kaspersky

Kaspersky Security Center Cloud コンソール

目次

JavaScript
Kaspersky Private Security Network（KPSN）
Kaspersky Security Center Cloud コンソールのアカウント
Kaspersky Security Center Cloud コンソールのオペレーター
Kaspersky Security Center Cloud コンソールの管理者
Kaspersky Security Network（KSN）
SSL
UEFI 保護デバイス
Web 管理プラグイン
アップデート
アプリケーションタグ
アプリケーションの一元管理
アプリケーションの直接管理
イベントの重要度
イベントリポジトリ
インストールパッケージ
ウイルスアウトブレイク
ウイルスアクティビティのしきい値
隔離
カスペルスキーのアップデートサーバー
仮想管理サーバー
管理グループ
管理サーバー
管理対象デバイス
強制インストール
グループタスク
現在のライセンス
互換性がないアプリケーション
脆弱性
接続ゲートウェイ
タスク
タスク設定
追加の定額制サービスのライセンス
定義データベース
ディストリビューションポイント
適用可能なアップデート
デバイスの所有者
デバイスのタグ
特定のデバイスに対するタスク
認証エージェント
ネットワークエージェント
ネットワークのアンチウイルスによる保護
ネットワーク保護ステータス
パッチの重要度
非武装地帯（DMZ）
復元
ブロードキャストドメイン
プログラム設定

Kaspersky Security Center Cloud コンソールのヘルプ

新機能

最新の製品リリースの新機能を確認できます。

ネットワーク保護の設定

組織の要件に従ってカスペルスキー製品のポリシーとタスクを設定し、組織のセキュリティを管理する方法を確認できます。

システム要件

サポート対象のオペレーティングシステムとアプリケーションのバージョンを確認できます。

カスペルスキー製品：定義データベースとソフトウェアモジュールの定期的なアップデート

保護システムの信頼性を維持する方法を確認できます。

Kaspersky Security Center Cloud コンソールのライセンス

Kaspersky Security Center Cloud コンソールの試用モードと製品モードの動作の詳細について確認できます。

監視とレポート

インフラストラクチャ、ネットワーク接続されたデバイスの保護ステータス、組織の現在の保護状態を管理するための統計情報を確認できます。レポートも使用できます。

初期設定

ワークスペースの使用を開始し、必要に応じて Kaspersky Security Center Cloud コンソールを設定する方法を確認できます。

脆弱性とパッチ管理

サードパーティ製ソフトウェアの脆弱性を検知して修正する方法を確認できます。

Kaspersky Security Center Cloud コンソールへの移行

既存の管理グループと関連オブジェクトを、オンプレミスの Kaspersky Security Center から Kaspersky Security Center Cloud コンソールに移行する方法を確認できます。

SIEM システムへのイベントのエクスポート

Syslog プロトコルを使用して、SIEM システムへのイベントのエクスポートを設定する方法を確認できます。

ネットワーク接続されたデバイスの検出

組織ネットワーク上の既存デバイスと新規デバイスの検出方法について説明しています。

クラウド環境での利用

クラウド環境の Amazon Web Services™、Microsoft Azure™、Google™ Cloud Platform での仮想マシンの保護について説明しています。

ディストリビューションポイントと接続ゲートウェイの調整

ディストリビューションポイントの設定方法を説明しています。

マネージドサービスプロバイダー（MSP）向けのクイックスタートガイド

MSP の管理者向けの、Kaspersky Security Center Cloud コンソールの操作方法を確認できます。

カスペルスキー製品：一元管理による導入

カスペルスキー製品の導入

新機能

2024 年 4 月のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- 新機能として、Cloud Discovery を実装しました。この機能を使用すると、Windows を実行している管理対象デバイスでのクラウドサービスの使用を監視し、不要と思われるクラウドサービスへのアクセスをブロックできます。Cloud Discovery は、ブラウザーやデスクトップアプリケーションからこれらのサービスにアクセスしようとするユーザーの試行を追跡します。

2024 年 2 月のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- 管理対象デバイスのリストから、1つまたは複数のデバイスを選択し、選択したデバイスで実行する既存のタスクを割り当てることができるようになりました。現在のデバイスのタスク範囲は、選択したデバイスに置き換えられます。

- 複数のデバイスにデバイスのタグを割り当てたり、複数のデバイスからデバイスのタグを一度に削除したりできるようになりました。管理対象デバイスのリストからデバイスを選択し、選択したデバイスに割り当てるタグ、または選択したデバイスから削除するタグを指定します。

- 管理対象デバイスのリストの外観とユーザーエクスペリエンスが最適化されました。新しい列［**タグ**］が追加され、デバイスタグでデバイスをフィルタリングする機能が追加されました。

2024 年 1 月のアップデート

Kaspersky Security Center Cloud コンソールは、Kaspersky Endpoint Security 12.4 for Windows をサポートするようになりました。

2023 年 12 月のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- SIEM システムへの接続を確認できるようになりました。

- Kaspersky Security Center Cloud コンソールは、Linux ベースのディストリビューションポイントを介した Microsoft Active Directory ドメインコントローラーと Samba ドメインコントローラーのポーリングをサポートするようになりました。

- Linux ベースの管理対象デバイスのリモート診断。

- Kaspersky Security Center Cloud コンソールは次のカスペルスキー製品をサポートするようになりました：

  - Kaspersky Endpoint Security for Windows バージョン 12.3 パッチ A

  - Kaspersky Endpoint Security 12.0 for Linux

- Kaspersky Endpoint Security 12.0 for Mac
- Kaspersky Endpoint Agent 3.16
- Kaspersky Embedded Systems Security 3.3 for Windows

- 以下のインターフェイスセクションは、製品機能の範囲外としてメインメニューから非表示になりました：
  - 暗号化イベント（［**操作**］→［**データ暗号化と保護機能**］→［**暗号化イベント**］）
  - IP アドレス範囲（［**検出と製品の導入**］→［**検出**］→［**IP アドレス範囲**］）
- Kaspersky Security Center Cloud コンソールのデータ処理契約書の本文を更新しました。
- 多くのブラウザーの旧バージョンはサポートされなくなりました（バージョン 102 より前の Firefox ESR）。

2023 年 9 月のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- Kaspersky Security Center Cloud コンソールは、 Kaspersky Embedded Systems Security 3.3 for Linux をサポートするようになりました。
- Kaspersky Security Center Cloud コンソールは、Kaspersky Endpoint Security 12.2 for Windows をサポートするようになりました。
- ［**アセット（デバイス）**］セクションでユーザーリストを操作する時のユーザーインターフェイスの最適化。

2023 年 6 月のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- 新しいハードニングガイドがリリースされました。このガイドを注意深く読み、セキュリティに関する推奨事項に従って Kaspersky Security Center Cloud コンソールとネットワークインフラストラクチャを構成することを強く推奨します。
- Kaspersky Security Center Cloud コンソールは、Kaspersky Endpoint Security 11.3 for Mac をサポートするようになりました。
- Kaspersky Security Center Cloud コンソールは、 Kaspersky Endpoint Security 11.4 for Linux をサポートするようになりました。
- Kaspersky Security Center Cloud コンソールを使用してファイルにイベントの抽出をエクスポートしてから、Kaspersky Security Center Windows または Kaspersky Security Center Linux にイベントの抽出をインポートできます。
- ディストリビューションポイントを、ネットワークエージェントによって管理されるデバイスのプッシュサーバーとして使用できるようになりました。この機能により、管理対象デバイスと管理サーバー間の継続的な接続が確立されます。

- Kaspersky Security Center Cloud コンソールを他のカスペルスキー製品と統合するための設定セクションが再編成されました。
- ［**リモート診断**］セクションのユーザーインターフェイスを再編成しました。
- デバイスの抽出に含まれるすべてのデバイスに関する情報を一度に CSV ファイルに保存できるようになりました。
- 表内のすべての項目を選択する機能など、ユーザーインターフェイスと可用性が多数改善されました。

2023 年 3 月更新

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- Kaspersky Security Center Cloud コンソールは、管理対象デバイスとしてクラスターとサーバーアレイをサポートするようになりました。カスペルスキー製品がクラスターノードにインストールされている場合、ネットワークエージェントはこの情報を管理サーバーに送信します。Web コンソールでは、クラスターとサーバーアレイは他の管理対象デバイスとは別に表示されます。各クラスターまたはサーバーアレイは、個別の分離不可能なオブジェクトとして管理してください。
- Kaspersky Security Center Cloud コンソールは、Kaspersky Endpoint Security 12.0 for Windows をサポートするようになりました。
- レポートに含めることができるエントリの最大数は、Web コンソールのレポートでは最大 2500 まで、ファイルにエクスポートするレポートでは最大 10,000 まで増加しました。
- 保護ステータスレポートに［*OK*］ステータスの管理対象デバイスを含めるかどうかを選択できるようになりました。
- 次のいずれかのライセンスを使用して、Kaspersky Security Center Cloud コンソールをアクティベートするか、リストされているライセンスを既存のワークスペースに追加できるようになりました：
  - Kaspersky Symphony Security
  - Kaspersky Symphony EDR
  - Kaspersky Symphony MDR
  - Kaspersky Symphony XDR
- Windows XP 用のネットワークエージェントの特別版がリリースされました。
- アップデートされた Linux 用ネットワークエージェントはKSN プロキシサービスをサポートします。Windows ベースのディストリビューションポイントに加えて、Linux ベースのディストリビューションポイントを使用して、管理対象デバイスからの Kaspersky Security Network（KSN）要求を転送できるようになりました。この機能により、ネットワーク上でトラフィックを分配しなおし、最適化できます。
- アップデートされた Linux 用ネットワークエージェントはアプリケーションレジストリ機能をサポートします。ネットワークエージェントが、Linux ベースの管理対象デバイスにインストールされているアプリケーションのリストを作成し、このリストを管理サーバーに送信できます。
- Kaspersky Security Center Cloud コンソールを使用してファイルにポリシーとタスクをエクスポートしてから、ポリシーとタスクを Kaspersky Security Center Windows または Kaspersky Security Center Linux にインポートできます。

2022 年 11 月のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- Kaspersky Security Center Cloud コンソールは、 Kaspersky Endpoint Security 11.3 for Linux をサポートするようになりました。
- Kaspersky Security Center Cloud コンソールは、Kaspersky Managed Detection and Response 2.1.18 のサポートを開始しました。
- Kaspersky Security Center Cloud コンソールは、macOS 13 をサポートするために、 Kaspersky Endpoint Security for Mac 11.2 および 11.2.1 のアップデートされたバージョンをサポートするようになりました。
- ［**機能紹介とチュートリアル**］セクションのビデオが更新されました。

2022 年 10 月のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- Kaspersky Security Center Cloud コンソールのデータ処理契約書の本文を更新しました。
- Kaspersky Security Center Cloud コンソールのインフラストラクチャで、現在ライセンスがなく、新たにライセンスを追加しなければ削除される可能性があるワークスペースについて通知するようになりました。
- Kaspersky Security Center Cloud コンソールは、 Kaspersky Endpoint Security 11.11.0 for Windows をサポートするようになりました。
- Kaspersky Security Center Cloud コンソールは、Kaspersky Endpoint Detection and Response Optimum 2.3 のサポートを開始しました。
- Kaspersky Embedded Systems Security 3.2 for Windows がサポートされるようになりました。

2022 年 9 月のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- 仮想管理サーバー専用の管理者を割り当てることができるようになりました。管理者用のユーザーアカウントを作成し、管理者に仮想管理サーバーへのアクセス権を付与します。割り当てられた管理者は、選択した仮想管理サーバーにのみアクセスでき、物理または仮想のプライマリ管理サーバーまたはその他のセカンダリ管理サーバーには接続できません。
- Kaspersky Security Center Cloud コンソールのライセンスを削除する際の操作が最適化されました。新しいメカニズムにより、最後の現在のライセンスを誤って削除するリスクを低減します。
- Linux ベースのディストリビューションポイントを使用して、*ディストリビューションポイントのリポジトリへのアップデートのダウンロード*タスクから、カスペルスキーのセキュリティ製品の定義データベースをダウンロードできるようになりました。
- ネットワークエージェントが日本語で使用可能になりました。

- Kaspersky Security Center Cloud コンソール のインターフェイスでは、セクション名はすべて大文字で表示されていましたが、最初の 1 文字のみが大文字で表示されるよう変更されました。

2022 年 8 月のアップデート

新しい言語のサポート：Kaspersky Security Center Cloud コンソールを日本語で利用できるようになりました。

2022 年 7 月のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- 新たにサポート対象となったカスペルスキー製品のバージョン：
  - Kaspersky Endpoint Agent 3.13
  - Kaspersky Endpoint Security 11.2.1 for Mac
  - Kaspersky Endpoint Security for iOS 1.0.0
  - Kaspersky Endpoint Security 11.10.0 for Windows
- Kaspersky Security Center Cloud コンソールの契約書およびデータ処理契約書の本文を更新しました。
- 新しい言語のサポート：Kaspersky Security Center Cloud コンソールのインフラストラクチャを日本語で利用できるようになりました。Kaspersky Security Center Cloud コンソールのワークスペースも、近く日本語で利用できるようになる予定です。

2022 年 4 月のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- Kaspersky Security Center Cloud コンソールは、Kaspersky Endpoint Security 11.9.0 for Windows をサポートするようになりました。
- Kaspersky Security Center Cloud コンソールは、Kaspersky Embedded Systems Security の日本語をサポートするようになりました。

2022 年 3 月 9 日のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- Kaspersky Endpoint Detection and Response Expert との連携が実装されました。
- インシデントレスポンスプラットフォーム（IRP）が実装されました。Kaspersky Security Center Cloud コンソールを使用して、セキュリティインシデントを管理できるようになりました。
- Kaspersky Security Center Cloud コンソールは、Kaspersky Endpoint Detection and Response Expert のライセンスを受け入れるようになりました。ライセンスの最小デバイス数は 50 です。

2022 年 2 月 11 日のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- Kaspersky Embedded Systems Security for Windows のライセンスをサポートするようになりました。
- Kaspersky Endpoint Security 11.8.0 for Windows がサポートされるようになりました。
- 日本語の配布パッケージを使用して Kaspersky Endpoint Security 11.8.0 for Windows をインストールできます。
- Kaspersky Endpoint Agent 3.11 がサポートされるようになりました。

