます。

インストーラーを設定する

このセクションでは、Kaspersky Security Center インストーラーのファイルとインストールの設定、および管理サーバーとネットワークエージェントをサイレントモードでインストールする方法に関する推奨事項を説明します。

一般情報

Kaspersky Security Center 15.1 のコンポーネント（管理サーバー、ネットワークエージェント、および管理コンソール）のインストーラーは、Windows インストーラー技術に基づき構築されています。MSI パッケージは、インストーラーの核です。このパッケージ形式により、Windows インストーラーの提供するすべての利点、すなわち拡張性、パッチ適用システムの可用性、変換システム、サードパーティ製ソリューションを使用したインストールの一元管理、およびオペレーティングシステムによる透過的な登録を享受できます。

サイレントモードでのインストール（応答ファイルを使用した場合）

管理サーバーとネットワークエージェントのインストーラーには、応答ファイル（ss_install.xml）を利用した機能があります。応答ファイルは、ユーザーが介入しないサイレントモードでのインストールのパラメータを統合したファイルです。ss_install.xml ファイルは、MSI パッケージと同じフォルダーにあり、サイレントモードでのインストール中に自動的に使用されます。サイレントインストールモードは、コマンドラインのキー「/s」を使用して有効にできます。

実行例の概要は次の通りです：

```
setup.exe /s
```

> サイレントモードでインストーラーを起動する前に、使用許諾契約書 (EULA) をお読みください。Kaspersky Security Center Linux 配布キットに EULA のテキストを含む TXT ファイルが含まれていない場合は、カスペルスキーの Web サイト からファイルをダウンロードできます。

ss_install.xml ファイルは、Kaspersky Security Center インストーラーの内部形式のパラメータのインスタンスです。配布パッケージには、既定のパラメータを含む ss_install.xml ファイルが含まれます。

> ファイル ss_install.xml は手動で変更しないでください。このファイルは、管理コンソールでインストールパッケージのパラメータを編集する際に、Kaspersky Security Center のツールを使用して変更できます。

管理サーバーのインストール用の応答ファイルを変更するには：

1. Kaspersky Security Center 配布パッケージを開きます。完全なパッケージの EXE ファイルを使用する場合は解凍します。
2. フォルダー Server からコマンドラインを開き、次のコマンドを実行します：

   ```
   setup.exe /r ss_install.xml
   ```

   Kaspersky Security Center のインストーラーが起動します。
3. ウィザードの手順に従って、Kaspersky Security Center のインストールを設定します。

ウィザードを終了すると、指定した新しい設定に従って応答ファイルが自動的に変更されます。

サイレントモードでのネットワークエージェントのインストール（応答ファイルを使用しない場合）

単一の msi パッケージを使用してネットワークエージェントをインストールすることで、標準的な方法で MSI プロパティの値を指定できます。このシナリオでは、グループポリシーを使用してネットワークエージェントをインストールできます。

インストールパッケージ Kaspersky Network Agent.msi の名前を変更しないでください。このパッケージの名前を変更すると、ネットワークエージェントの将来のアップデート時にインストールエラーが発生する可能性があります。

MSI プロパティを使用して定義されたパラメータと、応答ファイルで定義されたパラメータが競合するのを回避するには、プロパティ `DONT_USE_ANSWER_FILE=1` に設定して、応答ファイルを無効にすることができます。MSI ファイルは、Kaspersky Security Center 配布パッケージのフォルダー Packages\NetAgent\exec にあります。msi パッケージを使用したネットワークエージェントのインストーラーの実行例は次の通りです。

サイレントモードでのネットワークエージェントのインストールには、使用許諾契約書の条項への同意が必要です。 `EULA=1` パラメータは、使用許諾契約書の内容をすべて確認し、理解した上で条項に同意する場合にのみ使用してください。

例：
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

応答ファイル（拡張子が mst のファイル）を事前に準備することで、msi パッケージのインストールパラメータを定義することもできます。このコマンドは次のようになります：

例：
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

単一のコマンドで複数の応答ファイルを指定できます。

setup.exe を使用した部分インストールの設定

setup.exe を使用してアプリケーションのインストールを実行する場合、MSI の任意のプロパティ値を msi パッケージに追加できます。

このコマンドは次のようになります：

例：
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

管理サーバーのインストールパラメータ

以下の表では、管理サーバーをインストールする際に設定できる MSI プロパティについて説明しています。EULA と PRIVACYPOLICY を除き、すべてのパラメータの指定は省略可能です。

サイレントモードでの管理サーバーのインストールのパラメータ

MSI プロパティ	説明	設定可能な値
EULA	使用許諾契約書の条項の同意（必須）	• 1 – 使用許諾契約書の内容をすべて確認し、理解した上で条項に同意します。 • その他の値または値なし – 使用許諾契約書に同意しません（インストールは実行されません）。
PRIVACYPOLICY	プライバシーポリシーの条項の同意（必須）	• 1 – プライバシーポリシーに従ってデータが処理されて送信されること（第三国への送信を含む）を理解しました。プライバシーポリシーの内容をすべて確認し、理解した上で同意します。 • その他の値または値なし – プライバシーポリシーの条項に同意しません（インストールは実行されません）。
INSTALLATIONMODETYPE	管理サーバーのインストールの種別	• 標準 • カスタム
INSTALLDIR	アプリケーションのインストールフォルダー	文字列値
ADDLOCAL	インストールする機能一覧（カンマで区切ります）	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86 管理サーバーの適切なインストールに最小限必要なコンポーネントは次の通りです： `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	ネットワークの規模	• NRT_1_100：デバイスが 1 ～ 100 台 • NRT_100_1000：デバイスが 101 ～ 1000 台 • NRT_GREATER_1000：デバイスが 1000 台以上
SRV_ACCOUNT_TYPE	管理サーバーサービスを操作するユーザーを指定する方法	• SrvAccountDefault – ユーザーアカウントを自動的に作成する • SrvAccountUser – ユーザーアカウントを手動で定義する
SERVERACCOUNTNAME	サービスのユーザー名	文字列値
SERVERACCOUNTPWD	サービスのユーザーパスワード	文字列値
DBTYPE	データベースの種別	• MySQL – MySQL データベースまたは MariaDB データベースを使用する • MSSQL – Microsoft SQL Server (SQL Express) データベースを使用する
MYSQLSERVERNAME	MySQL サーバーまたは MariDB サーバーの完全名	文字列値
MYSQLSERVERPORT	MySQL サーバーまたは MariaDB サーバーに接続するためのポートの番号	数値
MYSQLDBNAME	MySQL サーバーデータベースまたは MariaDB サーバーデータベースの名前	文字列値
MYSQLACCOUNTNAME	MySQL サーバーデータベースまたは MariaDB サーバーデータベースに接続するためのユーザー名	文字列値
MYSQLACCOUNTPWD	MySQL サーバーデータベースまたは MariaDB サーバーデータベースに接続するためのユーザーのパスワード	文字列値

MSSQLCONNECTIONTYPE	MSSQL データベースの使用種別	• InstallMSSEE – パッケージからインストールする • ChooseExisting – インストール済みサーバーを使用する
MSSQLSERVERNAME	SQL Server インスタンスの名前	文字列値
MSSQLDBNAME	SQL Server データベースの名前	文字列値
MSSQLAUTHTYPE	SQL Server に接続するための認証方法	• Windows • SQLServer
MSSQLACCOUNTNAME	SQLServer モードで SQL Server に接続するためのユーザー名	文字列値
MSSQLACCOUNTPWD	SQLServer モードで SQL Server に接続するためのユーザーのパスワード	文字列値
CREATE_SHARE_TYPE	共有フォルダーを指定する方法	• Create – 新しい共有フォルダーを作成する。この場合、次のプロパティを定義する必要があります： • SHARELOCALPATH – ローカルフォルダーへのパス • SHAREFOLDERNAME – フォルダーのネットワーク名 • Null – EXISTSHAREFOLDERNAME プロパティを指定する必要があります
EXISTSHAREFOLDERNAME	既存の共有フォルダーの完全パス	文字列値
SERVERPORT	管理サーバーに接続するためのポート番号	数値
SERVERSSLPORT	管理サーバーとの SSL 接続を確立するためのポートの番号	数値
SERVERADDRESS	管理サーバーアドレス	文字列値
SERVERCERT2048BITS	管理サーバー証明書の鍵のサイズ（ビット）	• 1 – 管理サーバー証明書の鍵のサイズは 2048 ビット • 0 – 管理サーバー証明書の鍵のサイズは 1024 ビット • 値が指定されていない場合、管理サーバー証明書の鍵のサイズは 1024 ビットです
MOBILESERVERADDRESS	モバイルデバイスの接続用管理サーバーのアドレス（MobileSupport コンポーネントが選択されていない場合は無視されます）	文字列値

ネットワークエージェントのインストール設定

以下の表では、ネットワークエージェントをインストールする際に設定できる MSI プロパティについて説明しています。SERVERADDRESS を除き、すべてのパラメータの指定は省略可能です。

MSI のプロパティ

MSI プロパティ	説明	設定可能な値
DONT_USE_ANSWER_FILE	応答ファイルからインストールパラメータを読み込む	• 1 • Null
INSTALLDIR	インストールフォルダー	
SERVERADDRESS	管理サーバーのアドレス（必須）	

SERVERPORT	管理サーバーに接続するためのポートの番号	
SERVERSSLPORT	SSL 接続のポート番号	
USESSL	SSL 接続を使用するかどうか	• 1 • Null
OPENUDPPORT	UDP ポートを開くかどうか	• 1 • Null
UDPPORT	UDP ポート番号	
USEPROXY	プロキシサーバーを使用するかどうか	• 1 • Null
PROXYADDRESS	プロキシアドレス	
PROXYPORT	管理サーバーに接続するためのポートの番号	
PROXYLOGIN	プロキシサーバーに接続するためのアカウント	
PROXYPASSWORD	プロキシサーバーに接続するためのアカウントのパスワード インストールパッケージの設定では、特別な権限を持つアカウントを指定しないでください。	
GATEWAYMODE	接続ゲートウェイの使用モード	• 0 – 接続ゲートウェイを使用しない • 1– このネットワークエージェントを接続ゲートウェイとして使用する • 2 – 接続ゲートウェイを使用して管理サーバーに接続する
GATEWAYADDRESS	接続ゲートウェイアドレス	
CERTSELECTION	証明書を取得する方法	• GetOnFirstConnection – 管理サーバーから証明書を取得します。 • GetExistent – 既存の証明書を選択します。このオプションを選択した場合は、CERTFILE プロパティを定義する必要があります。
CERTFILE	証明書ファイルのパス	
VMVDI	VDI 向け動的モードを有効にする	• 1 • Null
LAUNCHPROGRAM	インストール後にネットワークエージェントサービスを実行するかどうか	• 1 • Null

仮想インフラストラクチャ

Kaspersky Security Center では仮想マシンの使用をサポートします。ネットワークエージェントとセキュリティ製品を各仮想マシンにインストールできます。また、ハイパーバイザーレベルで仮想マシンを保護できます。前者の場合、標準セキュリティ製品または Kaspersky Security for Virtualization Light Agent のいずれかを使用して、仮想マシンを保護できます。後者の場合、Kaspersky Security for Virtualization Agentless を使用できます。

Kaspersky Security Center は、以前の状態への仮想マシンのロールバックをサポートします。

仮想マシンの負荷を軽減するヒント

Kaspersky Security Center の一部の機能は、仮想マシンに対してはそれほど有効性がないと考えられます。ネットワークエージェントを仮想マシンにインストールする場合は、それらの機能の無効化を検討することが推奨されます。

ネットワークエージェントを仮想マシンまたは仮想マシンの生成を目的とするテンプレートにインストールする場合、以下の操作を実行してください：

- リモートインストールを実行している場合、ネットワークエージェントのインストールパッケージのプロパティウィンドウの［**詳細**］セクションで、［**VDI 向けに設定を最適化する**］をオンにします。
- ウィザードを使用して対話型インストールを実行している場合、ウィザードウィンドウで［**ネットワークエージェントの設定を仮想インフラストラクチャ用に最適化します**］をオンにします。

これらのオプションを選択すると、ネットワークエージェントの設定が変更されるため、以下の機能は（ポリシーを適用する前に）既定で引き続き無効化されます：

- インストールされたソフトウェアに関する情報の取得
- ハードウェアに関する情報の取得
- 検知された脆弱性に関する情報の取得
- 必要なアップデートに関する情報の取得

これらの機能は同一のソフトウェアと仮想ハードウェアを使用しているため、通常は仮想マシンでは必須ではありません。

機能の無効化は取り消すことができます。無効にした機能が必要になった場合、ネットワークエージェントのポリシーを使用して、またはネットワークエージェントのローカル設定を使用して有効にすることができます。ネットワークエージェントのローカル設定は、管理コンソールで関連デバイスのコンテキストメニューからアクセスできます。

動的仮想マシンのサポート

Kaspersky Security Center では動的仮想マシンをサポートします。仮想インフラストラクチャが組織ネットワークに導入されている場合、動的（一時）仮想マシンを特定の条件下で使用できます。動的仮想マシンは、管理者が準備したテンプレートに基づき、一意の名前で作成されます。ユーザーがしばらくの間仮想マシンで作業して、仮想マシンの電源をオフにすると、その仮想マシンは仮想インフラストラクチャから削除されます。Kaspersky Security Center が組織ネットワークに導入されている場合、動的（一時）仮想マシンを特定の条件下で使用できます。仮想マシンの電源をオフにした後は、対応するエントリも管理サーバーのデータベースから削除する必要があります。

仮想マシンのエントリの自動削除機能を活用するには、動的仮想マシンのテンプレートにネットワークエージェントをインストールする際に、次の場所で［**VDI 向け動的モードを有効にする**］をオンにします：

- リモートインストールの場合 – ネットワークエージェントのインストールパッケージのプロパティウィンドウで（［**詳細**］セクション）
- 対話型インストールの場合 – ネットワークエージェントのインストールウィザードで

ネットワークエージェントを物理デバイスにインストールする場合は、［**VDI 向け動的モードを有効にする**］をオンにしないでください。

動的仮想マシンのイベントを、それらの仮想マシンを削除した後もしばらくの間管理サーバーに保存したい場合、管理サーバーのプロパティウィンドウの［**イベントリポジトリ**］セクションで、［**デバイスの削除後にイベントを保管する**］をオンにし、イベントの最大保管時間（日数）を指定します。

仮想マシンのコピーのサポート

ネットワークエージェントがインストールされた仮想マシンをコピーする、またはネットワークエージェントがインストールされたテンプレートを使用して仮想マシンを作成する作業は、ハードディスクイメージを取得し、コピーしてネットワークエージェントを導入する場合と同一です。通常、仮想マシンをコピーする場合は、ディスクイメージをコピーしてネットワークエージェントを導入する場合と同じアクションを実行する必要があります。

ただし、以下に説明する 2 つの方法では、ネットワークエージェントでコピーが自動的に検出されます。そのため、「デバイスのハードディスクの取得とコピーによる導入」で説明する高度な操作を実行する必要はありません：

- ネットワークエージェントのインストール時に［**VDI 向け動的モードを有効にする**］をオンにした場合：オペレーティングシステムを再起動するたびに、この仮想マシンは、コピーされたかどうかに依存せず、新しいデバイスとして認識されます。
- VMware™、HyperV®、Xen® のいずれかのハイパーバイザーが使用されている場合：ネットワークエージェントでは、変更された仮想ハードウェアの ID によって、仮想マシンのコピーが検出されます。

仮想ハードウェアにおける変更の分析機能は、完全に信頼できるわけではありません。この方法を広く採用する前に、組織が現在使用しているハイパーバイザーのバージョンを用いて、小規模な仮想マシンのプールでテストする必要があります。

ネットワークエージェントをインストールしたデバイスでのファイルシステムロールバックのサポート

Kaspersky Security Center は配信アプリケーションです。ネットワークエージェントがインストールされたデバイスでファイルシステムを以前の状態にロールバックすると、データの非同期を引き起こし、Kaspersky Security Center が正しく機能しなくなります。

ファイルシステム（またはその一部）をロールバックできるのは、次の場合です：

- ハードディスクのイメージをコピーする場合

- 仮想インフラストラクチャを使用して仮想マシンの状態を復元する場合
- バックアップコピーまたは復元ポイントからデータを復元する場合

ネットワークエージェントがインストールされたデバイスのサードパーティ製ソフトウェアが、%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ フォルダーに影響を及ぼすシナリオのみが、Kaspersky Security Center にとって重要なシナリオです。そのため、可能な場合は復元手順からこのフォルダーを常に除外する必要があります。

一部の組織では、職場のルールでデバイスのファイルシステムのロールバックが規定されているため、バージョン 10 Maintenance Release 1 より、Kaspersky Security Center では、ネットワークエージェントがインストールされたデバイスでのファイルシステムのロールバックがサポートされるようになりました（管理サーバーとネットワークエージェントはバージョン 10 Maintenance Release 1 以降でなければなりません）。これらのデバイスは検出されると、完全にデータがクレンジングおよび同期化された管理サーバーに自動的に再接続されます。

Kaspersky Security Center 15.1 では、ファイルシステムのロールバック検出機能のサポートは既定で有効になっています。

ネットワークエージェントがインストールされたデバイスにおける %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ フォルダーのロールバックは、データの完全な再同期化に大量のリソースを必要とするため、可能な限り避けてください。

管理サーバーがインストールされたデバイスでは、システムステータスのロールバックは禁じられています。管理サーバーが使用するデータベースのロールバックも同様に禁じられています。

管理サーバーの状態は、標準の klbackup ユーティリティを使用する場合にのみバックアップコピーから復元できます。

モバイルユーザー用の接続プロファイルの概要

モバイルユーザー用のノート PC（以降「デバイス」とも表記）では、企業ネットワーク内でのデバイスの現在位置によっては、管理サーバーへの接続方法を変更する、または管理サーバーを切り替える必要があります。

接続プロファイルは、Windows および macOS を実行しているデバイスでのみサポートされます。

単一の管理サーバーに対する異なるアドレスの使用

ネットワークエージェントがインストールされたデバイスは、組織の社内ネットワークかイントラネット経由で管理サーバーに接続できます。そのため、ネットワークエージェントは異なるアドレスを使用して管理サーバーに接続することが必要になる場合があります。つまり、インターネット経由で接続された場合は外部管理サーバーアドレス、社内ネットワーク経由で接続された場合は内部管理サーバーアドレスが使用されます。

これを行うには、（インターネット経由で管理サーバーに接続するための）プロファイルを、ネットワークエージェントポリシーに追加する必要があります。ポリシープロパティでプロファイルを追加します（［**接続**］セクション、［**接続プロファイル**］サブセクション）。次に、プロファイル作成ウィンドウで、［**アップデートの受信にのみ使用する**］をオフにし、［**このプロファイルで指定された管理サーバー設定と接続設定を同期する**］をオンにします。接続ゲートウェイを使用して管理サーバーにアクセスする場合（たとえば、「インターネットアクセス：DMZ 内でネットワークエージェントを接続ゲートウェイとして使用する」で説明されているような Kaspersky Security Center の設定の場合）、接続プロファイルの該当フィールドで、接続ゲートウェイのアドレスを指定する必要があります。

現在のネットワークに応じた管理サーバーの切り替え

企業に、異なる管理サーバーを使用する複数のオフィスがあり、ネットワークエージェントがインストールされた一部のデバイスが管理サーバー間を移動している場合、現在のデバイスがあるオフィスのローカルネットワークの管理サーバーに、ネットワークエージェントを接続する必要があります。

この場合、各オフィスにおいて、ネットワークエージェントのポリシーのプロパティに、管理サーバーへの接続用プロファイルを作成する必要があります。ただし、独自のホーム管理サーバーがあるホームオフィスは除きます。接続プロファイルで管理サーバーのアドレスを指定し、次のように、［**アップデートの受信にのみ使用する**］をオンまたはオフにする必要があります：

- ローカルサーバーをアップデートのダウンロードのためだけに使用する間、ネットワークエージェントをホーム管理サーバーと同期する必要がある場合は、このオプションをオンにします。
- ネットワークエージェントをローカル管理サーバーで完全に管理する必要がある場合は、このオプションをオフにします。

その後、新たに作成したプロファイルに切り替える条件を設定します。ホームオフィスを除いて、オフィスごとに少なくとも 1 つの条件を設定する必要があります。各条件は、オフィスのネットワーク環境特有の項目を検出することを目的とします。条件が真の場合、対応するプロファイルがアクティブになります。いずれの条件も真でない場合、ネットワークエージェントはホーム管理サーバーに切り替わります。

モバイルデバイス管理機能の導入

このセクションでは、モバイルデバイス管理機能の初期導入について説明します。

KES デバイスの管理サーバーへの接続

KES デバイスに対する Kaspersky Device Management for iOS では、デバイスを管理サーバーに接続する方法に応じて、次の 2 つの導入スキームが可能です：

- デバイスを管理サーバーに直接接続する導入スキーム
- Kerberos の制約付き委任をサポートするリバースプロキシを含む導入スキーム

デバイスと管理サーバーの直接接続

KES デバイスは、管理サーバーのポート 13292 に直接接続できます。

KES デバイスと管理サーバーの接続では、使用する認証方法に応じて次の 2 つの選択肢が用意されています：

- ユーザー証明書を使用してデバイスを接続する
- ユーザー証明書を使用せずにデバイスを接続する

ユーザー証明書を使用してデバイスを接続する

ユーザー証明書を使用してデバイスを接続する場合、そのデバイスは、管理サーバーツールで該当の証明書が割り当てられているユーザーアカウントと関連付けられます。

この場合、双方向 SSL 認証（相互認証）が採用されます。管理サーバーとデバイスの双方が、証明書を使用して認証されます。

ユーザー証明書を使用せずにデバイスを接続する

ユーザー証明書を使用せずにデバイスを接続する場合、そのデバイスは、管理サーバーのいかなるユーザーアカウントとも関連付けられません。ただし、デバイスが証明書を受信すると、デバイスは、管理サーバーツールで該当の証明書が割り当てられているユーザーと関連付けられます。

そのデバイスを管理サーバーに接続する場合、片方向 SSL 認証が採用されるため、管理サーバーのみがその証明書を使用して認証されます。デバイスがユーザー証明書を取得した後、認証の種類は双方向 SSL 認証（双方向 SSL 認証、相互認証）に変更されます。

Kerberos の制約付き委任（KCD）を使用して KES デバイスをサーバーに接続するスキーム

Kerberos の制約付き委任（KCD）を使用して KES デバイスをサーバーに接続するスキームでは、以下を実現します：

- KCD をサポートするリバースプロキシとの統合
- Kerberos の制約付き委任（以下、「KCD」）を使用したモバイルデバイスの認証
- 公開鍵基盤（以下、「PKI」）との統合によるユーザー証明書の適用

この接続スキームを使用する場合は、以下に留意してください：

- KES デバイスのリバースプロキシへの接続タイプは「双方向 SSL 認証」でなければなりません。つまり、デバイスは専用のクライアント証明書（ユーザー証明書）を介してリバースプロキシに接続される必要があります。これを行うには、デバイスにインストールされている Kaspersky Endpoint Security for Android のインストールパッケージに、ユーザー証明書を統合する必要があります。この KES パッケージは、このデバイス（ユーザー）専用の管理サーバーによって作成される必要があります。
- 次のように、モバイルプロトコルの既定のサーバー証明書ではなく、専用（カスタマイズ済み）の証明書を指定する必要があります：

  1. 管理サーバーのプロパティウィンドウの［**管理サーバー接続設定**］セクションの［追加のポート］で、［**モバイルデバイス用ポートを開く**］をオンにし、ドロップダウンリストで［**証明書の追加**］を選択します。
  2. 表示されたウィンドウで、モバイルプロトコルへのアクセスポイントが管理サーバーで公開された際にリバースプロキシに設定されたものと同じ証明書を指定します。

- KES デバイスのユーザー証明書は、ドメインの Certificate Authority（CA）によって発行される必要があります。ドメインに複数のルート CA が含まれる場合、クライアント証明書（ユーザー証明書）は、リバースプロキシの公開に設定されている CA によって発行される必要があることに注意してください。

  以下の方法のいずれかを使用して、ユーザー証明書が、上述の要件を満たしていることを確認できます：

  - 新規パッケージウィザードと証明書インストールウィザードで、専用のユーザー証明書を指定します。
  - 管理サーバーとドメインの PKI を統合し、証明書発行ルールの該当する設定を定義します：

1. コンソールツリーで、［**モバイルデバイス管理**］フォルダーを展開し、［**証明書**］サブフォルダーを選択します。

2. ［**証明書**］フォルダーの作業領域で［**証明書の発行ルールを指定する**］をクリックし、［**証明書発行ルール**］を開きます。

3. ［**PKI（公開鍵基盤）の統合**］セクションで、公開鍵基盤との統合を設定します。

4. ［**モバイル証明書の発行**］セクションで、証明書のソースを指定します。

以下を前提としたKerberosの制約付き委任（KCD）の設定例を次に示します：

- 管理サーバーのモバイルプロトコルへのアクセスポイントがポート13292に設定されている。
- リバースプロキシを備えたデバイスの名前は、firewall.mydom.localです。
- 管理サーバーがインストールされたデバイスの名前がksc.mydom.localである。
- モバイルプロトコルへのアクセスポイントの外部公開名がkes4mob.mydom.globalである。

管理サーバーのドメインアカウント

管理サーバーサービスが実行されるドメインアカウント（例：KSCMobileSrvcUsr）を作成する必要があります。管理サーバーサービスのアカウントは、管理サーバーのインストール時に、またはklsrvswchユーティリティを使用して指定できます。klsrvswchユーティリティは、管理サーバーのインストールフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

ドメインアカウントを指定しなければならない理由は次の通りです：

- KESデバイスの管理機能は、管理サーバーにおいて不可欠であるため。
- Kerberosの制約付き委任（KCD）が適切に機能するには、受信側（すなわち管理サーバー）がドメインアカウントで実行される必要があるため。

http/kes4mob.mydom.localのサービスプリンシパル名

ドメインのKSCMobileSrvcUsrアカウントの下で、管理サーバーがインストールされたデバイスのポート13292にモバイルプロトコルサービスを発行するSPNを追加します。管理サーバーがインストールされたkes4mob.mydom.localデバイスでは、次のようになります：

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

リバースプロキシ（firewall.mydom.local）を持つデバイスのドメインプロパティを設定します

トラフィックを委任するには、SPNで定義されたサービス（http/kes4mob.mydom.local:13292）に対してリバースプロキシ（firewall.mydom.local）を備えたデバイスを信頼する必要があります。