2021 年 12 月 10 日のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- 内部ユーザーとの連携が改善されました。
  - ポータルで新規の内部ユーザーを追加できるようになりました。
  - ユーザー自身の権限の削除を防ぐようになりました。

2021 年 10 月 18 日のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- Kaspersky Security Center Cloud コンソールは、Kaspersky Endpoint Detection and Response Optimum 2.0 のサポートを開始しました。
- Kaspersky Security Center Cloud コンソールを使用して Android を実行しているモバイルデバイスを管理できるようになりました。
- 「マーケットプレイス」が新しいメニューセクションとして使用可能になりました。Kaspersky Security Center Cloud コンソールを使用してカスペルスキー製品を検索できます。
- 「カスペルスキーからの通知」が新しいメニューセクションとして使用可能になりました。カスペルスキーからの通知には、管理対象デバイスにインストールされているカスペルスキー製品に関連する情報が提供されます。このセクションの情報は定期的にアップデートされます。
- Kaspersky Security Center Cloud コンソールを使用して、Linux オペレーティングシステムで実行されているセカンダリ管理サーバーを管理できるようになりました。

2021 年 9 月 7 日のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- 新しいユーザーアカウントを作成せず、Active Directory アカウントを使用して、Active Directory フェデレーションサービス（ADFS）で Kaspersky Security Center Cloud コンソールにログインできるようになりました。

- Kaspersky Security Center Cloud コンソールを、Amazon Web Services、Microsoft Azure、Google Cloud のクラウド環境で利用できるようになりました。クラウド環境で仮想マシン（またはインスタンス）を保護するには、Kaspersky Hybrid Cloud Security ライセンスのいずれかが必要です。クラウド環境設定ウィザードを使用できます。

- ワークスペースあたりのデバイスの上限が 25,000 台になりました。

- Kaspersky Security Center Cloud コンソールで SIEM システムとの統合が使用可能になりました。Syslog プロトコルを使用して、SIEM システムにイベントをエクスポートできます。

- 仮想管理サーバーを作成できるようになりました。各仮想管理サーバーに、管理グループ、ポリシー、タスク、レポート、イベントの独自の構造を設定できます。仮想管理サーバーを使用すると、ワークフローが複雑なクライアント組織をワークスペース内で管理できます。ただし、オンプレミスで実行されている Kaspersky Security Center から Kaspersky Security Center Cloud コンソールに仮想管理サーバーを移行することはできません。

- 表の列の幅を調整し、データを並べ替えて検索できるようになりました。

- Kaspersky Business Hub と Kaspersky Security Center Cloud コンソールの安定性と可用性が改善されました。

2021 年 10 月 27 日のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- Kaspersky Security Center Cloud コンソールで、Kaspersky Endpoint Security 11.6.0 for Windows、Kaspersky Endpoint Security 11.1 for Mac パッチ A、Kaspersky Endpoint Agent 3.10（Kaspersky Endpoint Detection and Response Optimum の一部として）がサポートされるようになりました。

- 次のライセンスを使用できるようになりました：

  - Kaspersky Endpoint Detection and Response Optimum

  - Kaspersky Endpoint Security for Business Advanced

  - Kaspersky Total Security for Business

- 次の機能が実装されました：

  - 脆弱性とパッチ管理

  - 暗号化の管理

  - アプリケーションコントロール

  - アダプティブアノマリーコントロール

  - Windows デスクトップ共有を含む RDP セッション

- ナビゲーションメニューが縦型になり、Kaspersky Security Center の Microsoft 管理コンソールベースのインターフェイスに近いものになりました。

- テクニカルトレーニングのビデオを利用できるようになりました。製品の仕組みについて確認できます。

2020 年 6 月 30 日のアップデート

この Kaspersky Security Center Cloud コンソールのアップデートには、次の新機能と機能強化が追加されています：

- Kaspersky Security Center Cloud コンソールで、Kaspersky Security 11 for Windows Server がサポートされるようになりました（2020 年 9 月以降）。

- Kaspersky Security Center Cloud コンソールで、Kaspersky Endpoint Agent 3.9 および Kaspersky Endpoint Security 11.4.0 for Windows がサポートされるようになりました。

- クイックスタートウィザードが改善されました。使いやすさのため、いくつかのステップがなくなり、一連のステップが若干変更され、一部のテキストが編集されました。

- イタリア語で Kaspersky Security Center Cloud コンソールを利用できるようになりました。

- Kaspersky Security Center Cloud コンソールのインターフェイスから、任意の管理対象カスペルスキー製品の使用許諾契約書（EULA）への同意を取り消すことができるようになりました。EULA への同意を取り消す前に、選択したアプリケーションをアンインストールする必要があります。

- ワークスペースを削除できるようになりました。ワークスペースを削除用にマーキングすると、既定では 7 日後に自動的に削除されます。ただし、すぐに削除されるよう、ワークスペースの削除を強制できます。

- コンソールへのサインインに二段階認証が実装されました。

Kaspersky Security Center Cloud コンソール

このセクションでは、Kaspersky Security Center Cloud コンソールの目的、および主な機能とコンポーネントについて説明します。

Kaspersky Security Center Cloud コンソールは、カスペルスキーがホストおよび維持する製品です。ユーザーが Kaspersky Security Center Cloud コンソールをコンピューターまたはサーバーにインストールする必要はありません。Kaspersky Security Center Cloud コンソールにより、管理者はカスペルスキーのセキュリティ製品を企業ネットワークのデバイスにインストールしたり、リモートでスキャンを実行してタスクをアップデートしたり、管理対象アプリケーションのセキュリティポリシーを管理したりできます。管理者は、組織用デバイスのステータスのスナップショット、詳細なレポート、粒度の細かい保護ポリシーの設定を備えた、詳細なダッシュボードを使用できます。

Kaspersky Security Center Cloud コンソールの概要

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

Kaspersky Security Center Cloud コンソールでは、次のような操作が可能です：

- ネットワーク上のデバイスへのカスペルスキー製品のインストールおよびインストールされた製品の管理。
- 管理グループの階層を作成して、いくつかのクライアントデバイスを1つの単位として管理する。
- 仮想管理サーバーを作成し、階層に配置する。
- ワークステーションやサーバーを含む、ネットワークデバイスを保護する：
  - カスペルスキー製品で構築されたアンチマルウェアによる保護システムを管理する。
  - 次のような、検知とレスポンス（EDR および MDR）の機能を使用する（Kaspersky Endpoint Detection and Response または Kaspersky Managed Detection and Response のライセンスが必要）：
    - インシデントの分析と調査
    - 脅威の活動連鎖の図表の作成によるインシデントの可視化
    - レスポンスに対する手動の許可または拒否、またはすべてのレスポンスに対する自動許可の設定
- Kaspersky Security Center Cloud コンソールをマルチテナントアプリケーションとして使用する。
- クライアントデバイスにインストールされているカスペルスキー製品をリモートで管理する。
- クライアントデバイスに対するカスペルスキー製品のライセンスの一元的な配信を実行する。
- ネットワーク上のデバイスのセキュリティポリシーを作成して管理する。
- ユーザーアカウントを作成して管理する。
- ユーザーロールを作成して管理する（RBAC）。
- ネットワーク上のデバイスにインストールされた製品のタスクを作成して管理する。

- 各クライアント組織のセキュリティシステムのステータスに関するレポートを個別に表示する。

Kaspersky Security Center Cloud コンソールは、ブラウザーを使用してデバイスと管理サーバーとのインタラクションが確実に行われるようにする、クラウドベースの管理コンソールを使用して管理します。管理サーバーは、ネットワーク内のデバイスにインストールされたカスペルスキー製品の管理を目的として設計されたアプリケーションです。ブラウザーを使用して Kaspersky Security Center Cloud コンソールに接続する場合、ブラウザーは Kaspersky Security Center Cloud コンソールサーバーとの接続を確立します。

管理サーバーと、接続されたデータベース管理システム（DBMS）はクラウド環境に展開されており、サービスとしてユーザーに提供されます。管理サーバーと DBMS 双方のメンテナンスはサービスの一部です。Kaspersky Security Center Cloud コンソールのすべてのソフトウェアコンポーネントが最新状態に維持されます。管理サーバーと作成されたオブジェクト（ポリシーやタスクなど）は、安全性を維持するため定期的にバックアップされます。

Kaspersky Security Center Cloud コンソールは多言語で利用できます。本製品を開き直さずに、任意のタイミングでインターフェイスの言語を変更できます。

Kaspersky Security Center Cloud コンソールのシステム要件

管理コンソール

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

> Kaspersky Security Center Cloud コンソールの操作には、ブラウザーウィンドウまたはタブを 1 つしか使用できません。

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

ブラウザー：

- Google Chrome 100.0.4896.88 以降（Official Build）
- Microsoft Edge 100 以降
- macOS 上の Safari 15
- 「Yandex」ブラウザー 23.5.0.2271
- Mozilla Firefox 延長サポートリリース 102.0 またはそれ以降

ネットワークエージェント

ハードウェアの最小要件：

- CPU：動作周波数が 1 GHz 以上（64 ビット OS の場合、最小周波数は 1.4 GHz）
- メモリ：512 MB

- 使用可能なディスク容量：1 GB

脆弱性とパッチの管理のためのハードウェアの最小要件：

- CPU：動作周波数が 1.4 GHz 以上（64 ビット OS が必要です）
- メモリ：8 GB
- 使用可能なディスク容量：1 GB

ネットワークエージェントがサポートするオペレーティングシステム

オペレーティングシステム： Microsoft Windows	Microsoft Windows Embedded POSReady 2009（最新の Service Pack）32 ビット Microsoft Windows Embedded 7 Standard（Service Pack 1）32 ビット / 64 ビット Microsoft Windows Embedded 8.1 Industry Pro 32 ビット / 64 ビット Microsoft Windows 10 Enterprise 2015 LTSB 32 ビット / 64 ビット Microsoft Windows 10 Enterprise 2016 LTSB 32 ビット / 64 ビット Microsoft Windows 10 IoT Enterprise 2015 LTSB 32 ビット / 64 ビット Microsoft Windows 10 IoT Enterprise 2016 LTSB 32 ビット / 64 ビット Microsoft Windows 10 Enterprise 2019 LTSC 32 ビット / 64 ビット Microsoft Windows 10 IoT Enterprise バージョン 1703 32 ビット / 64 ビット Microsoft Windows 10 IoT Enterprise バージョン 1709 32 ビット / 64 ビット Microsoft Windows 10 IoT Enterprise バージョン 1803 32 ビット / 64 ビット Microsoft Windows 10 IoT Enterprise バージョン 1809 32 ビット / 64 ビット Microsoft Windows 10 20H2 IoT Enterprise 32 ビット / 64 ビット Microsoft Windows 10 21H2 IoT Enterprise 32 ビット / 64 ビット Microsoft Windows 10 IoT Enterprise 32 ビット / 64 ビット Microsoft Windows 10 IoT Enterprise バージョン 1909 32 ビット / 64 ビット Microsoft Windows 10 IoT Enterprise LTSC 2021 32 ビット / 64 ビット Microsoft Windows 10 IoT Enterprise バージョン 1607 32 ビット / 64 ビット Microsoft Windows 10 Home RS3（Fall Creators Update、v1709）32 ビット / 64 ビット Microsoft Windows 10 Pro RS3（Fall Creators Update、v1709）32 ビット / 64 ビット Microsoft Windows 10 Pro for Workstations RS3（Fall Creators Update、v1709）32 ビット / 64 ビット Microsoft Windows 10 Enterprise RS3（Fall Creators Update、v1709）32 ビット / 64 ビット Microsoft Windows 10 Education RS3（Fall Creators Update、v1709）32 ビット / 64 ビット Microsoft Windows 10 Home RS4（April 2018 Update、17134）32 ビット / 64 ビット

Microsoft Windows 10 Pro RS4（April 2018 Update、17134）32 ビット / 64 ビット

Microsoft Windows 10 Pro for Workstations RS4（April 2018 Update、17134）32 ビット / 64 ビット