SPNで定義されたサービス（http/kes4mob.mydom.local:13292）に対してリバースプロキシを備えたデバイスに信頼するには、管理者は以下の操作を実行する必要があります：

1. 「Active Directory Users and Computers」という名前のMicrosoft管理コンソールスナップインで、リバースプロキシがインストールされているデバイス（firewall.mydom.local）を選択します。

2. デバイスのプロパティの［**委任**］タブで、［**このコンピューターを、指定されたサービスの委任に限って信頼する**］トグルを［**任意の認証プロトコルを使用する**］に設定します。

3. ［**このアカウントが委任された資格情報を提供できるサービス**］リストに、SPN（http/kes4mob.mydom.local:13292）を追加します。

公開専用（カスタマイズ済み）の証明書（kes4mob.mydom.global）

管理サーバーのモバイルプロトコルを公開するには、FQDN kes4mob.mydom.global 専用（カスタマイズ済み）の証明書を発行し、管理コンソールにおいて、管理サーバーのモバイルプロトコル設定で、この証明書を既定のサーバー証明書の代わりに指定する必要があります。これを行うには、管理サーバーのプロパティウィンドウの［**管理サーバー接続設定**］セクションの［追加のポート］で、［**モバイルデバイス用ポートを開く**］をオンにし、次にドロップダウンリストで［**証明書の追加**］を選択します。

サーバー証明書のコンテナー（拡張子が p12 または pfx のファイル）には、ルート証明書（公開鍵）のチェーンも含まれる必要があることに留意してください。

リバースプロキシでの公開の設定

リバースプロキシ上で、モバイルデバイス側から kes4mob.mydom.global の 13292 番ポートに向かうトラフィックについては、FQND の kes4mob.mydom.global に対して発行されたサーバー証明書を使用して、SPN（http/kes4mob.mydom.local:13292）に KCD を設定する必要があります。公開中、および公開済みのアクセスポイント（管理サーバーのポート 13292）は、同じサーバー証明書を共有する必要があることに留意してください。

Firebase Cloud Messaging の使用

Android オペレーティングシステムが管理する KES デバイスにコマンドがタイミングよく確実に配信されるようにするため、Kaspersky Security Center ではプッシュ通知のメカニズムが使用されます。プッシュ通知は、Firebase Cloud Messaging（以下、FCM）を介して KES デバイスと管理サーバー間で交換されます。Kaspersky Security Center 管理コンソールで、Firebase Cloud Messaging サービスの設定を指定することで、サービスに KES デバイスを接続できます。

Firebase Cloud Messaging の設定を取得するには、Google アカウントが必要です。

FCM の使用を有効化するには：

1. 管理コンソールで、［**モバイルデバイス管理**］フォルダー、および［**モバイルデバイス**］フォルダーを選択します。

2. ［**モバイルデバイス**］フォルダーのコンテキストメニューで、［**プロパティ**］を選択します。

3. フォルダーのプロパティで、［**Firebase Cloud Messaging の設定**］セクションを選択します。

4. ［**Firebase プロジェクト番号**］フィールドに、FCM 送信者 ID を指定します。

5. ［**秘密鍵ファイル（JSON 形式）**］フィールドで、秘密鍵ファイルを選択します。

管理サーバーとの次回の同期時に、Android オペレーティングシステムが管理する KES デバイスが、Firebase Cloud Messaging に接続されます。

Firebase Cloud Messaging の設定は、［**設定をリセット**］をクリックして編集できます。

別の Firebase プロジェクトに切り替える場合は、FCM が再開されるまで 10 分間待つ必要があります。

FCM サービスは、以下のアドレス範囲で実行されます：

- KES デバイス側では、以下のアドレスのポート 443（HTTPS）、5228（HTTPS）、5229（HTTPS）、および 5230（HTTPS）に対するアクセスが必要です：
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Google の ASN 15169 に一覧表示されたすべての IP アドレス
- 管理サーバー側では、以下のアドレスのポート 443（HTTPS）に対するアクセスが必要です：
  - fcm.googleapis.com
  - Google の ASN 15169 に一覧表示されたすべての IP アドレス

管理コンソールの管理サーバーのプロパティで、プロキシサーバー設定（［**詳細**］→［**インターネットアクセスの設定**］）が指定されている場合、その設定が FCM とのやり取りに使用されます。

FCM の設定：送信者 ID と秘密鍵ファイルの取得

FCM を設定するには：

1. Google ポータル で登録します。
2. Firebase コンソール へ移動します。
3. 次のいずれかの手順を実行します：
   - 新しいプロジェクトを作成するには、［**プロジェクトの作成**］をクリックし、画面の指示に従います。
   - 既存のプロジェクトを開きます。
4. 歯車アイコンをクリックし、［**プロジェクト設定**］を選択します。
   ［**プロジェクト設定**］ウィンドウが開きます。
5. ［**クラウドメッセージング**］タブを選択します。
6. ［**Firebase Cloud Messaging API (V1)**］セクションの［**送信者 ID**］フィールドから関連する送信者 ID を取得します。
7. ［**サービスアカウント**］タブを選択し、［**新しい秘密鍵の生成**］をクリックします。
8. 開いたウィンドウで、［**鍵の生成**］をクリックして秘密鍵ファイルを生成し、ダウンロードします。

Firebase Cloud Messaging が設定されました。

公開鍵基盤との統合

公開鍵基盤（以下、「PKI」）との統合は、管理サーバーによるドメインユーザー証明書の発行を簡略化することが主な目的です。

管理者は、管理コンソールでユーザーのドメイン証明書を割り当てることができます。この作業は、以下の方法のいずれかを使用して行うことができます：

- 証明書インストールウィザードで、ファイルから専用（カスタマイズ済み）の証明書を割り当てます。
- PKI との統合を実施し、PKI が、特定の種別の証明書、またはすべての種別の証明書のソースとして機能するようにします。

PKI との統合は、［**モバイルデバイス管理**］ - ［**証明書**］フォルダーの作業領域で、［**公開鍵基盤と統合する**］をクリックして設定できます。

ドメインユーザー証明書の発行における PKI との統合の一般原則

管理コンソールで、［**モバイルデバイス管理**］ - ［**証明書**］フォルダーの作業領域の［**公開鍵基盤と統合する**］をクリックし、管理サーバーがドメインの CA（以下、「PKI との統合が実施されるアカウント」）経由でドメインユーザー証明書を発行するために使用するドメインアカウントを指定します。

以下に留意してください：

- PKI との統合の設定では、すべての種別の証明書に対して既定のテンプレートを指定できます。証明書の発行ルール（［**モバイルデバイス管理**］ - ［**証明書**］フォルダーの作業領域で、［**証明書の発行ルールを指定する**］をクリック）では、すべての種別の証明書に対して個別のテンプレートを指定できることに留意してください。
- PKI との統合が実施されるアカウントの証明書リポジトリで、専用の Enrollment Agent（EA）証明書が、管理サーバーがインストールされたデバイスにインストールされる必要があります。Enrollment Agent（EA）証明書は、ドメインの CA（Certificate Authority）の管理者によって発行されます。

PKI との統合が実施されるアカウントは、以下の基準を満たす必要があります：

- ドメインユーザーである。
- PKI との統合を開始した管理サーバーがインストールされたデバイスのローカル管理者である。
- *サービスとしてログオン*する権限がある。
- 管理サーバーがインストールされたデバイスは、永続的なユーザープロファイルを作成するために、少なくとも 1 度はこのアカウントで実行される必要がある。

Kaspersky Security Center Web サーバー

Kaspersky Security Center Web サーバー（「Web サーバー」とも表記）は、Kaspersky Security Center のコンポーネントです。Web サーバーは、スタンドアロンインストールパッケージ、モバイルデバイス用スタンドアロンインストールパッケージ、および共有フォルダーのファイルを公開することを目的に設計されています。

インストールパッケージは、Web サーバーで自動的に公開され、初回のダウンロード後に削除されます。管理者は、メールなど便利な方法を利用して、ユーザーに新しいリンクを送信します。

ユーザーはそのリンクをクリックして、必要な情報をモバイルデバイスにダウンロードできます。

Web サーバーの設定

Web サーバーの微調整が必要な場合は、Web サーバーのプロパティで、HTTP（8060）および HTTPS（8061）のポートを変更できます。ポートの変更に加えて、HTTPS のサーバー証明書を置き換えることや、HTTP の Web サーバーの FQDN を変更することが可能です。

その他の定期作業

このセクションでは、Kaspersky Security Center での定期作業に関する推奨事項について説明します。

管理コンソールでステータス信号およびログに記録されたイベントを監視する

管理コンソールでは、ステータス信号を確認することで、Kaspersky Security Center と管理対象デバイスの現在のステータスをすぐに参照できます。ステータス信号は、［**管理サーバー**］フォルダーの作業領域の［**監視**］タブに表示されます。このタブには、ステータス信号が表示された 6 つの情報パネルおよびログされたイベントがあります。ステータス信号とは、パネルの左側に表示される色付きの縦線です。ステータス信号が表示された各パネルは、Kaspersky Security Center の特定の機能範囲に対応しています（以下の表を参照）。

管理コンソールのステータス信号の対象範囲

パネル名	ステータス信号の範囲
製品の導入	組織ネットワーク内のデバイスへのネットワークエージェントとセキュリティ製品のインストール
管理スキーム	管理グループの構造。ネットワークのスキャン。デバイス移動ルール
プロテクション設定	セキュリティ製品の機能：保護ステータス、マルウェアスキャン
アップデート	アップデートとパッチ
監視	保護ステータス
管理サーバー	管理サーバーの機能とプロパティ

各ステータス信号は、以下の 5 色で表されます（下表を参照）。ステータス信号の色は、Kaspersky Security Center の現在のステータスと、記録されたイベントに基づきます。

ステータス信号の色コード

ステータス	ステータス信号の色	ステータス信号の色の意味
情報	緑	管理者の介入は必要ありません
警告	黄	管理者の介入が必要です。
緊急	赤	重大な問題が発生しました。問題を解決するには、管理者の介入が必要です。
情報	水色	管理対象デバイスのセキュリティに対する潜在的脅威または実際の脅威とは無関係のイベントが記録されました
情報	灰色	イベントの詳細が不明であるか、まだ取得されていません

［**監視**］タブのすべての情報パネルのステータス信号の色を緑にすることが、管理者の目標となります。

情報パネルには、ステータス信号と Kaspersky Security Center のステータスに影響するログに記録されたイベントも表示されます（下の表を参照）。

ログに記録されたイベントの名前、説明、およびステータス信号の色

ステータス信号の色	イベント種別の表示名	イベント種別	説明
赤	**%1 台のデバイスでライセンスの有効期間が終了しました**	IDS_AK_STATUS_LIC_EXPAIRED	この種別のイベントは、製品版ライセンスの有効期間が終了する時に発生します。 Kaspersky Security Center は 1 日 1 回、デバイスでライセンスの有効期限が切れているかどうかを確認します。 製品版ライセンスの有効期間が終了した場合は、Kaspersky Security Center は基本機能のみを提供します。 Kaspersky Security Center の使用を継続するには、製品版ライセンスを更新してください。
赤	**セキュリティによる保護が実行されていません：%1 台のデバイス**	IDS_AK_STATUS_AV_NOT_RUNNING	このタイプのイベントは、デバイスにインストールされているセキュリティ製品が実行されていない時に発生します。 Kaspersky Endpoint Security がデバイスで実行されていることを確認します。
赤	**プロテクションが無効になっています：%1 台のデバイス**	IDS_AK_STATUS_RTP_NOT_RUNNING	このタイプのイベントは、デバイス上のセキュリティ製品が指定された時間間隔より長く無効になっている場合に発生します。 デバイスのリアルタイム保護の現在のステータスを確認し、必要なすべての保護コンポーネントが有効になっていることを確認します。
赤	**デバイスでソフトウェアの脆弱性が検知されました**	IDS_AK_STATUS_VULNERABILITIES_FOUND	このタイプのイベントは、*脆弱性とアプリケーションのアップデートの検索*タスクが、デバイスにインストールされているアプリケーションで指定された深刻度の脆弱性を検知した時に発生します。 ［**アプリケーションの管理**］フォルダーの［**ソフトウェアのアップデート**］サブフォルダーで、適用可能なアップデートのリストをオンにします。このフォルダーには、管理サーバーが取得した、デバイスへ配信可能な Microsoft アプリケーションやその他のソフトウェア会社の製品のアップデートのリストが含まれます。 適用可能なアップデートの情報を確認した後、アップデートをデバイスにインストールできます。
赤	**緊急イベントが管理サーバーに登録されました**	IDS_AK_STATUS_EVENTS_OCCURED	このタイプのイベントは、管理サーバーの緊急イベントが検知された時に発生します。 管理サーバーに保存されているイベントのリストを確認し、緊急イベントを 1 つずつ修正します。
赤	**エラーが管理サーバーのイベントに登録されました**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	このタイプのイベントは、管理サーバー側で予期しないエラーが記録された時に発生します。 管理サーバーに保存されているイベントのリストを確認し、エラーを 1 つずつ修正します。
赤	**%1 台のデバイスとの接続が切断されました**	IDS_AK_STATUS_ADM_LOST_CONTROL1	このタイプのイベントは、管理サーバーとデバイス間の接続が失われた時に発生します。 切断されたデバイスのリストを表示し、それらを再接続してみてください。
赤	**%1 台のデバイスが管理サーバーに長期間接続されていません**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	このタイプのイベントは、デバイスの電源がオフになっているために、指定された時間内にデバイスが管理サーバーに接続されなかった場合に発生します。 デバイスの電源が入っていて、ネットワークエージェントが実行されていることを確認してください。
赤	**%1 台のデバイスが「OK」以外のステータスです**	IDS_AK_STATUS_HOST_NOT_OK	このタイプのイベントは、管理サーバーに接続されているデバイスの［*OK*］ステータスが［*緊急*］または［*警告*］に変化した時に発生します。

			Kaspersky Security Center のリモート診断ユーティリティを使用して、問題をトラブルシューティングできます。
赤	**定義データベースがアップデートされていません：%1 台のデバイス**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	このタイプのイベントは、定義データベースが指定された時間内にデバイスで更新されなかった場合に発生します。 指示に従って Kaspersky 定義データベースをアップデートします。
赤	**Windows Update 更新プログラムのチェックが長期間実行されていないデバイス：%1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	このタイプのイベントは、*Windows Update の同期の実行*タスクが指定された時間間隔内に実行されなかった時に発生します。 指示に従って、Windows Update の更新プログラムと管理サーバーとの同期を行います。
赤	**Kaspersky Security Center 用の %1 個のプラグインをインストールする必要があります**	IDS_AK_STATUS_PLUGINS_REQUIRED2	このタイプのイベントは、カスペルスキー製品用の追加のプラグインをインストールする必要がある時に発生します。 カスペルスキーのテクニカルサポートの Web ページから、カスペルスキー製品に必要な管理プラグインをダウンロードしてインストールします。

管理対象デバイスへのリモートアクセス

このセクションでは、管理対象デバイスへのリモートアクセスについて説明します。

［管理サーバーから切断しない］オプションを使用して、管理対象デバイスと管理サーバー間の継続的な接続を提供する

プッシュサーバーを使用しない場合、Kaspersky Security Center は、管理対象デバイスと管理サーバー間の継続的な接続を提供しません。管理対象デバイスのネットワークエージェントが、定期的に接続を確立し、管理サーバーと同期させます。同期セッションの間隔は、ネットワークエージェントのポリシーで定義されます。早期の同期実行が必要な場合、管理サーバー（または、使用されているディストリビューションポイント）は署名されたネットワークパケットを、IPv4 または IPv6 ネットワーク経由でネットワークエージェントの UDP ポートへ送信します。既定では、ポート番号は 15000 です。管理サーバーと管理対象デバイスとの間で UDP を使用した接続が確立できない場合、同期間隔の間の次の定期接続時に、ネットワークエージェントと管理サーバー間で同期が実行されます。

一部の動作は、ネットワークエージェントと管理サーバーが事前に接続されていないと実行できません。例：ローカルタスクの実行と停止、管理対象アプリケーションの統計情報の受信、トンネリング接続の作成など。この問題を解決するには、プッシュサーバーを使用していない場合は、［**管理サーバーから切断しない**］オプションを使用し、管理対象デバイスと管理サーバーの間に継続的な接続があることを確認します。

クライアントデバイスと管理サーバー間の継続的な接続を確認するには：

1. コンソールツリーで、［**管理対象デバイス**］フォルダーを選択します。
2. フォルダーのワークスペースで、継続的な接続を提供する管理対象デバイスを選択します。
3. デバイスのコンテキストメニューで［**プロパティ**］を選択します。
   選択したデバイスのプロパティウィンドウが表示されます。
4. 表示されたウィンドウの［**全般**］セクションで、［**管理サーバーから切断しない**］をオンにします。

継続的な接続が、管理デバイスと管理サーバー間で確立されます。

［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

デバイスと管理サーバー間の接続時間の確認について

デバイスのシャットダウン時に、ネットワークエージェントは管理サーバーにシャットダウンを通知します。管理コンソールでは、そのデバイスはシャットダウンと表示されます。ただし、ネットワークエージェントがすべてのシャットダウンを管理サーバーに通知できるわけではありません。そのため、管理サーバーは、各デバイスの［**管理サーバーへの接続**］属性（この属性の値は、管理コンソールのデバイスプロパティの［**全般**］セクションに表示されます）を定期的に分析し、ネットワークエージェントの現在の設定の同期間隔と比較します。あるデバイスが連続した同期間隔に 3 回を超えて応答していない場合、そのデバイスはシャットダウンとマーク付けされます。

強制同期について

Kaspersky Security Center では、管理対象デバイスのステータス、設定、タスク、ポリシーは自動的に同期されますが、場合によっては、現時点において指定されたデバイスで同期が実行されているかどうかを管理者が正確に知る必要があります。

管理コンソールにおける管理対象デバイスのコンテキストメニューでは、［**すべてのタスク**］メニューに［**強制同期**］コマンドが含まれます。Kaspersky Security Center 15.1 がこのコマンドを実行すると、管理サーバーはデバイスへの接続を試みます。この試行が成功すると、強制同期が実行されます。試行が失敗した場合は、ネットワークエージェントと管理サーバー間の次の定期接続まで待機してから同期が強制的に実行されます。

トンネリングについて

Kaspersky Security Center では、管理コンソールから管理サーバーを経由し、次にネットワークエージェントを経由して、管理対象デバイスの指定されたポートに到達する TCP 接続のトンネリングが可能です。トンネリングは、管理コンソールと管理対象デバイスを直接接続できない場合に、管理コンソールがインストールされたデバイスのクライアントアプリケーションを、管理対象デバイスの TCP ポートに接続するように設計されています。

たとえばトンネリングは、リモートデスクトップへの接続に使用され、既存セッションへの接続と新しいリモートセッションの作成の双方に対応しています。

トンネリングは、外部ツールを使用して有効にすることもできます。たとえば、管理者はこの方法で PuTTY ユーティリティ、VNC クライアント、およびその他のツールを実行できます。

サイジングガイド

このセクションでは、Kaspersky Security Center のサイジングについて説明します。

このガイドの概要

このガイドは、Kaspersky Security Center 15.1（以降、単に「Kaspersky Security Center」とも表記）をインストールおよび管理する担当者、および Kaspersky Security Center を使用する組織をサポートする担当者を対象としています。

カスペルスキー製品がインストールされたデバイス（モバイルデバイスを含む）の保護を Kaspersky Security Center によって管理するネットワークに対するすべての推奨事項と計算について説明します。モバイルデバイスなどその他の管理対象デバイスについては別途検討すべき内容がある場合、説明内で明示します。

様々な運用状況で最適なパフォーマンスを実現し維持するには、ネットワークに接続されたデバイスの数、ネットワークのトポロジー、必要な Kaspersky Security Center の機能を考慮する必要があります。

このガイドでは、次の項目について説明します：

- Kaspersky Security Center の制限
- Kaspersky Security Center の主要なコンポーネントに関する計算（管理サーバーとディストリビューションポイント）：
  - 管理サーバーとディストリビューションポイントのハードウェア要件
  - 管理サーバーの数と階層の算出
  - ディストリビューションポイントの数の計算と設定
- ネットワーク上のデバイス数に応じてイベントのデータベースへの記録を設定
- パフォーマンス最適化のための一般的なベストプラクティス
- Kaspersky Security Center のパフォーマンスを最適化するためのタスクの設定
- Kaspersky Security Center 管理サーバーと保護されるデバイスとの間のトラフィックレート（ネットワーク負荷）

このガイドは、以下の場合に参照してください：

- Kaspersky Security Center のインストールに先立ってリソースを計画する時
- Kaspersky Security Center が導入されているネットワークの規模の大幅な変更を計画する時
- テスト環境用の限定されたネットワークセグメントで Kaspersky Security Center を使用する段階から組織のネットワークへ Kaspersky Security Center を全面的に導入する段階へ移行する時
- 使用する Kaspersky Security Center の機能を変更する時

Kaspersky Security Center の制限に関する情報

以下の表では、現在のバージョンの Kaspersky Security Center の制限事項を示しています。

Kaspersky Security Center の制限

制限の種別	値
管理サーバーあたりの管理対象デバイスの最大数	100000
［**管理サーバーから切断しない**］がオンになっているデバイス数の上限	300
管理グループ数の上限	10,000
保存するイベント数の上限	45,000,000
ポリシーの数の上限	2000
タスクの数の上限	2000
Active Directory オブジェクト（ユーザー、デバイス、セキュリティグループの組織単位（OU）とアカウント）の合計数の上限	1,000,000
ポリシーのプロファイル数の上限	100
単一のプライマリ管理サーバー上のセカンダリ管理サーバー数の上限	500
仮想管理サーバー数の上限	500
単一のディストリビューションポイントが対象にすることができるデバイス数の上限（ディストリビューションポイントはモバイルデバイス以外のみをサポートできます）	10,000
単一の接続ゲートウェイを使用できるデバイス数の上限	10,000（モバイルデバイスを含む）
管理サーバーあたりのモバイルデバイスの最大数	100,000 − モバイル以外の管理対象デバイスの数

管理サーバーの計算

このセクションでは、管理サーバーとして使用するデバイスのソフトウェアおよびハードウェア要件について説明します。また、組織のネットワークの構成に応じた管理サーバーの数と階層を計算する際の推奨事項についても説明します。

管理サーバーのハードウェアリソースの計算

このセクションでは、管理サーバー用のハードウェアリソースを計画するための指針となる計算について説明します。脆弱性とパッチ管理機能を使用する際のディスク空き容量の計算に関する推奨事項については、別に説明します。

DBMS および管理サーバーのハードウェア要件

テストによって得られた DBMS および管理サーバーのハードウェア最小要件は、下記の表で示す通りです。サポートされるオペレーティングシステムと DBMS の完全なリストについては、システム要件のリストを参照してください。

管理サーバーと DBMS が別のデバイスにあり、ネットワークに 50,000 台のデバイスがある

管理サーバーがインストールされたデバイスの構成

ハードウェア	値
CPU	4 cores、2500 MHz
メモリ	8 GB
ハードディスク	300 GB、RAID（推奨）
ネットワークアダプター	1 Gbit

DBMS がインストールされたデバイスの構成

ハードウェア	値
CPU	4 cores、2500 MHz
メモリ	16 GB
ハードディスク	200 GB、SATA RAID
ネットワークアダプター	1 Gbit

管理サーバーと DBMS が同じデバイスにあり、ネットワークに 50,000 台のデバイスがある

管理サーバーと DBMS がインストールされたデバイスの構成

ハードウェア	値
CPU	8 コア、2500 MHz
メモリ	16 GB
ハードディスク	500 GB、SATA RAID
ネットワークアダプター	1 Gbit

管理サーバーと DBMS が別のデバイスにあり、ネットワークに 100,000 台のデバイスがある

管理サーバーがインストールされたデバイスの構成

ハードウェア	値
CPU	8 コア、2.13 GHz
メモリ	8 GB
ハードディスク	1 TB、RAID 使用
ネットワークアダプター	1 Gbit

DBMS がインストールされたデバイスの構成

ハードウェア	値
CPU	8 コア、2.53 GHz
メモリ	26 GB
ハードディスク	500 GB、SATA RAID
ネットワークアダプター	1 Gbit

テストは次の設定で実行されました：

- ディストリビューションポイントの自動割り当てが管理サーバー上で有効になっている、または、ディストリビューションポイントが推奨条件に従って手動で割り当てられている。

- バックアップタスクが、専用サーバーのファイルリソースにバックアップコピーを保存する。
- ネットワークエージェントの同期間隔が、以下の表で指定されたとおりに設定されている。

ネットワークエージェントの同期間隔

同期間隔（分）	管理対象デバイスの数
15	10,000
30	20000
45	30,000
60	40,000
75	50,000
150	100000

データベースの容量の計算

データベースのために予約する必要のあるディスク容量は次の計算式で計算できます：

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

説明：

- C はデバイスの数です。
- E は保存するイベントの数です。
- A は Active Directory オブジェクトの合計数です：
  - デバイスアカウント
  - ユーザーアカウント
  - セキュリティグループのアカウント
  - Active Directory 組織単位

  Active Directory のスキャンを無効化すると、A はゼロになります。
- N は、エンドポイントデバイスでインベントリされた実行可能ファイルの平均数です。
- F は、実行ファイルがインベントリされたエンドポイントデバイスの数です。

Kaspersky Endpoint Security のポリシーの設定で、実行しているアプリケーションに関する管理サーバーの通知を有効にする場合、実行しているアプリケーションについての情報をデータベースに保存するために (0.03 * C) GB を追加する必要があります。

管理サーバーで Windows Update を配信している（Windows Server Update Services サーバーとして動作する）と、データベースは追加で 2.5 GB の容量が必要になります。

動作中には、データベース内に*未割り当て領域*が常に存在します。そのため、実際のデータベースファイル（SQL Server を DBMS として使用している場合、既定では KAV.MDF ファイル）のサイズは、概算でデータベースが占有するディスク容量の倍の大きさになります。

トランザクションログ（SQL Server を DBMS として使用している場合、既定では KAV_log.LDF ファイル）のサイズを明示的に制限することは推奨されません。MAXSIZE パラメータの既定値を変更せずに使用することが推奨されます。ただし、このファイルの容量を制限する必要がある場合は、KAV_log.LDF で一般的に必要となる容量が 20480 MB であることを考慮した上で MAXSIZE パラメータを設定してください。