Microsoft Windows 10 Enterprise RS4（April 2018 Update、17134）32 ビット / 64 ビット

Microsoft Windows 10 Education RS4（April 2018 Update、17134）32 ビット / 64 ビット

Microsoft Windows 10 Home RS5（October 2018）32 ビット / 64 ビット

Microsoft Windows 10 Pro RS5（October 2018）32 ビット / 64 ビット

Microsoft Windows 10 Pro for Workstations RS5（October 2018）32 ビット / 64 ビット

Microsoft Windows 10 Enterprise RS5（October 2018）32 ビット / 64 ビット

Microsoft Windows 10 Education RS5（October 2018）32 ビット / 64 ビット

Microsoft Windows 10 Home 19H1 32 ビット / 64 ビット

Microsoft Windows 10 Pro 19H1 32 ビット / 64 ビット

Microsoft Windows 10 Pro for Workstations 19H1 32 ビット / 64 ビット

Microsoft Windows 10 Enterprise 19H1 32 ビット / 64 ビット

Microsoft Windows 10 Education 19H1 32 ビット / 64 ビット

Microsoft Windows 10 Home 19H2 32 ビット / 64 ビット

Microsoft Windows 10 Pro 19H2 32 ビット / 64 ビット

Microsoft Windows 10 Pro for Workstations 19H2 32 ビット / 64 ビット

Microsoft Windows 10 Enterprise 19H2 32 ビット / 64 ビット

Microsoft Windows 10 Education 19H2 32 ビット / 64 ビット

Microsoft Windows 10 Home 20H1（May 2020 Update）32 ビット / 64 ビット

Microsoft Windows 10 Pro 20H1（May 2020 Update）32 ビット / 64 ビット

Microsoft Windows 10 Enterprise 20H1（May 2020 Update）32 ビット / 64 ビット

Microsoft Windows 10 Education 20H1（May 2020 Update）32 ビット / 64 ビット

Microsoft Windows 10 Home 20H2（October 2020 Update）32 ビット / 64 ビット

Microsoft Windows 10 Pro 20H2（October 2020 Update）32 ビット / 64 ビット

Microsoft Windows 10 Enterprise 20H2（October 2020 Update）32 ビット / 64 ビット

Microsoft Windows 10 Education 20H2（October 2020 Update）32 ビット / 64 ビット

Microsoft Windows 10 Home 21H1（May 2021 Update）32 ビット / 64 ビット

Microsoft Windows 10 Pro 21H1（May 2021 Update）32 ビット / 64 ビット

Microsoft Windows 10 Enterprise 21H1（May 2021 Update）32 ビット / 64 ビット

Microsoft Windows 10 Education 21H1（May 2021 Update）32 ビット / 64 ビット

Microsoft Windows 10 Home 21H2（October 2021 Update）32 ビット / 64 ビット

Microsoft Windows 10 Pro 21H2（October 2021 Update）32 ビット / 64 ビット

Microsoft Windows 10 Enterprise 21H2（October 2021 Update）32 ビット / 64 ビット

Microsoft Windows 10 Education 21H2（October 2021 Update）32 ビット / 64 ビット

Microsoft Windows 10 Home 22H2 (October 2023 Update) 32 ビット / 64 ビット

Microsoft Windows 10 Pro 22H2 (October 2023 Update) 32 ビット / 64 ビット

Microsoft Windows 10 Enterprise 22H2 (October 2023 Update) 32 ビット / 64 ビット

Microsoft Windows 10 Education 22H2 (October 2023 Update) 32 ビット / 64 ビット

Microsoft Windows 11 Home 64 ビット

Microsoft Windows 11 Pro 64 ビット

Microsoft Windows 11 Enterprise 64 ビット

Microsoft Windows 11 Education 64 ビット

Microsoft Windows 11 22H2

Microsoft Windows 8.1 Pro 32 ビット / 64 ビット

Microsoft Windows 8.1 Enterprise 32 ビット / 64 ビット

Microsoft Windows 8 Pro 32 ビット / 64 ビット

Microsoft Windows 8 Enterprise 32 ビット / 64 ビット

Microsoft Windows 7 Professional（Service Pack 1 以降）32 ビット / 64 ビット

Microsoft Windows 7 Enterprise / Ultimate（Service Pack 1 以降）32 ビット / 64 ビット

Microsoft Windows 7 Home Basic/Premium（Service Pack 1 以降）32 ビット / 64 ビット

Microsoft Windows XP Professional（Service Pack 3 以降）32 ビット

Microsoft Windows XP Professional for Embedded Systems（Service Pack 3）32 ビット

Windows MultiPoint Server 2011 Standard / Premium 64 ビット

Windows Server 2008 Foundation（Service Pack 2）32 ビット / 64 ビット

Windows Server 2008 Service Pack 2（すべてのエディション）32 ビット / 64 ビット

Windows Server 2008 R2 Datacenter（Service Pack 1 以降）64 ビット

Windows Server 2008 R2 Enterprise（Service Pack 1 以降）64 ビット

Windows Server 2008 R2 Foundation（Service Pack 1 以降）64 ビット

Windows Server 2008 R2 Core Mode（Service Pack 1 以降）64 ビット

	Windows Server 2008 R2 Standard（Service Pack 1 以降）64 ビット Windows Server 2008 R2（Service Pack 1）（すべてのエディション）64 ビット Windows Server 2012 Server Core 64 ビット Windows Server 2012 Datacenter 64 ビット Windows Server 2012 Essentials 64 ビット Windows Server 2012 Foundation 64 ビット Windows Server 2012 Standard 64 ビット Windows Server 2012 R2 Server Core 64 ビット Windows Server 2012 R2 Datacenter 64 ビット Windows Server 2012 R2 Essentials 64 ビット Windows Server 2012 R2 Foundation 64 ビット Windows Server 2012 R2 Standard 64 ビット Windows Server 2016 Datacenter（LTSB）64 ビット Windows Server 2016 Standard（LTSB）64 ビット Windows Server 2016 Server Core（インストールオプション）（LTSB）64 ビット Windows Server 2019 Standard 64 ビット Windows Server 2019 Datacenter 64 ビット Windows Server 2019 Core 64 ビット Windows Server 2022 Standard 64 ビット Windows Server 2022 Datacenter 64 ビット Windows Server 2022 Core 64 ビット
オペレーティングシステム： Linux	Debian GNU/Linux 12（Bookworm） Debian GNU/Linux 11.x（Bullseye）32 ビット / 64 ビット Debian GNU/Linux 10.x（Buster）32 ビット / 64 ビット Ubuntu Server 22.04 LTS（Jammy Jellyfish）64 ビット Ubuntu Server 20.04 LTS（Focal Fossa）32 ビット / 64 ビット Ubuntu Server 18.04 LTS（Bionic Beaver）32 ビット / 64 ビット CentOS ストリーム 9 64 ビット CentOS 7.x 64 ビット Red Hat Enterprise Linux Server 9.x 64 ビット Red Hat Enterprise Linux Server 8.x 64 ビット Red Hat Enterprise Linux Server 7.x 64 ビット Red Hat Enterprise Linux Server 6.x 32 ビット / 64 ビット SUSE Linux Enterprise Server 12（すべての Service Pack）64 ビット SUSE Linux Enterprise Server 15（すべての Service Pack）64 ビット openSUSE 15 64 ビット Oracle Linux 7 64 ビット Oracle Linux 8 64 ビット Oracle Linux 9 64 ビット Linux Mint 20.x 64 ビット
オペレーティングシステム：	macOS Big Sur（11.x）

macOS	macOS Monterey（12.x） macOS Ventura（13.x）

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

次の仮想化プラットフォームがサポートされています：

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64 ビット
- Microsoft Hyper-V Server 2012 R2 64 ビット
- Microsoft Hyper-V Server 2016 64 ビット
- Microsoft Hyper-V Server 2019 64 ビット
- Microsoft Hyper-V Server 2022 64 ビット
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- カーネルベースの仮想マシン（ネットワークエージェントによってサポートされるすべての Linux オペレーティングシステム）

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

サポートされていないオペレーティングシステムとプラットフォーム

ネットワークエージェント

次のオペレーティングシステムはサポートされていません：

- Microsoft Windows Embedded POSReady 7 32 ビット / 64 ビット
- Microsoft Windows Embedded 8 Industry Pro 32 ビット / 64 ビット
- Microsoft Windows Embedded 8 Industry Enterprise 32 ビット / 64 ビット
- Microsoft Windows Embedded 8 Standard 32 ビット / 64 ビット
- Microsoft Windows Embedded 8.1 Industry Enterprise 32 ビット / 64 ビット
- Microsoft Windows Embedded 8.1 Industry Update 32 ビット / 64 ビット
- Microsoft Windows 10 Home（Threshold 1、1507）32 ビット / 64 ビット
- Microsoft Windows 10 Pro（Threshold 1、1507）32 ビット / 64 ビット
- Microsoft Windows 10 Enterprise（Threshold 1、1507）32 ビット / 64 ビット
- Microsoft Windows 10 Education（Threshold 1、1507）32 ビット / 64 ビット
- Microsoft Windows 10 Mobile（Threshold 1、1507）32 ビット
- Microsoft Windows 10 Mobile Enterprise（Threshold 1、1507）32 ビット
- Microsoft Windows 10 Home Threshold 2（November 2015 Update、1511）32 ビット / 64 ビット
- Microsoft Windows 10 Pro Threshold 2（November 2015 Update、1511）32 ビット / 64 ビット
- Microsoft Windows 10 Enterprise Threshold 2（November 2015 Update、1511）32 ビット / 64 ビット
- Microsoft Windows 10 Education Threshold 2（November 2015 Update、1511）32 ビット / 64 ビット
- Microsoft Windows 10 Mobile Threshold 2（November 2015 Update、1511）32 ビット
- Microsoft Windows 10 Mobile Enterprise Threshold 2（November 2015 Update、1511）32 ビット
- Microsoft Windows 10 Home RS1（Anniversary Update、1607）32 ビット / 64 ビット
- Microsoft Windows 10 Pro RS1（Anniversary Update、1607）32 ビット / 64 ビット
- Microsoft Windows 10 Enterprise RS1（Anniversary Update、1607）32 ビット / 64 ビット
- Microsoft Windows 10 Education RS1（Anniversary Update、1607）32 ビット / 64 ビット
- Microsoft Windows 10 Mobile RS1（Anniversary Update、1607）32 ビット
- Microsoft Windows 10 Mobile Enterprise RS1（Anniversary Update、1607）32 ビット
- Microsoft Windows 10 Home RS2（Creators Update、1703）32 ビット / 64 ビット
- Microsoft Windows 10 Pro RS2（Creators Update、1703）32 ビット / 64 ビット
- Microsoft Windows 10 Enterprise RS2（Creators Update、1703）32 ビット / 64 ビット
- Microsoft Windows 10 Education RS2（Creators Update、1703）32 ビット / 64 ビット

- Microsoft Windows 10 Mobile RS2（Creators Update、1703）32 ビット
- Microsoft Windows 10 Mobile Enterprise RS2（Creators Update、1703）32 ビット
- Microsoft Windows 10 Mobile RS3 32 ビット
- Microsoft Windows 10 Mobile Enterprise RS3 32 ビット
- Microsoft Windows 10 Mobile RS4 32 ビット
- Microsoft Windows 10 Mobile Enterprise RS4 32 ビット
- Microsoft Windows 10 Mobile RS5 32 ビット
- Microsoft Windows 10 Mobile Enterprise RS5 32 ビット
- Microsoft Windows 8（Core）32 ビット / 64 ビット
- Microsoft Windows 7 Professional 32 ビット / 64 ビット
- Microsoft Windows 7 Enterprise/Ultimate 32 ビット / 64 ビット
- Microsoft Windows 7 Home Basic/Premium 32 ビット / 64 ビット
- Microsoft Windows Vista Business（Service Pack 1）32 ビット / 64 ビット
- Microsoft Windows Vista Enterprise（Service Pack 1）32 ビット / 64 ビット
- Microsoft Windows Vista Ultimate（Service Pack 1）32 ビット / 64 ビット
- Microsoft Windows Vista Business（Service Pack 2 以降）32 ビット / 64 ビット
- Microsoft Windows Vista Enterprise（Service Pack 2 以降）32 ビット / 64 ビット
- Microsoft Windows Vista Ultimate（Service Pack 2 以降）32 ビット / 64 ビット
- Microsoft Windows XP Professional（Service Pack 2）32 ビット / 64 ビット
- Microsoft Windows XP Home Service Pack 3 以降 32 ビット
- Windows Essential Business Server 2008 Standard 64 ビット
- Windows Essential Business Server 2008 Premium 64 ビット
- Windows Small Business Server 2003 Standard（Service Pack 1）32 ビット
- Windows Small Business Server 2003 Premium（Service Pack 1）32 ビット
- Windows Small Business Server 2008 Standard 64 ビット
- Windows Small Business Server 2008 Premium 64 ビット
- Windows Small Business Server 2011 Premium Add-on 64 ビット
- Windows Small Business Server 2011 Standard 64 ビット

- Windows Small Business Server 2011 Essentials 64 ビット
- Windows Home Server 2011 64 ビット
- Windows MultiPoint Server 2010 Standard 64 ビット
- Windows MultiPoint Server 2010 Premium 64 ビット
- Windows MultiPoint Server 2012 Standard / Premium 64 ビット
- Microsoft Windows 2000 Server 32 ビット
- Windows Server 2003 Enterprise（Service Pack 2）32 ビット / 64 ビット
- Windows Server 2003 Standard（Service Pack 2）32 ビット / 64 ビット
- Windows Server 2003 R2 Enterprise（Service Pack 2）32 ビット / 64 ビット
- Windows Server 2003 R2 Standard（Service Pack 2）32 ビット / 64 ビット
- Windows Server 2008 Datacenter Service Pack 1 32 ビット / 64 ビット
- Windows Server 2008 Enterprise Service Pack 1 32 ビット / 64 ビット
- Windows Server 2008 Service Pack 1 Server Core 32 ビット / 64 ビット
- Windows Server 2008 Standard Service Pack 1 32 ビット / 64 ビット
- Windows Server 2008 Standard 32 ビット / 64 ビット
- Windows Server 2008 Enterprise 32 ビット / 64 ビット
- Windows Server 2008 Datacenter 32 ビット / 64 ビット
- Windows Server 2008 R2 Server Core 64 ビット
- Windows Server 2008 R2 Datacenter 64 ビット
- Windows Server 2008 R2 Enterprise 64 ビット
- Windows Server 2008 R2 Foundation 64 ビット
- Windows Server 2008 R2 Standard 64 ビット
- Windows Server 2016 Nano（インストールオプション）（CBB）
- Windows Storage Server 2008 32 ビット / 64 ビット
- Windows Storage Server 2008 Service Pack 2 64 ビット
- Windows Storage Server 2008 R2 64 ビット
- Windows Storage Server 2012 64 ビット
- Windows Storage Server 2012 R2 64 ビット

- Windows Storage Server 2016 64 ビット
- Windows Storage Server 2019 64 ビット
- Debian GNU/Linux 7.x（7.8 まで）32 ビット / 64 ビット
- Debian GNU/Linux 8.x（Jessie）32 ビット / 64 ビット
- Debian GNU/Linux 9.x（Stretch）32 ビット / 64 ビット
- Ubuntu Server 14.04 LTS（Trusty Tahr）32 ビット / 64 ビット
- Ubuntu Server 16.04 LTS（Xenial Xerus）32 ビット / 64 ビット
- Ubuntu Desktop 14.04 LTS（Trusty Tahr）32 ビット / 64 ビット
- Ubuntu Desktop 16.04 LTS（Xenial Xerus）32 ビット / 64 ビット
- Ubuntu Server 20.04.04 LTS（Focal Fossa）ARM 64 ビット
- Ubuntu Desktop 20.04 LTS（Focal Fossa）32 ビット / 64 ビット
- Ubuntu Desktop 18.04 LTS（Bionic Beaver）32 ビット / 64 ビット
- CentOS 6.x（6.6 まで）64 ビット
- CentOS 7.x ARM 64 ビット
- CentOS 8.x 64 ビット
- SUSE Linux Enterprise Desktop 12（すべての SP）64 ビット
- SUSE Linux Enterprise Desktop 15（すべての Service Pack）64 ビット
- SUSE Linux Enterprise Desktop 15（Service Pack 3）ARM 64 ビット
- ALT Server 10 64 ビット
- ALT Server 9.2 64 ビット
- ALT Workstation 10 32 ビット / 64 ビット
- ALT Workstation 9.2 32 ビット / 64 ビット
- ALT 8 SP Server（LKNV.11100-01）64 ビット
- ALT 8 SP Server（LKNV.11100-02）64 ビット
- ALT 8 SP Server（LKNV.11100-03）64 ビット
- ALT 8 SP Workstation（LKNV.11100-01）32 ビット / 64 ビット
- ALT 8 SP Workstation（LKNV.11100-02）32 ビット / 64 ビット
- ALT 8 SP Workstation（LKNV.11100-03）32 ビット / 64 ビット

- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64 ビット
- Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.7）64 ビット
- Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.6）64 ビット
- Astra Linux Common Edition（運用アップデート 2.12）64 ビット
- Astra Linux Special Edition RUSB.10152-02（運用アップデート 4.7）ARM 64 ビット
- Linux Mint 19.x 64 ビット
- AlterOS 7.5 以降 64 ビット
- Lotos（Linux コア バージョン 4.19.50、DE: MATE）64 ビット
- Mageia 4 32 ビット
- GosLinux IC6 64 ビット
- RED OS 7.3 64 ビット
- RED OS 7.3 Server 64 ビット
- RED OS 7.3 Certified Edition 64 ビット
- ROSA COBALT 7.9 64 ビット
- ROSA CHROME 12 64 ビット
- ROSA Enterprise Linux Server 7.3 64 ビット
- ROSA Enterprise Linux Desktop 7.3 64 ビット
- ROSA COBALT Workstation 7.3 64 ビット
- ROSA COBALT Server 7.3 64 ビット
- OS X 10.10 (Yosemite)
- OS X 10.11（El Capitan）
- macOS Sierra（10.12）
- macOS High Sierra（10.13）
- macOS Mojave（10.14）
- macOS Catalina（10.15）

次の仮想化プラットフォームはサポートされていません：

- VMware vSphere 4.1

- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64 ビット
- Microsoft Hyper-V Server 2008 R2 64 ビット
- Microsoft Hyper-V Server 2008 R2 Service Pack 1 以降 64 ビット
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7

互換性のあるカスペルスキーのアプリケーションとソリューション

異なる製品のライセンスにより、異なるカスペルスキー製品およびソリューションのセットが付与されます。

Kaspersky Security Center Cloud コンソールを使用して、次のカスペルスキー製品とソリューションを導入および管理できます：

- Kaspersky Security for Windows Server 11.0.1
- Kaspersky Endpoint Security 12.4 for Windows
- Kaspersky Endpoint Security 12.0 for Linux
- Kaspersky Endpoint Security 12.0 for Mac

- Kaspersky Embedded Systems Security 3.3 for Windows
- Kaspersky Embedded Systems Security 3.3 for Windows
- Kaspersky Endpoint Agent 3.16
- Kaspersky Endpoint Security for Android
- Kaspersky Endpoint Security for iOS

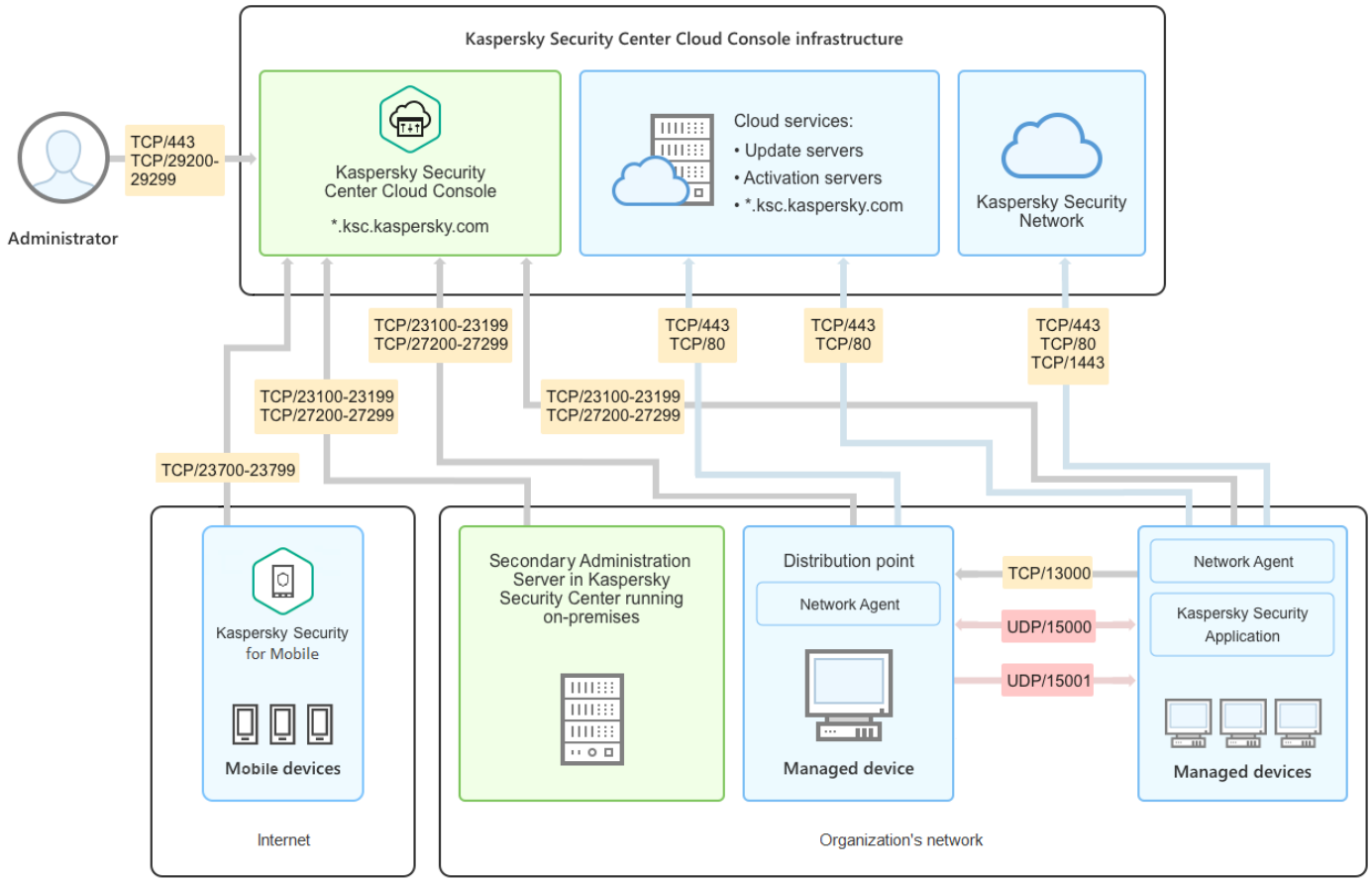
次のソリューションを統合して、セキュリティインシデントを表示および処理できます：

- Kaspersky Managed Detection and Response
- Kaspersky Endpoint Detection and Response Optimum 2.3
- Kaspersky Endpoint Detection and Response Expert

管理対象デバイスに新しいバージョンの製品をインストールし、ポリシーをアップデートせずに以前のポリシーを新しいバージョンの製品で使用しても、Kaspersky Security Center Cloud コンソールには製品からデータが提供されます。ただし、Kaspersky Security Center Cloud コンソールでは、ヘルプの処理される管理対象アプリケーションのデータに関するセクションで説明されているようにこのデータを処理できません。Kaspersky Security Center Cloud コンソールでこのデータを処理するには、新しいバージョンの製品用に新しいポリシーを作成する必要があります。

アーキテクチャ

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



Kaspersky Security Center Cloud コンソールのアーキテクチャ

クラウドベースのコンソールで管理される Kaspersky Security Center Cloud コンソールには主なコンポーネントが 2 つあります。Kaspersky Security Center Cloud コンソールのインフラストラクチャと顧客のインフラストラクチャです。

Kaspersky Security Center Cloud コンソールのインフラストラクチャは以下で構成されます：

- **クラウドベースの管理コンソール**：Kaspersky Security Center Cloud コンソールにより管理されているクライアント組織のネットワークの保護システムの構築や管理が可能な Web インターフェイスです。
- **クラウドサービス**：アップデートサーバーとアクティベーションサーバーを含みます。
- **Kaspersky Security Network（KSN）**：ファイル、Web リソース、ソフトウェアの評価情報が継続的にアップデートされるカスペルスキーのデータベースを格納するサーバー。KSN を使用することで、カスペルスキー製品がより迅速に新しい脅威に対応します。また、一部の保護コンポーネントのパフォーマンスが向上し、誤検知の可能性が減ります。

顧客のインフラストラクチャは以下で構成される場合があります：

- **ディストリビューションポイント**：ネットワークエージェントがインストールされており、アップデートの配信、ネットワークポーリング、アプリケーションのリモートインストール、管理グループやブロードキャストドメインでのコンピューター情報の取得に使用されるコンピューター。管理者が適切なデバイスを選択し、ディストリビューションポイントを手動で割り当てます。
- **管理対象デバイス**：Kaspersky Security Center Cloud コンソールで管理される、顧客のネットワークのコンピューター。各管理対象デバイスには、ネットワークエージェントとカスペルスキーのセキュリティ製品がインストールされている必要があります。

- **オンプレミスで実行されているセカンダリ管理サーバー**（任意）。オンプレミスの管理サーバーを使用して、管理サーバーの階層を作成できます。

Kaspersky Security Center Cloud コンソールで使用されるポート

カスペルスキーのインフラストラクチャに含まれる Kaspersky Security Center Cloud コンソールを使用するには、クライアントデバイスで次のポートを開き、インターネット接続を許可する必要があります（次の表を参照）：

クライアントデバイスで開いてインターネット接続を許可する必要があるポート：

ポート（またはポート範囲）	プロトコル	ポート（またはポート範囲）の目的
23100 ～ 23199	TCP/TLS	*.ksc.kaspersky.com の Kaspersky Security Center Cloud コンソール管理サーバーで、ネットワークエージェントとセカンダリ管理サーバーから接続を受信する。 カスペルスキーのインフラストラクチャは、この範囲内の任意のポート、およびこのマスク内の任意の URL を使用可能。ポートと URL は変更される場合があります。
23700 ～ 23799 （モバイルデバイスを管理している場合のみ）	TCP/TLS	モバイルデバイスから接続を受信する。 *.ksc.kaspersky.com の Kaspersky Security Center Cloud コンソール管理サーバーへの接続。 カスペルスキーのインフラストラクチャは、この範囲内の任意のポート、およびこのマスク内の任意の URL を使用可能。ポートと URL は変更される場合があります。
27200 ～ 27299	TCP/TLS	管理対象デバイスから製品のアクティベーション用の接続を受信する（モバイルデバイスを除く）。 *.ksc.kaspersky.com の Kaspersky Security Center Cloud コンソール管理サーバーへの接続。 カスペルスキーのインフラストラクチャは、この範囲内の任意のポート、およびこのマスク内の任意の URL を使用可能。ポートと URL は変更される場合があります。
29200 ～ 29299	TCP/TLS	*.ksc.kaspersky.com の Kaspersky Security Center Cloud コンソール管理サーバーから klsctunnel ユーティリティを使用した、管理対象デバイスへのトンネリング接続。 カスペルスキーのインフラストラクチャは、この範囲内の任意のポート、およびこのマスク内の任意の URL を使用可能。ポートと URL は変更される場合があります。
443	HTTPS	*.ksc.kaspersky.com の Kaspersky Security Center Cloud コンソールの discovery サービスへの接続。 カスペルスキーのインフラストラクチャでは、このマスク内で任意の Web アドレスを使用できます。
1443	TCP	Kaspersky Security Network への接続
80	TCP	接続は、*.digicert.com で Kaspersky Security Center 証明書の有効性を確認するために使用されます。 カスペルスキーのインフラストラクチャでは、このマスク内で任意の Web アドレスを使用できます。

下記の表に、ネットワークエージェントがインストールされているクライアントデバイスで開く必要のあるポートを示します。

クライアントデバイスで開く必要のあるポート

ポート番号	プロトコル	ポートの目的	範囲
15000	UDP	接続ゲートウェイ（使用している場合）からデータを受信する	クライアントデバイスの管理
15000	UDP ブロードキャスト	同じブロードキャストドメイン内の他のネットワークエージェントのデータを取得する	アップデートおよびインストールパッケージの提供
15001	UDP	ディストリビューションポイント（使用している場合）からマルチキャスト要求を受信する	ディストリビューションポイントからアップデートとインストールパッケージを受信する

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

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

下記の表に、ネットワークエージェントがディストリビューションポイントとしてインストールされているクライアントデバイスで開く必要のある追加のポートを示します。

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

ポート番号	プロトコル	ポートの目的	範囲
13000	TCP/TLS	ネットワークエージェントから接続を受信する	クライアントデバイスの管理、アップデートおよびインストールパッケージの提供。
13111（KSN プロキシサービスがデバイスで実行されている場合のみ）	TCP	管理対象デバイスから KSN プロキシサーバーへの要求を受信する	KSN プロキシサーバー
13295（ディストリビューションポイントをプッシュサーバーとして使用する場合のみ）	TCP/TLS	管理対象デバイスへのプッシュ通知の送信	プッシュサーバーとして使用しているディストリビューションポイント
15111（KSN プロキシサービスがデバイスで実行されている場合のみ）	UDP	管理対象デバイスから KSN プロキシサーバーへの要求を受信する	KSN プロキシサーバー
17111（KSN プロキシサービスがデバイスで実行されている場合のみ）	HTTPS	管理対象デバイスから KSN プロキシサーバーへの要求を受信する	KSN プロキシサーバー

ネットワークに管理サーバーが1台以上あり、プライマリ管理サーバーがカスペルスキーのインフラストラクチャ内に配置されている状態でセカンダリ管理サーバーとして使用する場合は、オンプレミスで実行されている Kaspersky Security Center で使用するポートのリストを参照してください。それらのポートを、セカンダリ管理サーバーとクライアントデバイスとの通信に使用します。

Kaspersky Security Center Cloud コンソールのインターフェイス

Kaspersky Security Center Cloud コンソールは Web インターフェイス経由で管理されます。

アプリケーションウィンドウには、次の項目が含まれます：

- ウィンドウ左側のメインメニュー
- ウィンドウ右側の作業領域

メインメニュー

メインメニューには次のセクションがあります：

- ［**機能紹介とチュートリアル**］：Kaspersky Security Center Cloud コンソールとセキュリティ製品の設定方法と使用方法に関するビデオが含まれています。