ディスク空き容量の計算（脆弱性とパッチ管理機能を使用する場合としない場合）

脆弱性とパッチ管理機能を使用しない場合のディスク空き容量の計算

管理サーバーの %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit フォルダーに必要な容量の見積もりは、次の式で概算できます：

(724 * C + 0.15 * E + 0.17 * A) KB

説明：

- C はデバイスの数です。
- E は保存するイベントの数です。
- A は Active Directory オブジェクトの合計数です：
  - デバイスアカウント
  - ユーザーアカウント
  - セキュリティグループのアカウント
  - Active Directory 組織単位

Active Directory のスキャンを無効化すると、A はゼロになります。

脆弱性とパッチ管理機能を使用する場合の追加容量の計算

- アップデート：アップデートを保存するには、共有フォルダーに少なくとも 4 GB の追加容量が必要です。
- インストールパッケージ：インストールパッケージを管理サーバーに保存する場合、共有フォルダーには、インストールに使用できるすべてのインストールパッケージの合計サイズと同等の空き容量が追加で必要です。
- リモートインストールタスク：リモートインストールタスクが管理サーバー上にある場合、インストール対象となるインストールパッケージの合計サイズと同等の空き容量が（フォルダー %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit に）追加で必要です。
- パッチ：パッチのインストールに管理サーバーを使用する場合、以下の追加容量が必要です：
  - パッチフォルダーには、ダウンロードしたすべてのパッチの合計サイズと同等の空き容量が必要です。既定では、パッチはフォルダー %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles に保存されます。

klsrvswch ユーティリティを使用して、パッチを保存するための別のフォルダーを指定できます。klsrvswch ユーティリティは、管理サーバーがインストールされているフォルダーにあります。既定のインストールパス：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

管理サーバーが WSUS サーバーとして使用されている場合、このフォルダーには少なくとも 100 GB を割り当てることが推奨されます。

- %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit フォルダーに、アップデート（パッチ）のインストールと脆弱性の修正を行うタスクの既存インスタンスによって参照されるパッチの合計サイズと同等の空き容量が必要です。

管理サーバーの数と構成の算出

プライマリ管理サーバーの負荷を軽減するため、各管理グループに管理サーバーを割り当てることができます。セカンダリ管理サーバーの数は、プライマリ管理サーバーあたり 500 を超えることができません。

組織のネットワークの構成に対応した管理サーバーの構成を作成することを推奨します。

動的仮想マシンを Kaspersky Security Center に接続する際の推奨事項

動的仮想マシン（単に「動的 VM」とも表記）は、静的仮想マシンより多くのリソースを消費します。

動的仮想マシンの詳細については、「動的仮想マシンのサポート」を参照してください。

新しい動的 VM が接続されると、Kaspersky Security Center は管理コンソールにこの動的 VM のアイコンを作成し、動的 VM を管理グループに移動します。その後、動的 VM が管理サーバーデータベースに追加されます。管理サーバーは、この動的 VM にインストールされたネットワークエージェントと完全に同期されます。

組織のネットワークでは、ネットワークエージェントは動的 VM ごとに次のネットワークリストを作成します：

- ハードウェア
- インストールされたソフトウェア
- 検知された脆弱性
- アプリケーションコントロールコンポーネントのイベントおよび実行可能ファイルのリスト

ネットワークエージェントは、これらのネットワークリストを管理サーバーに転送します。ネットワークリストのサイズは、動的 VM にインストールされているコンポーネントによって決まり、Kaspersky Security Center とデータベース管理システム（DBMS）のパフォーマンスに影響を与える可能性があります。負荷は非線形に増加する可能性があります。

ユーザーが動的 VM の操作を終了してオフにすると、このマシンは仮想インフラストラクチャから削除され、このマシンに関するエントリは管理サーバーデータベースから削除されます。

これらの操作はいずれも、Kaspersky Security Center と管理サーバーデータベースのリソースを大量に消費し、Kaspersky Security Center と DBMS のパフォーマンスを低下させる可能性があります。Kaspersky Security Center に接続する動的 VM は、最大 20,000 台にすることを推奨します。

接続された動的 VM が標準的な操作（データベースのアップデートなど）を実行し、メモリの消費が 80% 以内、使用可能なコアの消費が 75 ～ 80% 程度であれば、20,000 台以上の動的 VM を Kaspersky Security Center に接続できます。

動的 VM のポリシー設定、ソフトウェア、またはオペレーティングシステムを変更すると、リソースの消費が増減する可能性があります。80 ～ 95% のリソース消費が最適と判断されます。

ディストリビューションポイントと接続ゲートウェイの計算

このセクションでは、ディストリビューションポイントとして使用するデバイスのハードウェア要件と、組織のネットワークの構成に応じたディストリビューションポイントおよび接続ゲートウェイの数を計算する際の推奨事項について説明します。

ディストリビューションポイントの要件

10,000 台以下のクライアントデバイスでディストリビューションポイントを使用する場合、次の最小要件を満たしている必要があります（テストスタンドでの設定値）：

- CPU：Intel® Core™ i7-7700 CPU（3.60 GHz 4 コア）
- メモリ：8 GB
- 空きストレージ容量：120 GB

管理サーバー上でリモートインストールタスクが実行を待っている場合、ディストリビューションポイントがあるデバイスには、インストール対象となるインストールパッケージの合計サイズと同等の空き容量が必要です。

管理サーバー上でアップデート（パッチ）のインストールタスクと脆弱性の修正タスクが 1 つ以上保留されている場合、ディストリビューションポイントが動作しているデバイスには、インストールするすべてのパッチの合計サイズの 2 倍の空きディスク容量が追加で必要です。

ディストリビューションポイントがカスペルスキーのアップデートサーバーから直接定義データベースとアプリケーションソフトウェアモジュールのアップデートを受信するスキームを使用する場合は、ディストリビューションポイントがインターネットに接続されている必要があります。

ディストリビューションポイントの数の計算と設定

ネットワークに存在するクライアントデバイスの数に応じて、必要となるディストリビューションポイントの数も多くなります。ディストリビューションポイントの自動割り当ては、できるだけ使用しないでください。ディストリビューションポイントの自動割り当てが有効になっており、クライアントデバイスの数が非常に多い場合、管理サーバーがディストリビューションポイントの割り当てと設定を行います。

用途専用のディストリビューションポイントの使用

特定のデバイスをディストリビューションポイントとして使用する場合（たとえば、この用途専用で割り当てられたサーバー）、ディストリビューションポイントの自動割り当ては使用しないでください。また、ディストリビューションポイントとして使用するデバイスは、十分な空きディスク容量があること、定期的にシャットダウンされないこと、スリープモードが無効になっていることを確認してください。

単一のセグメントで構成されるネットワーク上での、デバイス数に応じた用途専用のディストリビューションポイントの数

ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
300 台未満	0（ディストリビューションポイントを割り当てない）
300 以上	許容：N/10,000 + 1、推奨：N/5,000 + 2（N はネットワーク上のデバイスの数）

複数のセグメントで構成されるネットワーク上での、デバイス数に応じた用途専用のディストリビューションポイントの数

各ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
10 台未満	0（ディストリビューションポイントを割り当てない）
10～100	1
100 以上	許容：N/10,000 + 1、推奨：N/5,000 + 2（N はネットワーク上のデバイスの数）

通常のクライアントデバイス（ワークステーション）のディストリビューションポイントとしての使用

通常のクライアントデバイス（ワークステーション）をディストリビューションポイントとして使用する場合、管理サーバーと通信チャネルの負荷低減のために、下表に従ってディストリビューションポイントを割り当ててください。

単一のセグメントで構成されるネットワーク上での、デバイス数に応じた、ディストリビューションポイントとして動作するワークステーションの数

ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
300 台未満	0（ディストリビューションポイントを割り当てない）
300 以上	N/300 + 1（N はネットワーク上のデバイスの数。ただし、ディストリビューションポイントは 3 台以上必要）

複数のセグメントで構成されるネットワーク上での、デバイス数に応じた、ディストリビューションポイントとして動作するワークステーションの数

各ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
10 台未満	0（ディストリビューションポイントを割り当てない）
10～30	1
31～300	2
300 以上	N/300 + 1（N はネットワーク上のデバイスの数。ただし、ディストリビューションポイントは 3 台以上必要）

ディストリビューションポイントがシャットダウンされた（もしくは、何らかの理由により使用できない）場合も、ディストリビューションポイントの対象範囲に含まれる管理対象デバイスは管理サーバーにアクセスしてアップデートを取得できます。

接続ゲートウェイの数の計算

接続ゲートウェイを使用する場合、接続ゲートウェイ専用のデバイスを割り当てることを推奨します。

また、接続ゲートウェイに接続できる管理対象デバイスは、モバイルデバイスを含めて最大で 10,000 台です。

タスクおよびポリシーのイベントに関する情報の記録

このセクションでは、管理サーバーのデータベースに保存するイベントに関する計算と、イベントの数を最小限にして管理サーバーの負荷を低減する方法に関する推奨事項について説明します。

既定では、各タスクおよびポリシーのプロパティによって、タスクの実行およびポリシーの適用に関するすべてのイベントが保存されます。

しかし、タスクが頻繁に（週に数回など）多くのデバイス（たとえば 10,000 台以上）に対して実行される場合、イベントの数が多すぎてデータベースの容量を超えてしまうことがあります。この場合、タスクの設定で次のいずれかを選択してください：

- **タスクの進捗に関連したイベントを保存**：この場合、データベースは、タスクの開始、進捗、完了（成功、警告、エラー）に関する情報のみを、タスクが実行されるデバイスから受信します。
- **タスク実行結果のみ保存**：この場合、データベースは、タスクの完了（成功、警告、エラー）に関する情報のみを、タスクが実行されるデバイスから受信します。

ポリシーが多くのデバイス（たとえば 10,000 台以上）に対して定義されている場合も、イベントの数が多すぎてデータベースの容量を超えてしまうことがあります。この場合、ポリシーの設定で、最も緊急イベントのみ記録を有効にしてください。その他のイベントは記録を無効にします。

それにより、データベース内のイベントの数を削減することで、データベース内のイベントの分析を伴う操作の実行速度を向上し、多数のイベントによって緊急イベントが上書きされる可能性を低下させることができます。

また、タスクまたはポリシーに関連するイベントの保存期間を短くすることもできます。既定の期間は、タスクに関連するイベントは 7 日、ポリシーに関連するイベントは 30 日です。イベントの保存期間を変更する際は、組織で運用している業務手順と、システム管理者がイベントを分析するのにかかる時間を考慮してください。

次の場合には、イベントの保存期間を変更してください：

- グループタスクの中間状態の変更に関するイベントやポリシー適用に関するイベントが、Kaspersky Security Center データベース内のすべてのイベントの大部分を占める場合。
- データベースに保存できるイベント数の上限を超え、イベントの自動削除に関する項目が Kaspersky イベントログに記録される場合。

1 つのデバイスから送信されるイベントの数が 1 日あたり 20 を超えないように、イベント記録オプションを選択してください。必要に応じて、この上限をわずかに超過することができますが、そのためにはネットワークに接続されたデバイスの数が比較的少数（10,000 未満）である必要があります。

タスクごとの考慮事項と最適な設定

タスクによっては、ネットワーク上のデバイスの数に関して特別な考慮事項があります。このセクションでは、そのようなタスクに推奨される最適な設定について説明します。

デバイスの検索、データバックアップタスク、管理サーバーのメンテナンスタスク、Kaspersky Endpoint Security をアップデートするグループタスクは、Kaspersky Security Center の基本機能の一部です。

デバイスの検索の頻度

既定のデバイスの検索の頻度を高くすることは推奨されません。ドメインコントローラーに過大な負荷がかかる可能性があります。それよりむしろ、組織の必要に応じてポーリングの頻度をできるだけ低くしてください。最適なスケジュールを算出する際の推奨事項を次の表に示します：

デバイスの検索のスケジュール

ネットワーク上のデバイスの数	推奨されるデバイスの検索の頻度
10,000 台未満	既定またはより低い頻度
10,000 台以上	1 日に 1 回またはより低い頻度

管理サーバーデータのバックアップタスクと管理サーバーのメンテナンスタスク

管理サーバーは、以下のタスクの実行中は動作を停止します：

- 管理サーバーデータのバックアップ
- 管理サーバーのメンテナンス

これらのタスクの実行中は、データベースがデータを受信できません。

これらのタスクが別の管理サーバータスクと同時に実行されないように、タスクのスケジュールを変更する必要がある場合があります。

Kaspersky Endpoint Security をアップデートするグループタスク

管理サーバーがアップデート元として動作する場合、Kaspersky Endpoint Security 10 以降のグループアップデートタスクに推奨されるスケジュールオプションは、［**新しいアップデートがリポジトリにダウンロードされ次第**］と［**タスクの開始を自動的かつランダムに遅延させる**］です。

カスペルスキーのサーバーからリポジトリにダウンロードをアップデートするローカルタスクが各ディストリビューションポイントで作成される場合、Kaspersky Endpoint Security のグループアップデートタスクをスケジュールによって定期的に実行することを推奨します。この場合、ランダムに遅延させる時間の範囲を 1 時間に設定する必要があります。

インベントリタスク

実行ファイルに関する情報を取得しながら定義データベースの負荷を軽減できます。これを行うには、標準的なソフトウェアがインストールされている参照デバイスで、Kaspersky Endpoint Security のインベントリタスクを実行することを推奨します。

管理サーバーが 1 台のデバイスから受信できる実行ファイルは、最大で 150,000 個です。この上限に達すると、Kaspersky Security Center が新しいファイルを受信できなくなります。

通常、一般的なクライアントデバイスのファイルの数は 60,000 を超えません。ファイルサーバー上の実行ファイルの数はそれより大きい場合があり、150,000 の上限を超えることもあります。

テスト測定によると、Kaspersky Endpoint Security 11 がインストールされ、サードパーティ製品がインストールされていない、Windows 7 オペレーティングシステムで動作するデバイスでインベントリタスクを実行すると、次のような結果が得られました：

- ［**DLL モジュールのインベントリ**］と［**スクリプトファイルのインベントリ**］がオフの場合、約 3000 ファイル
- ［**DLL モジュールのインベントリ**］と［**スクリプトファイルのインベントリ**］がオンの場合、インストールされているオペレーティングシステムサービスパックの数に応じて 10,000 ～ 20,000 ファイル
- ［**スクリプトファイルのインベントリ**］のみがオンの場合、約 10,000 ファイル

管理サーバーと保護されるデバイスとの間のネットワーク負荷に関する詳細情報

このセクションでは、ネットワークトラフィックのテスト測定の結果とその測定の実行条件について説明します。組織内（または管理サーバーと管理対象デバイスがある組織との間）のネットワークインフラストラクチャとネットワークチャネルのスループットを計画する際、この情報を参照できます。ネットワークのスループットがわかると、様々なデータ転送操作にかかる時間を見積もることができます。

様々なシナリオでのトラフィック

次の表に、様々なシナリオでの管理サーバーと管理対象デバイスとの間のトラフィックに関する測定テストの結果を示します。

既定では、デバイスは 15 分に 1 回またはより長い間隔で管理サーバーと同期します。ただし、管理サーバーでポリシーやタスクの設定を変更した場合、そのポリシーまたはタスクが適用されるデバイスで事前に同期が実行され、新しい設定がデバイスに転送されます。

管理サーバーと管理対象デバイスとの間のトラフィック

シナリオ	管理サーバーから各管理対象デバイスへのトラフィック	各管理対象デバイスから管理サーバーへのトラフィック
Kaspersky Endpoint Security 11.7 for Windows とアップデートされた定義データベースのインストール	390 MB	3.3 MB
ネットワークエージェントのインストール	75 MB	397 KB
ネットワークエージェントと Kaspersky Endpoint Security 11.7 for Windows の同時インストール	459 MB	3.6 MB
パッケージ内のデータベースをアップデートしない定義データベースの初回のアップデート（Kaspersky Security Network への参加が無効な場合）	113 MB	1.8 MB
定義データベースの定期アップデート（Kaspersky Security Network への参加が有効な場合）	22 MB	373 MB
デバイス上の定義データベースをアップデートする前の初回の同期（ポリシーとタスクの転送）	382 KB	446 KB
デバイス上の定義データベースをアップデートした後の初回の同期	20 KB	157 KB
管理サーバーに変更がない場合の同期（定期）	18 KB	23 KB
グループポリシーで 1 つの設定を変更した時の同期（変更直後）	19 KB	20 KB

グループタスクで1つの設定を変更した時の同期（変更直後）	14 KB	11 KB
強制同期	110 KB	109 KB
「**ウイルスの検知**」イベント（1件のウイルス）	44 KB	50 KB
「**ウイルスの検知**」イベント（10件のウイルス）	58 KB	77 KB
アプリケーションレジストリリストを有効にした後のワンタイムトラフィック	最大 10 KB	最大 12 KB
アプリケーションレジストリリストが有効になっている場合の毎日のトラフィック	最大 840 KB	最大 1 MB

24時間あたりの平均トラフィック

管理サーバーと管理対象デバイス間の24時間あたりの平均トラフィックは次の通りです：

- 管理サーバーから管理対象デバイスへのトラフィックは840 KBです
- 管理対象デバイスから管理サーバーへのトラフィックは1 MB

トラフィックは次の条件下で測定されました：

- 管理対象デバイスにはネットワークエージェントおよびKaspersky Endpoint Security 11.6 for Windowsがインストールされている
- デバイスはディストリビューションポイントに割り当てられていない
- 脆弱性とパッチ管理が無効
- 管理サーバーとの同期間隔は15分

テクニカルサポートへの問い合わせ

このセクションでは、サポートを受ける方法および提供条件について説明します。

テクニカルサポートのご利用方法

Kaspersky Security Center のドキュメントや Kaspersky Security Center の情報源で問題のソリューションが見つからない場合、カスペルスキーのテクニカルサポートに問い合わせてください。テクニカルサポート担当者が、Kaspersky Security Center のインストール方法や使用方法についてのお問い合わせに回答いたします。

カスペルスキーによる Kaspersky Security Center のサポートは、本製品のライフサイクル期間中に提供されます（アプリケーションのサポートライフサイクルページを参照）。テクニカルサポートに連絡する前に、サポートサービス規約をご確認ください。

テクニカルサポートサービスの内容については、サポートセンターのご案内を参照してください。

- テクニカルサポートサイトにアクセスする
- カスペルスキーカンパニーアカウントからテクニカルサポートへリクエストを送信

カスペルスキーカンパニーアカウントによるテクニカルサポート

カスペルスキーカンパニーアカウントは、カスペルスキー製品を使用する法人向けのポータルです。このポータルは、オンラインリクエストを通じてユーザーとカスペルスキーのエキスパートの交流を促進するよう設計されています。また、オンラインリクエストの進捗をモニターでき、リクエストの履歴を保存することができます。

カスペルスキーカンパニーアカウントでは、シングルアカウントで組織の全従業員を登録できます。シングルアカウントによって、登録従業員からカスペルスキーまでのオンラインリクエストを一元管理でき、カスペルスキーカンパニーアカウントを介して従業員の権限を管理することもできます。

カスペルスキーカンパニーアカウントのポータルは、次の言語で利用できます：

- 英語
- スペイン語
- イタリア語
- ドイツ語
- ポーランド語
- ポルトガル語
- ロシア語
- フランス語

- 日本語

カスペルスキーカンパニーアカウントについて詳しくは、テクニカルサポートサイトをご覧ください。

管理サーバーのダンプファイルの取得

管理サーバーのダンプファイルには、ある時点での管理サーバープロセスに関するすべての情報が含まれています。管理サーバーのダンプファイルは、［%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\~dumps］フォルダーに保存されます。ダンプファイルは、Kaspersky Security Center が使用されている限り保存され、削除されると完全に削除されます。ダンプファイルが自動的にカスペルスキーに送信されることはありません。

管理サーバーがクラッシュした場合は、カスペルスキーテクニカルサポートにお問い合わせください。テクニカルサポートの担当者が、カスペルスキーでより詳細な分析を行うために管理サーバーのダンプファイルのご提供をお客様にお願いする場合があります。

ダンプファイルには個人データが含まれている可能性があります。情報をカスペルスキーに送信する前に、不正アクセスから保護することを推奨します。

製品の情報源

カスペルスキーの Web サイトの Kaspersky Security Center のページ

カスペルスキー Web サイトの Kaspersky Security Center のページで、本製品と機能、使用に関する一般的な情報を確認できます。

ナレッジベースの Kaspersky Security Center のページ

カスペルスキーのテクニカルサポートサイトに*ナレッジベース*のセクションがあります。

ナレッジベースの Kaspersky Security Center のページに、製品の購入、インストール、使用の方法について、役立つ情報、推奨事項、および FAQ への回答が掲載されています。

ナレッジベースの記事では、本製品だけではなく他のカスペルスキー製品に関連した質問にも回答しています。ナレッジベースの記事に、テクニカルサポートからのニュースが掲載されることもあります。

カスペルスキー製品の Web コミュニティの利用

特に緊急の対応が必要ではない場合は、カスペルスキーのフォーラムをご利用ください。ここでは、カスペルスキーのエキスパートやカスペルスキー製品のユーザーが、様々なトピックで意見交換しています。

フォーラムでは、これまでに公開されたトピックの閲覧、コメントの書き込み、新しいトピックの作成が可能です。

> オンラインの情報源を使用するには、インターネット接続が必要です。

問題の解決策が見つからない場合は、カスペルスキーのテクニカルサポートまでお問い合わせください。

Amazon EC2 インスタンス

Amazon Web Services を使用し、AMI イメージに基づいて作成された仮想マシン。

AMI（Amazon Machine Image）

仮想マシンを実行する場合に必要なソフトウェア設定が含まれるテンプレート。単一の AMI に基づいて複数のインスタンスを作成できます。

AWS IAM アクセスキー

ライセンス ID（「AKIAIOSFODNN7EXAMPLE」など）と秘密鍵（「wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY」など）で構成される組み合わせ。このペアは IAM ユーザーに属し、AWS サービスへのアクセス権限を取得するために使用されます。

AWS アプリケーションプログラムインターフェイス（AWS API）

Kaspersky Security Center によって使用され AWS プラットフォームのアプリケーションプログラミングインターフェイス。特に、AWS API ツールは、クラウドセグメントのポーリングとインスタンスでのネットワークエージェントのインストールで使用されます。

AWS 管理コンソール

AWS リソースの表示と管理を行える Web インターフェイス。AWS 管理コンソールは Web 上（https://aws.amazon.com/console/）で使用できます。

Cloud Discovery

Cloud Discovery は、組織のクラウドインフラストラクチャを保護する Cloud Access Security Broker（CASB）ソリューションのコンポーネントです。Cloud Discovery は、クラウドサービスへのユーザーアクセスを管理します。クラウドサービスには、Microsoft Teams、Salesforce、Microsoft Office 365 などがあります。クラウドサービスは、*データ交換*、*メッセンジャー*、*メール*などのカテゴリにグループ化されています。

HTTPS

データ転送用のセキュアプロトコル。ブラウザーと Web サーバーの通信に暗号を使用します。HTTPS は、企業データや財務データなどの制限付き情報へのアクセスに使用されます。

IAM ユーザー

AWS サービスのユーザー。IAM ユーザーには、クラウドセグメントポーリングを実行する権限があります。

IAM ロール

AWS ベースのサービスに対してリクエストを実行する権限の集合。IAM ロールは、特定のユーザーやグループとリンクしておらず、AWS IAM アクセスキーを使用せずにアクセス権を付与します。IAM ユーザー、EC2 インスタンス、AWS ベースのアプリケーションまたはサービスに IAM ロールを割り当てることができます。

ID およびアクセス管理（IAM）

他の AWS サービスとリソースへのユーザーアクセス管理を有効にする AWS サービス。

iOS MDM サーバー

クライアントデバイスにインストールされる Kaspersky Security Center のコンポーネントの 1 つ。iOS モバイルデバイスの管理サーバーへの接続と、APNs（Apple Push Notifications Service）による iOS モバイルデバイスの管理を可能にします。

iOS MDM デバイス

iOS MDM プロトコルを使用して iOS MDM サーバーに接続されたモバイルデバイス。iOS オペレーティングシステムで動作しているデバイスが、iOS MDM プロトコルを使用して接続および管理できます。

iOS MDM プロファイル

iOS モバイルデバイスと管理サーバーとの接続に関する一連の設定。ユーザーが iOS MDM プロファイルをモバイルデバイスにインストールすると、そのモバイルデバイスが管理サーバーに接続できます。

JavaScript

Web ページのパフォーマンスを拡張するプログラミング言語。JavaScript を使用して作成された Web ページでは、Web サーバーからの新しいデータでブラウザーの表示をアップデートすることなく、インターフェイス要素の表示を変更したり、新しいウィンドウを表示したりできます。JavaScript を使用して作成されたページを表示するには、ブラウザーの設定で JavaScript のサポートを有効にします。

Kaspersky Private Security Network（KPSN）

Kaspersky Private Security Network は、カスペルスキー製品がインストールされたデバイスのユーザーがデバイスから Kaspersky Security Network にデータを送信することなく、Kaspersky Security Network の評価データベースとその他の統計データにアクセスできるようにするソリューションです。Kaspersky Private Security Network は、次のいずれかの理由で Kaspersky Security Network にアクセスできない法人ユーザーの方を対象として開発されています：

- デバイスがインターネットに接続されていない。
- 国外や企業 LAN の外へのデータの送信が、法律または社内のセキュリティポリシーで禁止されている。

Kaspersky Security Center Web サーバー

管理サーバーとともにインストールされる Kaspersky Security Center のコンポーネントの1つ。Web サーバーは、スタンドアロンインストールパッケージ、iOS MDM プロファイル、および共有フォルダーのファイルをネットワーク上で伝送できるように設計されています。

Kaspersky Security Center オペレーター

Kaspersky Security Center システムで管理している保護システムのステータスと動作を監視するユーザー。

Kaspersky Security Center 管理者

Kaspersky Security Center システムを使用して、アプリケーションの動作をリモートで一元管理する担当者。

Kaspersky Security Center システム正常性検証ツール（SHV）

Kaspersky Security Center のコンポーネントの1つで、Kaspersky Security Center と Microsoft NAP を同時運用している場合のオペレーティングシステムの操作性をチェックします。

Kaspersky Security Center のアップグレード

Kaspersky Security Center の旧バージョンがインストールされているデバイスに、新バージョンのアプリケーションをインストールする手順。

Kaspersky Security Network（KSN）

ファイル、Web リソース、ソフトウェアの評価情報が定期的に更新されるカスペルスキーのデータベースへのアクセスを提供するクラウドサービスの基盤。KSN を使用することで、カスペルスキー製品がより迅速に新しい脅威に対応します。また、一部の保護コンポーネントのパフォーマンスが向上し、誤検知の可能性が減ります。