  Mozilla Firefox ブラウザーで、ポップアップウィンドウの［**機能紹介とチュートリアル**］セクションで動画を再生し、ピクチャーインピクチャーモードで動画を開き、ポップアップウィンドウで動画を閉じると、ピクチャーインピクチャーモードの動画も閉じられます。

- ［**管理サーバー**］：現在接続している管理サーバーの名前が表示されます。設定アイコン（）をクリックして、管理サーバーのプロパティを開きます。
- ［**監視とレポート**］：インフラストラクチャの状況、保護ステータス、統計情報を提供します。
- ［**アセット（デバイス）**］：クライアントデバイス、タスク、 カスペルスキー製品ポリシーを管理するためのツールが含まれています。
- ［**ユーザーとロール**］：ユーザーとロールを管理し、ユーザーにロールを割り当ててユーザー権限を構成し、ポリシープロファイルをロールに関連付けることができます。
- ［**操作**］：製品のライセンス管理、パッチの管理、サードパーティ製品の管理など、さまざまな操作が含まれます。これにより、アプリケーションリポジトリへのアクセスも可能になります。
- ［**検出と製品の導入**］：ネットワークをポーリングしてクライアントデバイスを検出し、デバイスを管理グループに手動または自動で配布できます。これには、クイックスタートウィザードと製品導入ウィザードも含まれています。
- ［**マーケットプレイス**］：カスペルスキーの法人向けソリューション全体に関する情報が含まれており、必要なソリューションを選択して、カスペルスキーの Web サイトでそれらのソリューションの購入に進むことができます。
- **設定**：Kaspersky Security Center Cloud コンソールを他のカスペルスキー製品と統合するための設定が含まれています。インターフェイスの言語またはテーマなど、インターフェイスの表示に関連する個人設定も含まれます。

- **アカウントメニュー**：オンラインヘルプへのリンクとカスペルスキーのテクニカルサポートに関する情報が含まれています。Kaspersky Security Center Cloud コンソールからログアウトもできます。

作業領域

作業領域には、アプリケーション Web インターフェイスウィンドウのセクションで表示を選択した情報が表示されます。また、情報の表示方法の構成に使用できるコントロール要素も含まれています。

Kaspersky Security Center Cloud コンソールの言語版

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

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

Kaspersky Security Center と Kaspersky Security Center Cloud コンソールの比較

Kaspersky Security Center を次の用途で使用できます：

- クラウドソリューションとしての使用

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

- オンプレミスソリューションとしての使用（Windows ベースまたは Linux ベース）

  Kaspersky Security Center をローカルデバイスにインストールし、ネットワークのセキュリティシステムを MMC ベースの管理コンソール、または Kaspersky Security Center Web コンソールで管理します。

  Windows ベースの製品に加え、Kaspersky Security Center Linux も利用できます。Kaspersky Security Center Linux は、Linux のみの環境における要件を満たすため、Linux ベースの管理サーバーを使用して、Linux デバイスの保護を導入および管理するように設計されています。Windows ベースの Kaspersky Security Center と Kaspersky Security Center Linux には異なる機能が搭載されています。

次の表で、Kaspersky Security Center と Kaspersky Security Center Cloud コンソールの主な機能を比較できます。

オンプレミスで実行される Kaspersky Security Center、およびクラウドソリューションとして実行される Kaspersky Security Center の機能の比較

機能またはプロパティ	Kaspersky Security Center 14（オンプレミスで実行）	Kaspersky Security Center Cloud コンソール
管理サーバーの位置	オンプレミス	クラウド
データベース管理システム（DBMS）の位置	オンプレミス	クラウド
Web ベースの管理コンソール	✓	✓
管理サーバーと DBMS のメンテナンス	顧客が管理	カスペルスキーが管理
管理サーバーの階層構造	✓	✓ （Kaspersky Security Center Cloud コンソールの管理サーバーは階層のプライマリ管理サーバーとしてのみ動作し、ポリシーとタスクの監視用にのみ使用できます）
管理グループの階層	✓	✓
管理対象デバイスと関連オブジェクトの、オンプレミスの Kaspersky Security Center から Kaspersky Security Center Cloud コンソールへの移行	✓	✓
ネットワークポーリング	✓	✓ （ディストリビューションポイントを使用してのみ）
管理対象デバイスの最大数	100000	25,000
Windows、Linux、macOS の管理対象デバイスの保護	✓	✓
モバイルデバイスの保護	✓	✓ （Kaspersky Endpoint Security for Android および Kaspersky Security for iOS のみがサポートされています）
パブリッククラウドインフラストラクチャの保護	✓	✓
デバイスベースのセキュリティ管理	✓	✓
製品ポリシー	✓	✓
カスペルスキー製品のタスク	✓	✓
Kaspersky Security Network	✓	✓
KSN プロキシサーバー	✓	✓ （ディストリビューションポイントでのみ）
Kaspersky Private Security Network	✓	–
カスペルスキー製品のライセンスの一元的な配信	✓	✓
別の管理サーバーへの管理対象デバイ	✓	–

スの切り替え		（別の管理サーバーに切り替えるには、管理対象デバイスのネットワークエージェントを再インストールする必要があります）
仮想管理サーバーのサポート	✓	✓
サードパーティ製ソフトウェアのアップデートのインストールと脆弱性の修正	✓	✓ （サードパーティ製品の脆弱性を修正するために、推奨の修正のみがインストール可能です）
管理対象デバイスで発生したイベントについての通知	✓	✓
ユーザーアカウントの作成と管理	✓	✓
データベース内のイベント数の上限	400,000 （最大 45,000,000 まで増やすことができます）	400,000 （管理対象デバイスの数に依存します）
SIEM システムとの統合	✓	✓ （Syslog 形式と TLS over TCP プロトコルの使用によってのみ）
WSUS サーバーとしての管理サーバーの使用	✓	–
ポリシーとタスクのステータスの監視	✓	✓
管理グループのクラスターとサーバーアレイのサポート	✓ （MMC ベースの管理コンソールのみ）	–
オペレーティングシステムのリモートインストール	✓	–
SNMP サポート	✓	–

基本概念

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

ネットワークエージェント

管理サーバーとデバイスとのインタラクションは、Kaspersky Security Center Cloud コンソールのコンポーネントの*ネットワークエージェント*によって行われます。ネットワークエージェントは、Kaspersky Security Center Cloud コンソールを使用してカスペルスキー製品を管理するすべてのデバイスにインストールする必要があります。

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

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

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

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

ネットワークエージェントによって管理対象デバイスと管理サーバーが同期します。管理サーバーと管理対象デバイスは、Kaspersky Security Center Cloud コンソールを数時間ごとに自動的に同期します。管理サーバーが設定する同期間隔（以降、「ハートビート」とも表記）は、管理対象デバイスの数に応じて異なります。

管理グループ

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

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

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

1台の管理対象デバイスが所属できる管理グループは1つだけです。

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

管理サーバーの階層構造

管理サーバーは、「プライマリ」と「セカンダリ」の階層に配置できます。各管理サーバーは、階層の複数のネストレベル上に複数のセカンダリ管理サーバーを保持できます。セカンダリ管理サーバーのネストレベルに制限はありません。プライマリ管理サーバーの管理グループには、すべてのセカンダリ管理サーバーのクライアントデバイスが含められます。

Kaspersky Security Center Cloud コンソール管理サーバーはプライマリ管理サーバーとしてのみ動作でき、セカンダリサーバーとして、オンプレミスで実行されているセカンダリ管理サーバーのみ保持できます。

オンプレミスで実行されている管理サーバーから Kaspersky Security Center Cloud コンソール管理サーバーへの移行時に、管理サーバーを階層に配置できます。その後、移行を緩和するため、管理対象デバイスを一部のみ Kaspersky Security Center Cloud コンソール管理サーバーの管理下に移動できます。その他の管理対象デバイスは、オンプレミスの管理サーバーの管理下に残ります。これにより、Kaspersky Security Center Cloud コンソールの管理機能を、限られた数の管理対象デバイスに対してテストできます。同時に、ネットワーク全体の管理と監視をテストするためのポリシー、タスク、レポート、その他のオブジェクトを設定できます。これにより、オンプレミスの管理サーバーで設定されているオブジェクトに、必要に応じて切り替えることができます。

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

仮想管理サーバー

仮想管理サーバー（*仮想サーバー*とも表記）は、クライアント組織のネットワークの保護を管理する、Kaspersky Security Center Cloud コンソールのコンポーネントです。各仮想管理サーバーの管理グループには独自の構造があり、ポリシー、タスク、レポート、イベントなど、独自の手段で管理と監視が行われます。ワークフローが複雑な組織は、仮想管理サーバーの機能範囲を利用できます。

仮想管理サーバーには次の制限があります：

- 仮想管理サーバーは、Kaspersky Security Center Cloud コンソールの製品モードでのみサポートされています。
- 仮想管理サーバーでは、セカンダリ管理サーバー（仮想サーバーを含む）の作成がサポートされていません。
- オンプレミスの Kaspersky Security Center から Kaspersky Security Center Cloud コンソールに仮想管理サーバーを移行することはできません。

- 専用の管理者が仮想管理サーバーを管理することはありません。既定で、プライマリ管理サーバーの管理者がすべての仮想管理サーバーも管理します。
- 仮想サーバー上で作成されたユーザーには、管理サーバー上のロールを割り当てることはできません。
- 仮想管理サーバーのプロパティウィンドウでは、セクション数が限られています。

ディストリビューションポイント

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

- アップデートおよびインストールパッケージをグループ内のクライアントデバイスに配信します（UDP を使用したマルチキャスト経由の配信を含む）。アップデートは、ディストリビューションポイント用に作成されたアップデートタスクを使用して、カスペルスキーのアップデートサーバーから受信可能です。

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

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

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

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

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

- 新しいデバイスを検出したり既存のデバイスの情報を更新するために、ネットワークを検索します。
- Microsoft Windows のツールを使用して、サードパーティのソフトウェアやカスペルスキー製品のリモートインストールを実行します。ネットワークエージェントを使用しないでクライアントデバイスにインストールすることもできます。

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

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

  > この機能は、Linux または macOS を実行するディストリビューションポイントデバイスでサポートされていません。

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

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

ネットワークエージェントがインストールされているデバイスには、管理グループに応じて手動でディストリビューションポイントを割り当てる必要があります。指定された管理グループのディストリビューションポイントの完全なリストは、ディストリビューションポイントのリストのレポートに表示されます。

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

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

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

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

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

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

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

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

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

Web 管理プラグイン

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

管理プラグインには次の機能があります：

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

ポリシー

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

ポリシーのステータス

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

ポリシーは、次のルールに従って機能します：

- 1つのアプリケーションに対して、異なる値を持つ複数のポリシーを定義することができます。
- 現在のアプリケーションに対してアクティブにできるポリシーは1つだけです。
- 特定のイベントが発生した時に、非アクティブポリシーを有効化できます。たとえば、ウイルスアウトブレイク中に、より厳格なアンチウイルスによる保護設定を適用することができます。

- ポリシーには子ポリシーを設定できます。

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

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

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

ポリシープロファイルは、次のルールに従って機能します：

- ポリシープロファイルは、特定の有効化条件下で有効になります。
- ポリシープロファイルには、ポリシー設定とは異なる設定値が含まれます。
- ポリシープロファイルを有効化すると、管理対象デバイスの有効な設定が変更されます。
- 1つのポリシーに最大100個のポリシープロファイルを含めることができます。

ポリシーのプロファイル

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

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

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

ローカルアプリケーション設定とポリシーの関連付け

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

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

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

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

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

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

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

- グループポリシー（設定の変更がロックされている場合）。

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

本製品のライセンス

このセクションでは、本製品のライセンスについて説明します。

Kaspersky Security Center Cloud コンソールのライセンス：シナリオ

このシナリオの手順に従って、ライセンスを使用して Kaspersky Security Center Cloud コンソールと管理対象セキュリティ製品の使用を開始できます。

Kaspersky Security Center Cloud コンソールでは、クライアントデバイスにカスペルスキー製品のライセンスを一元的に配信し、使用状況の監視およびライセンスの更新を実行できます。

Kaspersky Security Center Cloud コンソールを既に使用している場合は、マーケットプレイスにアクセスしてカスペルスキーのビジネスソリューション全体を確認し、必要なソリューションを選択して、カスペルスキーの Web サイトで購入プロセスに進むことができます。

ライセンスを購入する前に Kaspersky Security Center Cloud コンソールの機能を試用モードで試す

最初に Kaspersky Security Center Cloud コンソールを無料で試すことができます。無料で試すには、30 日間で終了する試用版のワークスペースを作成します。無期限で使用できる製品版のワークスペースが必要な場合は、ライセンスを購入する必要があります。

試用モードに続いて製品モードに切り替えることはできません。30 日の有効期間が終了すると、試用版のワークスペースはコンテンツ全体を含めてすべて自動的に削除されます。

実行するステップ

このシナリオは段階的に進行します：

1. **製品モードの Kaspersky Security Center Cloud コンソールにライセンスを付与するためのアクティベーションコードを取得する。ライセンスを購入する**

   異なるライセンスによって、カスペルスキーの異なる製品およびサービスが使用可能になるため、複数のライセンスを購入した方がよい場合があります。

   購入できるライセンスと、各ライセンスのデバイスの最小数を確認してください。

   Kaspersky Security Center Cloud コンソールは、複数のカスペルスキー製品の一部として提供されます。使用する製品を選択して、そのライセンスを購入してください。10,000 台以上のデバイスに対応するライセンスを購入する場合は、特別な要求としてカスペルスキーまたはカスペルスキーパートナーに問い合わせる必要があります。

   表を使用して、脆弱性とパッチ管理のどの機能が、どのライセンスで使用可能かを確認してください。

   Microsoft Azure などのクラウド環境で Kaspersky Security Center Cloud コンソールを使用する場合は、クラウド環境のライセンスオプションについてお読みください。

   マネージドサービスプロバイダー（MSP）である場合は、「MSP 向けの Kaspersky Security Center Cloud コンソールのライセンスについて」をお読みください。