KES デバイス

Kaspersky Security Center 管理サーバーに接続され、Kaspersky Endpoint Security for Android アプリを用いて管理されるモバイルデバイス。

MITM 攻撃

真ん中の男。組織の IT インフラストラクチャに対する攻撃。ハッカーが 2 つのアクセスポイント間の通信リンクを乗っ取り、中継し、必要に応じてこれらのアクセスポイント間の接続を変更します。

SSL

インターネットおよびローカルネットワークで使用されるデータ暗号化プロトコル。Secure Sockets Layer（SSL）は Web アプリケーションで使用され、クライアントとサーバーの間のセキュアな接続を確立します。

UEFI 保護デバイス

BIOS レベルでカスペルスキーのソリューションまたは UEFI 用アプリケーションが統合されたデバイス。統合された保護により、システムが起動した瞬間からデバイスのセキュリティを確保し、同時に、ソフトウェアが統合されていないデバイスでの保護が、セキュリティ製品の起動後にのみ機能し始めるようにします。

Windows Server Update Services（WSUS）

Microsoft アプリケーションの更新プログラムを組織ネットワーク内のユーザーのコンピューターに配信するために使用するアプリケーション。

アップデート

カスペルスキーのアップデートサーバーから取得した新しいファイル（定義データベースまたはソフトウェアモジュール）を置換または追加する処理。

アプリケーションの一元管理

Kaspersky Security Center が備える管理サービスを使用した、アプリケーションのリモート管理。

アプリケーションの直接管理

ローカルインターフェイスを使用したアプリケーション管理。

アプリストア

Kaspersky Security Center のコンポーネント。アプリストアを使用すると、Android デバイスの所有者が自分でアプリケーションをインストールできます。アプリストアでは、アプリケーションの APK ファイルや Google Play のリンクを公開できます。

アンチウイルスサービスプロバイダー

クライアント組織にカスペルスキー製品に基づくアンチウイルスサービスを提供する組織。

イベントの重要度

カスペルスキー製品の動作時に発生したイベントのプロパティ。次のレベルに分かれています：

- 緊急
- 機能エラー
- 警告
- 情報

イベント発生の状況によって、同じ種別のイベントで重要度が異なる場合があります。

イベントリポジトリ

管理サーバーデータベースのうち、Kaspersky Security Center で発生するイベントに関する情報の保管専用の領域です。

インストールパッケージ

カスペルスキー製品のリモートインストール用に作成されるファイルセット。リモート管理システム Kaspersky Security Center を使用して作成します。インストールパッケージには、アプリケーションをインストールし、インストール後にすぐに実行させるのに必要な設定の範囲が含まれます。設定は、アプリケーションの既定値になります。インストールパッケージは、配布キットに含まれる拡張子が kpd および kud のファイルを使用して作成されます。

ウイルスアウトブレイク

デバイスをウイルスに感染させるための、一連の意図的な試み。

ウイルスアクティビティのしきい値

指定した種別のイベントに関して設定する、制限時間内で許容するイベント発生数の上限。この値を超過すると、ウイルスアクティビティが増加してウイルスアウトブレイクの脅威があると判断されます。ウイルスアウトブレイクの脅威に対してタイムリーな対応が可能になるため、ウイルスアウトブレイクの発生中に重要な役割を果たします。

カスペルスキーのアップデートサーバー

カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。

仮想管理サーバー

クライアント組織のネットワークの保護システムを管理する Kaspersky Security Center のコンポーネント。

仮想管理サーバーは特殊なセカンダリ管理サーバーであり、物理管理サーバーと比較すると、次の制限があります：

- 仮想管理サーバーは、プライマリ管理サーバー上にのみ作成できます。
- 仮想管理サーバーは、プライマリ管理サーバーのデータベースを使用します。仮想管理サーバーではデータのバックアップと復元タスク、およびアップデートのスキャンとダウンロードタスクはサポートされていません。
- 仮想サーバーでは、セカンダリ管理サーバー（仮想サーバーを含む）の作成がサポートされていません。

管理グループ

機能およびインストールされているカスペルスキー製品に応じてデバイスをまとめたグループ。複数のデバイスを 1 つのグループとして管理できます。1 つのグループに下位のグループとして他のグループを含めることができます。グループにインストールされている各アプリケーションに対してグループポリシーやグループタスクを作成することができます。

管理コンソール

Windows ベースの Kaspersky Security Center（別名「MMC ベースの管理コンソール」）のコンポーネント。このコンポーネントは、管理サーバーとネットワークエージェントの管理サービスに対してユーザーインターフェイスを提供します。

管理コンピューター

管理コンソールがインストールされたデバイス、または Kaspersky Security Center Web コンソールを管理者が開くために使用するデバイスです。このコンポーネントにより、Kaspersky Security Center の管理に使用できるインターフェイスが提供されます。

管理コンピューターは、Kaspersky Security Center のサーバー部分の設定と管理に使用されます。管理コンピューターを使用して、カスペルスキー製品に基づいて一元化されたアンチウイルスによる企業内 LAN の保護を構築および管理します。

管理サーバー

企業ネットワークにインストールされているすべてのカスペルスキー製品に関する情報を一元的に保管する Kaspersky Security Center のコンポーネント。製品の管理にも使用できます。

管理サーバークライアント（クライアントデバイス）

ネットワークエージェントがインストールされ管理対象のカスペルスキー製品が実行されているデバイス、サーバー、またはワークステーション。

管理サーバー証明書

管理サーバーが次の目的で使用する証明書：

- MMC ベースの管理コンソールまたは Kaspersky Security Center Web コンソールに接続する際の管理サーバーの認証
- 管理対象デバイスでの管理サーバーとネットワークエージェントとの安全な連携
- プライマリ管理サーバーをセカンダリ管理サーバーに接続する際の管理サーバーの認証

証明書は、管理サーバーをインストールすると自動的に作成され、管理サーバーに保存されます。

管理サーバーデータのバックアップ

管理サーバーのデータをバックアップし、後でバックアップユーティリティを使用して復元できるようにコピーすること。ユーティリティで保存できるデータは次の通りです：

- 管理サーバーのデータベース（管理サーバーに保存されているポリシー、タスク、アプリケーション設定、イベント）
- 管理グループとクライアントデバイスの構造についての設定情報
- アプリケーションリモートインストール用のインストールファイルのリポジトリ（フォルダーの内容としては、Packages と Uninstall Updates が含まれます）
- 管理サーバー証明書

管理サーバーデータの復元

バックアップユーティリティを使用して、バックアップに保存されている情報から管理サーバーデータを復元すること。ユーティリティで復元できるデータは次の通りです：

- 管理サーバーのデータベース（管理サーバーに保存されているポリシー、タスク、アプリケーション設定、イベント）

- 管理グループとクライアントコンピューターの構造についての設定情報
- アプリケーションリモートインストール用のインストールファイルのリポジトリ（フォルダーの内容としては、Packages と Uninstall Updates が含まれます）
- 管理サーバー証明書

管理者権限

Exchange 組織内の Exchange オブジェクトの管理に必要な、ユーザー権限および特権のレベル。

管理対象デバイス

管理グループに含まれる企業ネットワークデバイス。

管理プラグイン

管理コンソールを使用してアプリケーションを管理するためのインターフェイスを備えた特別なコンポーネント。各アプリケーションには独自のプラグインがあります。このプラグインは、Kaspersky Security Center を使用して管理可能なすべてのカスペルスキー製品に含まれています。

強制インストール

カスペルスキー製品のリモートインストール方法。指定したクライアントデバイスに、ソフトウェアをインストールできます。強制インストールでは、タスクで使用されるアカウントに、クライアントデバイス上でアプリケーションをリモート実行する権限が必要です。この方法は、Microsoft Windows オペレーティングシステムが実行され、この機能をサポートするデバイスに製品をインストールする場合に推奨されます。

共有証明書

ユーザーのモバイルデバイスを識別することを目的とした証明書。

クライアント管理者

クライアント組織のスタッフ。アンチウイルスのステータスを監視します。

クラウド環境

クラウドプラットフォームをベースに、ネットワークに統合される仮想マシンとその他の仮想リソース。

グループタスク

管理グループに定義され、そのグループ内のすべてのクライアントデバイスで実行されるタスク。

現在のライセンス

アプリケーションによって現在使用されているライセンス。

互換性がないアプリケーション

サードパーティ製のアンチウイルス製品、または Kaspersky Security Center を使用した管理に対応していないカスペルスキー製品。

サービスプロバイダーの管理者

アンチウイルスサービスプロバイダーのスタッフ。サービスプロバイダーの管理者は、カスペルスキー製品に基づき、アンチウイルスシステムをインストールおよび管理し、テクニカルサポートを顧客に提供します。

手動インストール

配布パッケージからの、企業ネットワーク上のデバイスへのセキュリティ製品のインストール。手動インストールには、管理者または別の IT スペシャリストの参加が必要です。通常、手動インストールは、リモートインストールでエラーが発生した場合に行います。

脆弱性

マルウェアの開発者がオペレーティングシステムやプログラムに侵入してその完全性を損なわせるために利用する可能性のあるオペレーティングシステムまたはプログラムの欠陥。オペレーティングシステムに多くの脆弱性があると、機能の信頼性が損なわれます。侵入したウイルスによってオペレーティングシステム自体またはインストールされているアプリケーションで障害が引き起こされる可能性があるためです。

接続ゲートウェイ

*接続ゲートウェイ*は、特別なモードで動作するネットワークエージェントです。接続ゲートウェイは、他のネットワークエージェントからの接続を受け入れ、サーバーとの独自の接続を介してそれらを管理サーバーにトンネリングします。通常のネットワークエージェントとは異なり、接続ゲートウェイは、管理サーバーへの接続を確立するのではなく、管理サーバーからの接続を待機します。

設定プロファイル

iOS MDM モバイルデバイスの設定と制限事項に関するポリシー。

タスク

カスペルスキー製品によって実行される機能はタスクとして実装されます。ファイルのリアルタイム保護、デバイスの完全スキャン、定義データベースのアップデートなどのタスクがあります。

タスク設定

各タスク種別に固有のアプリケーション設定です。

追加（または予備）ライセンス

製品を使用する権限を認定する、現在使用されていないライセンス。

定義データベース

定義データベースの公開時点で、カスペルスキーが把握しているコンピューターセキュリティへの脅威についての情報を含むデータベース。定義データベース内のエントリによって、スキャンしているオブジェクトで悪意のあるコードを検知できます。定義データベースはカスペルスキーのエキスパートにより作成され、1時間ごとにアップデートされます。

ディストリビューションポイント

ネットワークエージェントがインストールされており、アップデートの配信やアプリケーションのリモートインストール、管理グループやブロードキャストドメインでのコンピューター情報の取得に使用されるコンピューター。ディストリビューションポイントは、アップデート配信時の管理サーバーの負荷軽減およびネットワークトラフィックの最適化の目的で設計されています。ディストリビューションポイントは、管理サーバーによって自動的に、または管理者によって手動で割り当てられます。ディストリビューションポイントは、以前のバージョンの製品ではアップデートエージェントという名称でした。

適用可能なアップデート

カスペルスキーのソフトウェアモジュールに関する一連のアップデート（一定期間に蓄積された重大なアップデート、アプリケーションのアーキテクチャへの変更を含む）

デバイスの所有者

デバイスで特定の操作が必要になった際に管理者が連絡できるユーザー。

特定のデバイスに対するタスク

任意の管理グループに属する一連のクライアントデバイスに割り当てられ、それらのデバイスで実行されるタスク。

内部ユーザー

内部ユーザーのアカウントは、仮想管理サーバーを操作するために使用します。Kaspersky Security Center によって、実際のユーザーの権限がアプリケーションの内部ユーザーに付与されます。

内部ユーザーのアカウントは、Kaspersky Security Center 内でのみ作成および使用されます。内部ユーザーに関するデータは、オペレーティングシステムには送信されません。Kaspersky Security Center が内部ユーザーを認証します。

認証エージェント

起動可能なハードディスクの暗号化後に、暗号化されたハードディスクへのアクセス権を取得してオペレーティングシステムを読み込むための認証手順を完了することができるインターフェイス。

ネットワークエージェント

管理サーバーと特定のネットワークノード（ワークステーションまたはサーバー）にインストールされているカスペルスキー製品との間のやり取りを受け持つ Kaspersky Security Center のコンポーネント。このコンポーネントは、カスペルスキーの Microsoft® Windows® 用の製品に共通した機能です。Unix 系の OS および macOS 用には、それぞれ異なるバージョンのネットワークエージェントがあります。

ネットワークのアンチウイルスによる保護

組織のネットワークにウイルスやスパムが侵入する危険性を軽減し、ネットワーク攻撃やフィッシングなどの脅威を防ぐ一連の技術的、組織的対策。ネットワークセキュリティは、セキュリティ製品およびサービスを使用して企業のセキュリティポリシーに従い、正しく適用することで向上します。

ネットワーク保護ステータス

企業ネットワーク内のデバイスのセキュリティレベルを定義する現在の保護ステータス。ネットワーク保護ステータスには、インストール済みセキュリティ製品、ライセンスの使用、検知された脅威の数と種類のような要因を含みます。