2. **ワークスペースの作成時に Kaspersky Security Center Cloud コンソールをアクティベートする**

Kaspersky Security Center Cloud コンソールをアクティベートするには、ワークスペースの作成時にライセンスを指定します。

ライセンスが複数ある場合は、そのいずれかを指定します。その後、管理対象カスペルスキー製品をアクティベートするため、Kaspersky Security Center Cloud コンソールで他のライセンスを追加する必要があります。

3 管理サーバーリポジトリに管理対象アプリケーションのライセンスを追加する

ライセンスを配信する前に、これらのライセンスを管理サーバーリポジトリに追加する必要があります。

ワークスペースの作成時に指定したライセンスは、自動的に管理サーバーリポジトリに追加されます。

複数のライセンスがある場合は、Kaspersky Security Center Cloud コンソールの管理サーバーリポジトリに1つずつライセンスを追加します。

4 管理対象アプリケーションにライセンスを配信する

保護するすべてのデバイスにライセンスを配信する方法を選択します：

- 自動配信

  異なる複数の管理対象アプリケーションを使用し、特定のアクティベーションコードをアプリケーションに配信する必要がある場合は、他の配信方法を選択してください。

  Kaspersky Security Center を使用して、使用可能なライセンスを管理対象アプリケーションに自動配信できます。ここでは、3個のライセンスが管理サーバーのリポジトリに保管されている場合を例にします。［**管理対象デバイスにライセンスを自動配信する**］を3個のライセンスすべてに対してオンにしていると仮定します。カスペルスキーのセキュリティ製品（例：Kaspersky Endpoint Security for Windows）が、組織内のデバイスにインストールされているとします。デバイスで、ライセンスを配信する必要がある新しい管理対象アプリケーションが検出されます。たとえば、リポジトリ内に保管されている、名前がそれぞれ「*Key_1*」「*Key_2*」である2個のライセンス情報ファイルを、そのデバイスの管理対象アプリケーションに配信できます。そのうち1個のライセンス情報ファイルが、管理対象アプリケーションに配信されます。この場合、どのライセンス情報ファイルが配信されるかは予測できません。自動配信されるライセンスに対して、管理者が設定可能な項目がないからです。

  ライセンスが配信されると、そのライセンスに対してインストール数が再度計上されます。ライセンスを適用可能な製品数を超えないように、適用中の製品数を確認しておく必要があります。ライセンスを適用可能なインストール数の上限を超えると、ライセンスが適用されていないすべてのデバイスのステータスが「*緊急*」になります。

  実行手順の説明：

  - ライセンスの管理サーバーリポジトリへの追加
  - ライセンスの自動配信

- 管理対象アプリケーションへのライセンスの追加タスクを使用して配信

  管理対象アプリケーションへのライセンスの追加タスクを使用する場合、配信する必要があるライセンスを選択後、対象デバイスを都合のよい方法で選択できます。たとえば、管理グループを選択したり、デバイスの抽出を使用したりすることが可能です。

  実行手順の説明：

  - ライセンスの管理サーバーリポジトリへの追加
  - ライセンスのクライアントデバイスへの配信

- アクティベーションコードまたはライセンス情報ファイルを手動でデバイスに追加

インストール済みのカスペルスキー製品を、製品インターフェイス内のツールを使用してローカルでアクティベーションできます。詳しくは、インストールされているアプリケーションのヘルプを参照してください。

5. **管理対象カスペルスキー製品がどのデバイスでアクティベートされているかを確認する**

   ライセンスが正しく配信されたことを確認するには、製品で使用されているライセンスのリストを表示します。

6. **ライセンスの有効期限に関連するイベントを設定する**

   イベントを設定して、ライセンスがすべて使用されたか、有効期限が近い場合に通知されるようにします：

   - 管理サーバーの緊急イベント
   - 管理サーバーの機能エラーイベント
   - 管理サーバーの警告イベント
   - 管理サーバーの情報イベント

Kaspersky Security Center Cloud コンソールの試用モードについて

*試用モード*は、ユーザーが Kaspersky Security Center Cloud コンソールの機能を確認するための、Kaspersky Security Center Cloud コンソールの特別なモードです。このモードでは、有効期間が 30 日に限定されているワークスペースで操作を実行できます。試用モードは、試用版のワークスペースを作成すると自動的にアクティベートされます。試用モードで利用できる一連の機能は、標準の Kaspersky Endpoint Security for Business Advanced ライセンスの範囲の機能と同じです。

Kaspersky Security Center Cloud コンソールでは、特別なライセンスが必要な機能がサポートされていないため、管理サーバーにライセンスを付与する必要がありません。Kaspersky Security Center Cloud コンソールを試用モードで利用する場合、1つ目のワークスペースを作成すると試用版ライセンスが自動的に付与されます。

試用モードに続いて製品モードに切り替えることはできません。30 日の有効期間が終了すると、試用版のワークスペースはコンテンツ全体を含めてすべて自動的に削除されます。

Kaspersky Security Center Cloud コンソールの機能を試用モードで利用する際は、次の制限が適用されます。

- 管理サーバーの階層は作成できません。仮想管理サーバーは作成できません。
- ［**ライセンス**］セクションは読み取り専用で使用できます。このセクションでは、ライセンスの追加と削除を含むすべての操作が禁止されます。
- カスタムインストールパッケージは作成できません。
- ユーザーにカスタムロールは作成できません。
- ［ウイルスアウトブレイク］機能は利用できません。［ウイルスアウトブレイク］イベントは保存されず、通知は送信されません。
- ［**削除されたオブジェクト**］リポジトリは利用できません。
- データベースへのバッチイベント（大量に発生したイベント）の追加は有効にできません。

- オンプレミスモードからクラウドコンソールモードへの管理サーバーの移行はサポートされていません。
- 管理サーバーやネットワークエージェントなど、管理サーバーのコンポーネントからの KSN の統計情報は、カスペルスキーに送信されません。

いくつかの制限は、製品の一部のオブジェクトの作成にも適用されます（次の表を参照）。このようなオブジェクトの作成を試行して、これらのいずれかの制限に違反した場合は、オブジェクトの作成がブロックされて制限に関するエラーメッセージが表示されます。

試用モードの Kaspersky Security Center Cloud コンソールオブジェクトの作成における制限

制限の種別	値
ポリシー	8
タスク	17
ライセンス	1
インストールパッケージ	5
デバイスの抽出（設定済みのインスタンスは含まず）	5
イベントの抽出（設定済みのインスタンスは含まず）	5
デバイス移動ルール	3
同じ種別のレポートテンプレート	10
内部セキュリティグループ	20
管理対象デバイス	20

マーケットプレイスを使用してカスペルスキーの法人向けソリューションを選択する

［**マーケットプレイス**］はカスペルスキーのビジネスソリューションを全体的に表示できるメインメニューのセクションです。必要なものを選択してカスペルスキーの Web サイトに移動して購入プロセスに進むことができます。フィルターを使用してお客様の組織や情報セキュリティシステムの要件に一致するソリューションのみを表示することが可能です。ソリューションを選択すると、Kaspersky Security Center Cloud コンソールにより、そのソリューションの詳細について確認できるカスペルスキーの Web ページにリダイレクトされます。各 Web ページで、製品の購入に進んだり、購入に関する手順を確認したりできます。

［**マーケットプレイス**］セクションでは、次の条件を使用してカスペルスキー製品をフィルターすることができます：

- 保護対象のデバイスの数（エンドポイント、サーバー、その他の種別の資産）：
  - 50～250
  - 250～1000
  - 1000 以上
- 組織の情報セキュリティチームの成熟度：
  - **基本のセキュリティ**

このレベルは IT チームを 1 つのみ持つ企業に典型的なレベルです。脅威は、自動的に可能な最大数ブロックされます。

- **最適なセキュリティ**

  このレベルは IT チーム内に IT セキュリティ機能を持つ特定の IT チームを持つ企業に典型的なレベルです。このレベルでは、企業はコモディティ型の脅威や既存の防御メカニズムを回避する脅威などに対応するソリューションを必要とします。

- **高度なセキュリティ**

  このレベルは複雑で分散化された IT 環境を持つ機能に典型的なレベルです。IT セキュリティチームの熟練度が高い、または企業が SOC（セキュリティオペレーションセンター）チームを持っているなどのレベルです。必要とされるソリューションは、複雑な脅威および標的型攻撃に対応するものです。

- 保護対象の資産の種別：
  - **エンドポイント**：物理および仮想マシン、埋め込みシステムなどの社員のワークステーション
  - **サーバー**：物理および仮想サーバー
  - **クラウド**：パブリック、プライベート、またはハイブリッドのクラウド環境およびクラウドサービス
  - **ネットワーク**：ローカルエリアネットワーク、IT インフラストラクチャ
  - **サービス**：カスペルスキーによって提供されるセキュリティ関連のサービス

カスペルスキーのビジネスソリューションを検索および購入するには：

1. メインメニューで、［**マーケットプレイス**］に移動します。

   既定では、セクションにはすべての使用可能なカスペルスキーのビジネスソリューションが表示されています。

2. 企業に合ったソリューションのみを表示するには、フィルターで必要な値を選択します。

3. 購入する、もしくは詳細を確認したいソリューションをクリックします。

   ソリューションの Web ページにリダイレクトされます。画面上の説明に従って、購入プロセスを進められます。

各ライセンスのライセンス数とデバイスの最小数

Kaspersky Security Center Cloud コンソールを製品モードで利用する場合、1 つ目のワークスペースを作成する前にライセンスを購入する必要があります。次の表に、購入できるライセンスと、各ライセンスのデバイスの最小数（保護するデバイス数がこれより少ない場合も該当）を示します：

Kaspersky Security Center Cloud コンソールを使用可能にするライセンス

ライセンス	デバイスの最小数（保護するデバイス数がこれより少ない場合も該当）
Kaspersky Endpoint Security for Business Select	製品版ライセンスの場合：300 製品版（定額制）ライセンスの場合：100
Kaspersky Endpoint Security for Business Advanced	製品版ライセンスの場合：300 製品版（定額制）ライセンスの場合：100

Kaspersky Total Security for Business	300
Kaspersky Endpoint Detection and Response Optimum	製品版ライセンスの場合：300 製品版（定額制）ライセンスの場合：100
Kaspersky Endpoint Detection and Response Expert	50
Kaspersky Hybrid Cloud Security、デスクトップ	製品版ライセンスの場合：300 製品版（定額制）ライセンスの場合：100
Kaspersky Hybrid Cloud Security、サーバー	50
Kaspersky Hybrid Cloud Security、コア	20
Kaspersky Hybrid Cloud Security、CPU	20
Kaspersky Hybrid Cloud Security Enterprise、デスクトップ	製品版ライセンスの場合：300 製品版（定額制）ライセンスの場合：100
Kaspersky Hybrid Cloud Security Enterprise、サーバー	50
Kaspersky Hybrid Cloud Security Enterprise、CPU	20
Kaspersky Embedded Systems Security	300
Kaspersky Embedded Systems Security Compliance Edition	300
Kaspersky Symphony（現在はロシアでのみ使用可能）	300
Kaspersky Next EDR Foundations	300 ユーザー（各ユーザーライセンスは 1 台の PC/Mac デバイスと 2 台のモバイルデバイスに適用可能）
Kaspersky Next EDR Optimum	300 ユーザー (各ユーザー ライセンスは 1 台の PC/Mac デバイスと 2 台のモバイル デバイスに適用可能)
Kaspersky Next XDR Expert	250 ユーザー（各ユーザーライセンスは 1 台の PC/Mac デバイスと 2 台のモバイルデバイスに適用可能）

ワークスペースあたりのデバイス数の上限は 25,000 台です。10,000 台を超えるデバイスを保護する場合は、別のワークスペースを作成する必要があります。これを行うには、 カスペルスキーテクニカルサポートに問い合わせます。問い合わせの際は、次の情報を記載する必要があります。

- **ユーザーのメールアドレス**— Kaspersky Security Center Cloud コンソールに登録されたユーザーのメールアドレス。このユーザーには、作成されたワークスペースで管理者権限が付与されます。

  Kaspersky Security Center Cloud コンソールでアカウントを作成した後で、会社を登録してワークスペースを作成する必要はありません。問い合わせには、会社とワークスペースに関する情報を指定します。

- **会社名**— Kaspersky Security Center Cloud コンソールを使用する会社の名前。
- **会社の国**— その会社が所在する国。
- **ワークスペース名**— 会社用に作成されるワークスペースの名前。

- **推定エンドポイント数**– 新しいワークスペースで保護するクライアント デバイスの総数（モバイル デバイスを含む）。

- **ワークスペースの国** – 新しいワークスペースを配置する国。このパラメータは、ワークスペースを格納するデータセンターの選択に影響します。

  米国またはカナダにワークスペースを配置する場合は、州または郡を指定してデータセンターのリージョンを決定してください。

  会社の国と**ワークスペースの国**のパラメータは同じである場合があります。

- **アクティベーションコード**– Kaspersky Security Center Cloud コンソールの購入後に受け取るアクティベーションコード。購入するライセンスが、保護する必要があるすべてのクライアントデバイスに適用されることを確認してください。

問い合わせを送信すると、カスペルスキーの担当者が指定された会社を登録し、その会社のワークスペースを作成します。ワークスペースの作成が完了すると、メールで通知が届きます。Kaspersky Security Center Cloud コンソールでアカウントにログインして、結果を確認できます。

ライセンス制限超過のイベント

Kaspersky Security Center Cloud コンソールには、クライアントデバイスにインストールされたカスペルスキー製品がライセンスによる制限を超過した時のイベントに関する情報が表示されます。

ライセンスの制限を超過した時のイベントの重要度は、次のルールに従って決定されます：

- 単一のライセンスが現在適用されている台数が、そのライセンスが対応している合計台数の 90 ～ 100% である場合、重要度が「**情報**」のイベントが発生します。

- 単一のライセンスが現在適用されている台数が、そのライセンスが対応している合計台数の 100 ～ 110% である場合、重要度が「**警告**」のイベントが発生します。

- If the number of currently used units covered by a single license exceeds 110% of the total number of units covered by the license, the event is published with the **Critical event** importance level.

管理対象デバイスへのアクティベーションコードの配信方法

管理対象デバイスにインストールされているカスペルスキー製品には、各製品のアクティベーションコードを適用してライセンスを付与する必要があります。管理対象アプリケーションへのライセンス付与にライセンス情報ファイルは使用できません。アクティベーションコードのみ使用できます。アクティベーションコードは次の方法で配信できます：

- 自動配信

- 管理対象アプリケーションへのライセンスの追加タスク

- 管理対象アプリケーションの手動アクティベーション

カスペルスキー製品は同時に 1 つ以上のライセンスを使用することがあります。たとえば、Kaspersky Endpoint Security for Windows は 2 つのライセンスを使用することがあります。1 つは Kaspersky Endpoint Security for Windows 用で、もう 1 つは Endpoint Detection and Response 機能のアクティベーション用です。

さらに、カスペルスキー製品には現在のライセンスに加えて予備のライセンスを設定することができます。カスペルスキー製品は、現時点で現在のライセンスを使用し、現在のライセンスの有効期限が切れた後に適用する予備のライセンスを保存します。上記のいずれかの方法で、新しい現在のライセンスまたは予備のライセンスを追加できます。ライセンスを追加するアプリケーションは、ライセンスが現在のライセンスか予備のライセンスかを定義します。ライセンスの定義は、新しいライセンスの追加方法には依存しません。

ライセンスの管理サーバーリポジトリへの追加

Kaspersky Security Center Cloud コンソールでライセンスを追加すると、ライセンスの設定が管理サーバーで保存されます。アプリケーションでは、この情報に基づいて、ライセンス使用レポートを生成し、ライセンスの有効期限と、ライセンスのプロパティで設定されるライセンスの制限事項の違反について管理者に通知します。ライセンス使用の通知の設定は管理サーバーで設定できます。

ライセンスを管理サーバーリポジトリに追加するには：

1. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。
2. ［**追加**］をクリックします。
3. テキストフィールドにアクティベーションコードを入力し、［**送信**］をクリックします。
4. ［**閉じる**］をクリックします。

管理サーバーのリポジトリにライセンスが追加されます。

ライセンスのクライアントデバイスへの配信

Kaspersky Security Center Cloud コンソールでは、ライセンスをクライアントデバイスに自動的に配信、またはライセンスの追加タスクから配信できます。

配信前に、ライセンスを管理サーバーリポジトリに追加します。

［ライセンスの追加］タスクを通じてクライアントデバイスにライセンスを配信するには、次の手順を実行します：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. ［**アプリケーション**］ドロップダウンリストで、ライセンスを追加する製品を選択します。
4. ［**タスク種別**］リストから、［**ライセンスの追加**］タスクを選択します。
5. ［**タスク名**］フィールドに、新しいタスクの名前を指定します。
6. タスクを割り当てるデバイスを選択します。

7. ウィザードの［**ライセンス情報ファイルの選択**］手順で、［**ライセンスの追加**］リンクをクリックしてライセンスを追加します。

8. ［ライセンスの追加］ペインで、次のいずれかのオプションを使用してライセンスを追加します：

   ライセンスを追加する必要があるのは、［ライセンスの追加］タスクを作成する前にライセンスを管理サーバーのリポジトリに追加しなかった場合のみです。

   - ［**アクティベーションコードの入力**］オプションを選択してアクティベーションコードを入力し、次の手順を実行します：

     a. アクティベーションコードを指定して［**送信**］ボタンをクリックしてください。

     ライセンスに関する情報が［ライセンスの追加］ペインに表示されます。

     b. ［**保存**］をクリックします。

     管理対象デバイスにライセンスを自動的に配信する場合は、［**管理対象デバイスにライセンスを自動配信する**］オプションを有効にします。

     ［ライセンスの追加］ペインが閉じます。

   - ［**ライセンス情報ファイルの追加**］オプションを選択してライセンスファイルを追加し、次の操作を実行します：

     a. ［**ライセンス情報ファイルの選択**］ボタンをクリックします。

     b. ［ライセンス情報ファイルの選択］ウィンドウが開いたら、ライセンス情報ファイルを選択し、［**開く**］をクリックします。

     ライセンスに関する情報が［ライセンスの追加］ペインに表示されます。

     c. ［**保存**］をクリックします。

     管理対象デバイスにライセンスを自動的に配信する場合は、［**管理対象デバイスにライセンスを自動配信する**］オプションを有効にします。

     ［ライセンスの追加］ペインが閉じます。

9. ライセンスのテーブルで［ライセンス］を選択します。

10. このライセンスを予備のライセンスとして使用する場合は、ウィザードの［**ライセンス情報**］手順で、［**予備のライセンスとして使用する**］オプションを有効にします。

    この場合、予備ライセンスの有効期限が切れた後に現在のライセンスが適用されます。

11. ウィザードの［**タスク作成の終了**］ステップで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。

    このオプションをオンにしない場合、タスクは既定の設定で作成されます。既定の設定からの変更は、後からいつでも実行できます。

12. ［**終了**］をクリックします。

ウィザードではタスクを作成します。［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスクのプロパティウィンドウが自動的に表示されます。このウィンドウでは、［一般的なタスク設定］を指定し、必要に応じてタスク作成時に指定した設定を変更できます。

タスクのリストで作成されたタスクの名前をクリックして、タスクのプロパティウィンドウを開くこともできます。

タスクが作成、設定され、タスクリストに表示されます。

13. タスクを実行するには、タスクリストで目的のタスクを選択し、［**開始**］をクリックします。
    タスクのプロパティウィンドウの［**スケジュール**］タブでタスクの開始スケジュールを設定することもできます。
    スケジュール開始設定の詳細については、「タスクの一般設定」を参照してください。

タスクが完了すると、選択したデバイスにライセンスが導入されます。

ライセンスの自動配信

Kaspersky Security Center Cloud コンソールでは、管理サーバーのライセンスリポジトリにあるライセンスを管理対象デバイスに自動配信できます。

管理対象デバイスにライセンスを自動配信するには：

1. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。
2. デバイスに自動配信するライセンスをクリックします。
3. 表示されるライセンスのプロパティウィンドウで、スイッチを［**管理対象デバイスにライセンスを自動配信する**］に切り替えます。
4. ［**保存**］をクリックします。

ライセンスは、互換性のあるすべてのデバイスに自動的に配信されます。

ライセンスはネットワークエージェント経由で配信されます。アプリケーションに対するライセンスの配信タスクは作成されません。

ライセンスが自動配信される際、デバイス数へのライセンスの制限が適用されます。ライセンスの制限は、ライセンスのプロパティで設定済みです。ライセンス数の上限に達した場合は、デバイスへの配信は自動的に停止します。

管理対象デバイスのアプリケーションをアクティベートするため、定額制サービスのライセンスに［**管理対象デバイスにライセンスを自動配信する**］を指定している場合で、同時にアクティブな試用版ライセンスを持っている場合、試用版のライセンスは有効期限の 8 日前に自動的に定額制サービスのライセンスに置換されます。

管理サーバーのリポジトリでの使用中のライセンスに関する情報の表示

管理サーバーのリポジトリに追加されているライセンスのリストを表示するには：

メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。

管理サーバーのリポジトリに追加されているアクティベーションコードのリストが表示されます。

ライセンスの詳細情報を表示するには：

1. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。
2. 目的のライセンスの名前をクリックします。

ライセンスのプロパティウィンドウが表示され、次の情報を確認できます：

- ［**全般**］タブ：ライセンスに関する主要な情報
- ［**デバイス**］タブ：このライセンスが、インストールされているカスペルスキー製品のアクティベーションに使用されたクライアントデバイスのリスト

特定のカスペルスキー製品で使用中のライセンスに関する情報の表示

カスペルスキー製品で使用されているライセンスを確認するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   デバイスが未割り当てデバイスグループに属している場合は、代わりに［**検出と製品の導入**］→［**未割り当てデバイス**］の順に選択します。
2. 目的のデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**アプリケーション**］セクションを選択します。
4. 表示された製品のリストで、ライセンスキーを表示する製品を選択します。
5. 製品のプロパティウィンドウが表示されるので、［**全般**］タブの［**ライセンス**］セクションに移動します。
   このセクションの作業領域に情報が表示されます。

リポジトリからのライセンスの削除

管理サーバーのリポジトリからライセンスを削除できます。次の場合、Kaspersky Security Center Cloud コンソールは 90 日後にワークスペースを自動的に削除します：

- リポジトリに手動で追加された最後のライセンス（現在のライセンス、予備のライセンス、または使用されていないライセンス）を削除した。
- 最後のライセンスの有効期限が切れた。

ワークスペースが削除されると、Kaspersky Security Center Cloud コンソールを使用してネットワークの保護を管理できなくなります。また、Kaspersky Security Center Cloud コンソールからのデータも完全に失われます。必要に応じて、ワークスペースを手動で削除できます。削除しない場合は、管理サーバーのリポジトリに少なくとも1つライセンスを保持することを推奨します。

事前に予備のライセンスを追加した状態でライセンスを削除した場合、現在のライセンスが削除されるか期限が切れた後に予備のライセンスが自動的に現在のライセンスになります。

管理対象デバイスに追加済みの現在のライセンスを管理サーバーのリポジトリから削除した場合、管理対象デバイスにインストールされている製品は動作を継続します。

ライセンスを管理サーバーリポジトリから削除するには：

1. 削除するライセンスが管理サーバーで使用されていないことを確認します。管理サーバーで使用されている場合、ライセンスを削除することはできません。チェックを実行するには：

   a. メインメニューで、管理サーバーの横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

   b. ［**全般**］タブで、［**ライセンス**］セクションを選択します。

   c. 開いたセクションに必要なライセンスが表示されている場合は、［**現在のライセンスの削除**］をクリックし、処理内容を確定します。その後、削除されたライセンスが管理サーバーで使用されることはありませんが、ライセンスは管理サーバーのリポジトリに残ります。必要なライセンスが表示されない場合、管理サーバーはこのライセンスを使用していません。

2. メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。

3. 必要なライセンスを選択し、［**削除**］をクリックします。

4. 表示されるウィンドウで、［**リスクを理解した上でライセンスを削除する**］チェックボックスをオンにします。これは、最後のライセンスを削除すると、ワークスペースが削除され、管理対象デバイスを制御できなくなることを認識していることを意味します。次に、［**削除**］をクリックします。

その結果、選択したライセンスがリポジトリから削除されます。

削除されたライセンスを再び追加したり、新しいライセンスを追加することもできます。最後のライセンスを削除した場合、ワークスペースが削除されていない限り、ライセンスを追加することもできます。Kaspersky Security Center Cloud コンソールは、削除の 30 日前、7 日前、および1日前にワークスペースの管理者に通知します。

カスペルスキー製品がアクティベートされていないデバイスのリストの表示

カスペルスキー製品がインストールされているが、アクティベートされていない（ライセンスがないか、有効期間が終了した場合など）すべてのデバイスのリストを表示できます。

カスペルスキー製品がアクティベートされていないデバイスを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。

   タスクのリストが表示されます。

2. 該当するカスペルスキー製品に関連するアップデートタスクの名前をクリックします。
   タスクのプロパティウィンドウにいくつかの名前付きタブが表示されます。

3. タスクのプロパティウィンドウで［**履歴**］セクションを選択します。
   ［**デバイス**］列に、タスクが成功したデバイスが表示されます。

4. ［**デバイス**］列を並べ替えます。
   ［**デバイス**］列に、タスクが成功したデバイスが表示されます。ライセンスがないためタスクが失敗したデバイスでは、製品がアクティベートされていません。

使用許諾契約書による同意の取り消し

一部のクライアントデバイスの保護を停止する場合、任意の管理対象カスペルスキー製品の使用許諾契約書（EULA）への同意を取り消すことができます。EULA への同意を取り消す前に、選択した製品とそのインストールパッケージをアンインストールする必要があります。インストールパッケージは、管理サーバーとその仮想管理サーバーから削除する必要があります。

仮想管理サーバー上での EULA への同意は、仮想管理サーバーまたはプライマリ管理サーバーで取り消すことができます。プライマリ管理サーバー上での EULA への同意は、プライマリ管理サーバー上でしか取り消すことはできません。

管理対象のカスペルスキー製品の EULA を取り消すには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. 管理サーバーのプロパティウィンドウの［**全般**］タブで、［**使用許諾契約書**］セクションを選択します。
   インストールパッケージの作成時、またはアップデートのシームレスインストール時に同意した EULA のリストが表示されます。

3. リストから、同意を取り消す EULA を選択します。
   EULA の以下のプロパティを確認できます：

   - EULA に同意した日付
   - EULA に同意したユーザーの名前
   - EULA への同意を取り消すことができるかどうか

4. EULA に同意した日付のうち任意のものをクリックし、次のデータが表示されるプロパティウィンドウを開きます：

   - EULA に同意したユーザーの名前
   - EULA に同意した日付
   - EULA の一意な識別子（UID）
   - EULA のテキスト

- EULA に関連するオブジェクト、および各オブジェクトの名前と種別のリスト（インストールパッケージ、シームレスアップデート）

5. EULA のプロパティウィンドウの下部で、［**使用許諾契約書への同意を取り消す**］をクリックします。

   製品をアンインストールしないと選択した EULA への同意を取り消すことができない、またはプライマリ管理サーバーでしかこの EULA への同意を取り消すことができない場合は、［**使用許諾契約書への同意を取り消す**］の代わりにこの制限についての通知が表示されます。

   EULA への同意の取り消しを妨げるオブジェクト（インストールパッケージ、およびそのパッケージを使用するタスク）が存在する場合、そのオブジェクトに関する通知が表示されます。これらのオブジェクトを削除するまで、取り消しの動作を続行できません。

   表示されたウィンドウで、この EULA に対応するカスペルスキー製品を最初にアンインストールすることが必要であることが示されます。

6. ボタンをクリックして取り消しを確定します。

これで EULA が取り消されました。［**使用許諾契約書** ］セクションの使用許諾契約書のリストに表示されなくなります。EULA のプロパティウィンドウが閉じ、製品がインストールされなくなります。

カスペルスキー製品のライセンスの更新

有効期間の終了した、または有効期間がまもなく終了する（残り 30 日以内）のカスペルスキー製品のライセンスを更新できます。

最後のライセンスの有効期限が切れている場合、Kaspersky Security Center Cloud コンソールは 90 日後にワークスペースを自動的に削除します。その結果、Kaspersky Security Center Cloud コンソールを使用してネットワークの保護を管理することはできなくなります。また、Kaspersky Security Center Cloud コンソールからのデータも完全に失われます。ワークスペースを保持するために、古いライセンスを更新するか、管理サーバーのリポジトリに新しいライセンスを追加することを推奨します。