ハードニングガイド

Kaspersky Security Center とそのコンポーネントの構成に関する推奨事項と機能で、その侵害リスクを低減することを目的としています。

バックアップフォルダー

管理サーバーデータのコピーを保管するための特別なフォルダー。バックアップユーティリティによって作成されます。

パッチの重要度

パッチの属性の1つ。Microsoft のパッチおよびサードパーティのパッチには、5 つの重要度があります：

- 緊急
- 高
- 中
- 低
- 不明

サードパーティのパッチまたは Microsoft のパッチの重要度は、パッチが修正する脆弱性のうち、最も高い重要度によって決定されます。

非武装地帯（DMZ）

非武装地帯は、サーバーを含むローカルネットワークのセグメントで、グローバル Web からの要求に応えます。組織のローカルネットワークのセキュリティを確保するために、非武装地帯から LAN へのアクセスがファイアウォールで保護されます。

復元

隔離またはバックアップ内のオブジェクトを、隔離、感染駆除、削除される前の元のフォルダーまたはユーザーが指定したフォルダーに移動すること。

ブロードキャストドメイン

OSI 基本参照モデル（Open Systems Interconnection Basic Refernce Model）のレベルにおける、ブロードキャストチャネルを使用してすべてのノードがデータ交換を行えるネットワークの論理領域。

プログラム設定

あらゆる種類のタスクに共通していて、アプリケーションの動作全体を管理するアプリケーション設定（アプリケーションパフォーマンス設定、レポート設定、バックアップ設定など）。

プロビジョニングプロファイル

iOS モバイルデバイスでのアプリケーションの動作に関する設定の集まり。プロビジョニングプロファイルには、ライセンスに関する情報が書き込まれています。このプロファイルは、特定のアプリケーションにリンクされています。

ホーム管理サーバー

ネットワークエージェントのインストール中に指定した管理サーバー。ホーム管理サーバーは、ネットワークエージェントの接続プロファイルを設定するために使用できます。

保護ステータス

コンピューターのセキュリティレベルを定義する現在の保護ステータス。

ポリシー

ポリシーは、アプリケーションの設定を決定するとともに、管理グループ内のコンピューターにインストールされたアプリケーションを設定する権限を管理します。各アプリケーションについて個別にポリシーを作成する必要があります。各管理グループのコンピューターにインストールされたアプリケーションについて複数のポリシーを作成できますが、各管理グループ内で1つのアプリケーションについて一度に適用されるポリシーは1つだけです。

モバイルデバイスサーバー

Kaspersky Security Center のコンポーネントの1つ。モバイルデバイスへのアクセスを可能にし、管理コンソールからモバイルデバイスを管理できるようにします。

ライセンス情報ファイル

拡張子が「KEY」のファイル。このファイルを使用することで、カスペルスキー製品を試用版または製品版ライセンスで使用できます。

ライセンス認証済みアプリケーショングループ

管理者が設定した基準（製造元別など）に基づいて作成されるアプリケーションのグループ。クライアントデバイスへのインストールのグループごとの統計情報が保持されます。

ライセンスの有効期間

ユーザーがアプリケーションの機能および追加サービスへのアクセス権を有する期間。使用できるサービスは、ライセンスの種別によって異なります。

リモートインストール

Kaspersky Security Center を使用した、カスペルスキー製品のインストール。

ローカルインストール

組織のネットワーク上のデバイスにセキュリティ製品をインストールするには、セキュリティ製品の配布パッケージからインストールを手動で開始する方法、またはコンピューターに事前にダウンロードしておいた公開済みインストールパッケージを手動で起動する方法があります。

ローカルタスク

1台のクライアントコンピューターを対象として定義、実行されるタスク。

サードパーティ製のコードに関する情報

サードパーティのコードに関する情報は、ファイル legal_notices.txt に記載され、カスペルスキー製品のインストールフォルダーに保存されています。

商標に関する通知

登録商標とサービスマークに関する権利は各所有者に帰属します。

Adobe、Acrobat、Flash、Shockwave、PostScript は、Adobe の米国および他の国における登録商標または商標です。

AMD、AMD64 は、Advanced Micro Devices, Inc. の商標または登録商標です。

Amazon、Amazon Web Services、AWS、Amazon EC2、AWS Marketplace は、Amazon.com, Inc. またはその関連会社の商標です。

Apache は、Apache Software Foundation の登録商標または商標です。

AirPlay、AirDrop、AirPrint、App Store、Apple、Apple Configurator、AppleScript、FaceTime、FileVault、iBook、iBooks、iCloud、iPad、iPhone、iTunes、Leopard、macOS、Mac、Mac OS、OS X、Safari、Snow Leopard、Tiger、QuickTime、Touch ID は、Apple Inc. の商標です。

Arm は、Arm Limited（またはその子会社）の米国および / またはその他の国における登録商標です。

Bluetooth の表記、マークおよびロゴは、Bluetooth SIG, Inc. に所有権があります。

Ubuntu LTS は Canonical Ltd の登録商標です。

Cisco Systems、Cisco、Cisco Jabber、IOS は、米国およびその他の国における Cisco Systems, Inc. およびその子会社の登録商標です。

Citrix、XenServer は、米国およびその他の国における Cloud Software Group, Inc. およびその子会社の登録商標または商標です。

Corel は、カナダ、米国およびその他の国における Corel Corporation およびその子会社の商標または登録商標です。

Cloudflare、Cloudflare のロゴ、および Cloudflare Workers は、米国およびその他の法域における Cloudflare, Inc. の商標や登録商標です。

Dropbox は、Dropbox, Inc. の商標です。

Radmin は、Famatech の登録商標です。

Firebird は、Firebird Foundation の登録商標です。

Foxit は、Foxit Corporation の登録商標です。

FreeBSD は、FreeBSD Foundation の登録商標です。

Google、Android、Chrome、Chromium、Dalvik、Firebase、Google Chrome、Google Earth、Google Play、Google Maps、Hangouts、Google Public DNS、YouTube は、Google LLC の商標です。

EulerOS、FusionCompute、FusionSphere は、Huawei Technologies Co., Ltd. の商標です。

Intel、Core、Xeon は米国およびその他の国における Intel Corporation の商標です。

IBM および QRadar は、世界各国で International Business Machines Corporation が所有する登録商標です。

Node.js は Joyent Inc. の商標です。

Linux は、米国およびその他の国における Linus Torvalds 氏の登録商標です。

Logitech は Logitech の米国および他の国における登録商標または商標です。

Microsoft、Active Directory、ActiveSync、BitLocker、Excel、Forefront、Internet Explorer、InfoPath、Hyper-V、Microsoft Edge、MultiPoint、MS-DOS、Office 365、PowerShell、PowerPoint、SharePoint、SQL Server、OneNote、Outlook、Skype、Tahoma、Visio、Win32、Windows、Windows PowerShell、Windows Media、Windows Mobile、Windows Server、Windows Phone、Windows Vista、and Windows Azure は、Microsoft グループ企業の商標です。

CVE は、The MITRE Corporation の登録商標です。

Mozilla、Firefox、Thunderbird は、米国およびその他の国における Mozilla Foundation の商標です。

Novell は、米国およびその他の国における Novell Enterprises Inc. の登録商標です。

NetWare は、米国およびその他の国における Novell, Inc. の登録商標です。

OpenSSL は、OpenSSL Software Foundation が所有する商標です。

Oracle、Java、JavaScript、TouchDown は、Oracle とその関連会社の両方またはいずれかの登録商標です。

Parallels、Parallels ロゴ、および Coherence は、Parallels International GmbH の商標または登録商標です。

Chef は、Progress Software Corporation およびその子会社または関連会社の、米国およびその他の国における商標または登録商標です。

Puppet は、Puppet, Inc. の商標または登録商標です。

Python は Python Software Foundation の登録商標または商標です。

Red Hat、CentOS、Fedora、Red Hat Enterprise Linux は、Red Hat, Inc. またはその子会社の米国および他の国における商標または登録商標です。

Ansible は、米国およびその他の国における Red Hat, Inc. の登録商標です。

CentOS は、Red Hat, Inc. またはその子会社の米国および他の国における商標または登録商標です。

BlackBerry は、Research In Motion Limited の米国における登録商標であり、その他の国における登録商標または登録出願中の商標です。

SAMSUNG は、米国およびその他の国における SAMSUNG の登録商標です。

Debian は、Software in the Public Interest, Inc. の登録商標です。

Splunk、SPL は、Splunk, Inc. の米国およびその他の国における登録商標です。

SUSE は、米国およびその他の国における SUSE LLC の登録商標です。

Symbian の商標は Symbian Foundation Ltd. が所有します。

OpenAPI は、Linux Foundation の登録商標です。

VMware、VMware vSphere、VMware Workstation は、VMware, Inc. の米国およびその他の国における商標または登録商標です。

UNIX は米国およびその他の国における登録商標で、X/Open Company Limited のライセンス契約の下で排他的に使用されています。

Zabbix は Zabbix SIA の登録商標です。

既知の問題

Kaspersky Security Center Web コンソールには、本製品の動作には大きな影響を与えない複数の制限があります：

- 暗号化の強度を確保するには、管理サーバー証明書は SHA-2 を使用して署名され、鍵の長さが 2048 以上である必要があります。証明書を再発行する必要がある場合は、Kaspersky Security Center ナレッジベースを参照してください。

- Kaspersky Security Center 15.1 Web コンソールで「**N 日ごと**」および「**曜日別**」のスケジュール設定を使用してタスクを作成し、そのタスクを以前のバージョンの Kaspersky Security Center Web コンソールまたは Kaspersky Security Center 管理コンソールで開くと（たとえば、タスクが Linux ベースと Windows ベースの両方のセカンダリ管理サーバーにも適用されている場合）、スケジュール設定が正しく表示されないか、エラーが発生する可能性があります。

- ARM アーキテクチャをベースとし、Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.7）を実行しているデバイスからネットワークエージェントを削除するタスクを実行すると、ネットワークエージェントは正常に削除されますが、タスクリスト内の現在の進行状況のタスクステータスはフリーズします。

- Kaspersky Endpoint Security for Windows ポリシーには、Kaspersky Endpoint Security for Windows に表示される保護レベルと一致しない保護レベルが表示されます。

- Exchange ActiveSync はサポートされなくなりましたが、Kaspersky Device Management for iOS ポリシーのプロパティウィンドウには、［**EAS デバイスの設定**］セクションが引き続き含まれています。

- デバイス名にキリル文字が含まれるデバイスに Kaspersky Security Center がインストールされており、管理サーバー上で KSN プロキシが有効になっている場合、HTTPS 経由の KSN への接続は失敗します。

- ［**認証を要求してこのユーザーアカウントの変更権限をチェックする**］がオンになっているユーザーアカウントのプロパティを変更しようとし、［**アカウント保護**］ウィンドウで［**キャンセル**］をクリックすると、予期しないエラーが発生します。

- ローカル［**IOC スキャン**］タスクが正常に完了すると、タスクリストにタスクステータスが［**スケジュール済み**］として表示されます。

- デバイスの時刻またはタイムゾーンを変更する場合は、Kaspersky Security Center Web コンソールサービスを再起動する必要があります。

- デバイスでプロキシが使用され、プロキシ環境変数が設定されている場合、Kaspersky Security Center Web コンソールのインストーラーがフリーズする可能性があります。

- *ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクまたは*アップデート検証*タスクをインポートすると、［**タスクが割り当てられるデバイスを選択する**］オプションがオンになります。これらのタスクは、デバイスの抽出または特定のデバイスに割り当てることはできません。*ディストリビューションポイントのリポジトリにアップデートをダウンロードする*か、特定のデバイスに*アップデート検証*タスクを割り当てると、タスクは正しくインポートされません。

- ネットワークエージェント 15 がインストールされた Linux ディストリビューションポイントを使用して Active Directory ポーリングを実行する場合は、アドレスとユーザー資格情報を指定した Active Directory ドメインのみをポーリングできます。現在の Active Directory ドメインと Active Directory ドメインフォレストのポーリングは使用できません。

- Windows ネットワークポーリングを実行した後、クライアントデバイスが見つからない場合があります。

- ［**セカンダリ管理サーバー追加**］ウィザードで、将来のセカンダリサーバーでの認証用に二段階認証が有効になっているアカウントを指定すると、ウィザードはエラーで終了します。この問題を解決するには、二段階認証を無効にしたアカウントを指定するか、将来のセカンダリサーバーから階層を作成します。

- Kaspersky Security Center Web コンソールへのログイン中に、ドメイン認証を使用して仮想管理サーバーを接続先に指定してからログアウトし、プライマリ管理サーバーへのログインを試行すると、Kaspersky Security Center Web コンソールは仮想管理サーバーへの接続を試行します。プライマリ管理サーバーへ接続するには、ブラウザーを再び開きます。

- Windows ネットワークの完全または簡易ポーリングで空の結果が返されます。

- Kaspersky Security Center Web コンソールと Identity an Access Manager をインストールしてから Kaspersky Security Center Web コンソールの管理サーバーを変更した場合、Identity and Access Manager は新しい管理サーバーの情報を取得しません。

- 1つ以上のネットワークアダプターを持つ管理対象デバイスが管理サーバーにネットワークアダプターの MAC アドレスに関する情報を送信する際、管理サーバーへの接続に使用されていないものの情報を送信することがあります。

- 指定したアカウントに対して実行スクリプトのリモートタスクを開始し、タスク設定で割り当てられているアカウントを変更した場合、変更は保存されません。タスクが割り当てられているアカウントを変更するには、タスク設定でタスクを停止し、再起動します。