有効期間が終了した、または有効期間がまもなく終了するライセンスについての通知を表示するには：

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**操作**］→［**ライセンス管理**］→［**カスペルスキーのライセンス**］の順に選択します。
   - ［**監視とレポート**］→［**ダッシュボード**］の順に移動し、通知の横にある［**有効期間がまもなく終了するライセンスを表示**］をクリックします。

   ［**カスペルスキーのライセンス** ］ウィンドウが表示され、有効期間がまもなく終了する、または有効期間が終了したライセンスを表示および更新できます。

2. ライセンスを更新する場合は、必要なライセンスに隣接する［**ライセンスの更新**］をクリックします。

ライセンスの更新リンクをクリックすることで、お客様はカスペルスキーにソフトウェアの識別子、バージョン、言語版、ライセンス識別子、および販売代理店経由でライセンスが提供されたかどうかを示す属性のデータを送信することに同意したものとします。これらのデータは、ライセンスの有効期間の決定に必要です。

3. 表示されるライセンス更新サービスのウィンドウで、ライセンスを更新する手順に従ってください。
   有効期間がまもなく終了するライセンスが更新されます。

Kaspersky Security Center Cloud コンソールでは、ライセンスの有効期間の終了間近になると次のスケジュールで通知が表示されます：

- 有効期限の 30 日前
- 有効期限の 7 日前
- 有効期限の 3 日前
- 有効期限の 24 時間前
- ライセンスの有効期間が終了した時

ライセンスの有効期限後の Kaspersky Security Center Cloud コンソールの使用

ライセンスの有効期限後、Kaspersky Security Center Cloud コンソールを、最長 90 日間制限なしで使用できる権限がカスペルスキーによって付与される場合があります。この期間中、管理サーバー、ネットワークエージェント、Kaspersky Security Center Cloud コンソールの Web インターフェイスは制限なく動作します。また、Kaspersky Security Center Cloud コンソールは、現在の KSN アクセス設定に従って KSN 統計をカスペルスキーに送信します。管理対象アプリケーションは機能が制限されて動作します（詳細については、これらの製品のガイドを参照してください）。

ライセンスが 90 日間期限切れになると、Kaspersky Security Center Cloud コンソールはワークスペースを自動的に削除します。ワークスペースを保持したい場合は、有効期限が切れたライセンスを 1 つ以上更新するか、リポジトリに新しいライセンスを追加してください。

Kaspersky Security Network（KSN）

このセクションでは、Kaspersky Security Network（KSN）というオンラインサービスのインフラストラクチャの使用方法を説明します。KSN の詳細、および KSN を有効にする方法、KSN へのアクセスの設定方法、KSN プロキシサーバーの使用の統計を表示する方法を説明します。

KSN について

Kaspersky Security Network（KSN）は、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのナレッジベースへのオンラインアクセスを提供するオンラインサービスの基盤です。Kaspersky Security Network のデータを使用することにより、脅威に対するカスペルスキー製品の対応が迅速化され、一部の保護コンポーネントの効果が高まり、誤検知のリスクが低減されます。KSN によって、カスペルスキーの評価データベースを使用して、クライアントデバイスにインストールされたアプリケーションの情報を取得できます。

KSN に参加すると、Kaspersky Security Center Cloud コンソールによって管理されるクライアントデバイス上にインストールされたカスペルスキー製品の動作に関する情報を、自動的にカスペルスキーに送信することに同意したことになります。情報は、現在の KSN アクセス設定に従って転送されます。カスペルスキーのアナリストは、受け取った情報をさらに分析し、Kaspersky Security Network の評価および統計データベースに追加します。

クイックスタートウィザードの実行時には、KSN に参加するよう促されます。アプリケーションの使用時であればいつでも、KSN の使用を開始または停止できます。

お客様は KSN を有効にする際に同意した KSN に関する声明に従って KSN を使用するものとします。KSN に関する声明が更新された場合は、管理サーバーをアップデートまたはアップグレードする際に更新された声明が表示されます。更新された KSN に関する声明に同意することも拒否することも可能です。拒否した場合は、以前に同意した KSN 声明の以前のバージョンの内容に従って KSN の使用が継続されます。

KSN が有効になっている場合、Kaspersky Security Center Cloud コンソールは KSN サーバーがアクセス可能であるかどうかを確認します。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。これは、管理対象デバイスのセキュリティレベルを確実に管理するために必要です。

管理サーバーが管理するクライアントデバイスは、KSN プロキシサーバーを使用して KSN と対話します。KSN プロキシサーバーは次の機能を提供します：

- クライアントデバイスは、インターネットに直接アクセスできない場合でも、KSN に要求を送信し、情報を転送できます。
- KSN プロキシサーバーでは処理データをキャッシュに保存するため、送信チャネルの負荷が軽減され、クライアントデバイスから要求された情報を待つ時間が短縮されます。

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

KSN の有効化および無効化

KSN を有効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**KSN 設定**］セクションを選択します。
3. スイッチを［**Kaspersky Security Network の使用が［有効］です**］の位置まで移動します。
   KSN が有効です。
   この切り替えスイッチが有効になっていると、クライアントデバイスがパッチのインストール結果をカスペルスキーに送信します。このスイッチを有効にする際には、KSN 声明の条項を読み、それに同意する必要があります。
4. ［**保存**］をクリックします。

KSN を無効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**KSN 設定**］セクションを選択します。
3. スイッチを［**Kaspersky Security Network の使用が［無効］です**］の位置まで移動します。
   KSN が無効です。
   この切り替えスイッチが無効の位置にあると、クライアントデバイスはパッチのインストール結果をカスペルスキーに送信しません。
4. ［**保存**］をクリックします。

同意した KSN に関する声明の表示

Kaspersky Security Network (KSN) を有効にする際には、KSN に関する声明を読み、同意する必要があります。同意した KSN に関する声明はいつでも表示できます。

同意した KSN に関する声明を表示するには：

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**KSN 設定**］セクションを選択します。
3. ［**Kaspersky Security Network に関する声明を表示**］をクリックします。

表示されたウィンドウで、同意した KSN に関する声明の内容を表示できます。

更新された KSN に関する声明の同意

お客様は KSN を有効にする際に同意した KSN に関する声明に従って KSN を使用するものとします。KSN 声明が更新された場合、Kaspersky Security Center Cloud コンソールを開いた時に自動的に表示されます。更新された KSN に関する声明に同意することも拒否することも可能です。拒否した場合は、以前に同意した KSN 声明の以前のバージョンの内容に従って KSN の使用が継続されます。更新された KSN 声明は後から表示、同意することができます。

更新された KSN 声明を表示して同意するには：

1. 製品のメインウィンドウの右上部にある[**通知の表示**]をクリックします。
   ［**通知**］ウィンドウが開きます。
2. ［**更新された KSN 声明を表示**］をクリックします。
   ［**Kaspersky Security Network に関する声明の更新**］ウィンドウが開きます。
3. KSN に関する声明を読み、次のうち 1 つを選択して対応を判断します：

   - **更新された KSN 声明の内容に同意する**

- **更新前の声明の内容に従って KSN を使用する**

選択に応じて、KSN は更新前の、もしくは更新された KSN 声明の規約に従い動作します。管理サーバーのプロパティからいつでも同意した KSN 声明の本文を表示できます。

ディストリビューションポイントが KSN プロキシサーバーとして機能するかどうかの確認

ディストリビューションポイントとして機能するように割り当てられた管理対象デバイスで、KSN プロキシサーバーを有効にできます。ksnproxy サービスがデバイスで実行されている場合、管理対象デバイスは KSN プロキシサーバーとして機能します。デバイスでこのサービスをローカルで確認し、オンまたはオフにできます。

Windows ベースまたは Linux ベースのデバイスをディストリビューションポイントとして割り当てることができます。ディストリビューションポイントのチェック方法は、このディストリビューションポイントのオペレーティングシステムによって異なります。

Windows ベースのディストリビューションポイントが KSN プロキシサーバーとして機能するかどうかを確認するには：

1. ディストリビューションポイントデバイスの Windows で、［**サービス**］（［**すべてのプログラム**］→［**管理ツール**］→［**サービス**］）を開きます。
2. サービスのリストで、ksnproxy サービスが実行されているかを確認します。

   ksnproxy サービスが実行されている場合、デバイス上のネットワークエージェントは Kaspersky Security Network に参加し、ディストリビューションポイントの範囲に含まれる管理対象デバイスの KSN プロキシサーバーとして機能します。

必要に応じて ksnproxy サービスをオフにできます。この場合、ディストリビューションポイントのネットワークエージェントは Kaspersky Security Network への参加を停止します。この操作にはローカル管理者権限が必要です。

Linux ベースのディストリビューションポイントが KSN プロキシサーバーとして機能するかどうかを確認するには：

1. ディストリビューションポイントのデバイスで、実行中のプロセスの一覧を表示します。
2. 実行中のプロセスのリストで、`/opt/kaspersky/ksc64/sbin/ksnproxy` プロセスが実行されているかどうかを確認します。

`/opt/kaspersky/ksc64/sbin/ksnproxy` プロセスが実行されている場合、デバイス上のネットワークエージェントは Kaspersky Security Network に参加し、ディストリビューションポイントの範囲に含まれる管理対象デバイスの KSN プロキシサーバーとして機能します。

ライセンスの定義

このセクションでは、Kaspersky Security Center Cloud コンソールで管理するカスペルスキー製品のライセンスに関連する概念の定義について説明します。

ライセンスについて

*ライセンス*は、署名されたライセンス契約（使用許諾契約書）の条件に基づいて提供される、Kaspersky Security Center Cloud コンソールを使用する期限付きの権利です。

サービスの範囲と有効期間は、アプリケーションが使用されるライセンスによって異なります。

次のライセンス種別があります：

- *試用版*

  製品の試用を目的とした無償ライセンス。試用版ライセンスは通常、有効期間が短く設定されています。

  試用版ライセンスの有効期間が終了すると、Kaspersky Security Center Cloud コンソールのすべての機能が無効になります。製品の使用を継続するには、製品版ライセンスを購入する必要があります。

  試用ライセンスに基づいてアプリケーションを使用できるのは、1回の試用期間のみです。

- *製品版*

  有料ライセンス。

  製品版ライセンスの有効期限が切れると、本製品の主要な機能が無効になります。Kaspersky Security Center Cloud コンソールの使用を継続するには、製品版ライセンスを更新する必要があります。商用ライセンスの有効期限が切れると、アプリケーションを引き続き使用できなくなり、デバイスから削除する必要があります。

  有効期間が終了する前、すべてのセキュリティ脅威から継続的に保護された環境を維持できるようにライセンスを更新することを推奨します。

ライセンス証書について

*ライセンス証書*とは、ライセンス情報ファイルまたはアクティベーションコードに付随して受け取る文書です。

ライセンス証書には、提供されたライセンスに関する次の情報が含まれています：

- ライセンス情報の数値または注文番号
- ライセンスが適用されるユーザーの情報
- 提供されたライセンスを使用したアクティベーションが可能である製品の情報
- ライセンスの上限（提供されたライセンスで使用可能な製品が使用できるデバイスの台数など）
- ライセンスの有効期間の開始日
- ライセンスの有効期間または有効期間の終了日
- ライセンス種別

ライセンス情報について

*ライセンス情報*とは、使用許諾契約書の条項に基づいてアクティベーションを適用して製品を使用できる数値の並びです。ライセンス情報は、カスペルスキーによって生成されます。

*アクティベーションコード*を入力して、アプリケーションにライセンスを追加できます。ライセンス情報は、製品に追加した後、インターフェイスに一意の英数字の並びで表示されます。

使用許諾契約書の条項に違反した場合、カスペルスキーがライセンス情報をブロックします。ライセンス情報がブロックされた際に、製品を使用したい場合は、別のライセンス情報を追加する必要があります。

ライセンスには、現在のライセンスまたは予備のライセンスがあります。

現在のライセンス：アプリケーションによって現在使用されているライセンス。現在のライセンスは、試用版または製品版のライセンス情報として追加できます。製品に指定できる現在のライセンスは1つのみで、2つ以上の現在のライセンスを指定することはできません。

予備のライセンス：アプリケーションを使用する権限をユーザーに付与する、現在使用されていないライセンス。予備のライセンスは、現在のライセンスの有効期間が終了すると、自動的に適用されます。予備のライセンスは、現在のライセンスが追加済みである場合にのみ、追加できます。

試用版のライセンスは、現在のライセンスとしてのみ追加できます。試用版のライセンスを予備のライセンスとして追加することはできません。

アクティベーションコードについて

*アクティベーションコード*は、英数字20文字の一意な並びで構成されます。アクティベーションコードを入力すると、Kaspersky Security Center Cloudコンソールをアクティベートするライセンスを追加することができます。アクティベーションコードは、Kaspersky Security Center Cloudコンソールを購入すると提供されます。

アクティベーションコードを使用して製品をアクティベートするには、カスペルスキーのアクティベーションサーバーと接続を確立するためのインターネット接続が必要です。システムDNSを使用したサーバーへのアクセスが不可能な場合は、パブリックDNSサーバーが使用されます。

アクティベーションコードを使用して製品をアクティベートした後、ライセンスの現在のステータスを確認するリクエストが、製品からカスペルスキーのアクティベーションサーバーに定期的に送信される場合があります。アプリケーションからリクエストを送信するには、インターネット接続が必要です。

アプリケーションのインストール後にアクティベーションコードを紛失した場合は、ライセンスを購入したカスペルスキーのパートナー企業に連絡してください。

管理対象アプリケーションのアクティベーションにライセンス情報ファイルは使用できません。アクティベーションコードのみ使用できます。

定額制サービスについて

*Kaspersky Security Center Cloud コンソールの定額制サービス*とは、選択した設定（有効期限、保護されるデバイスの台数）でのアプリケーションの使用を注文することです。Kaspersky Security Center Cloudコンソールの定額制サービスをサービスプロバイダー（インターネットプロバイダーなど）に登録できます。定額制サービスは手動および自動で更新することができ、キャンセルすることもできます。

定額制サービスの期間は制限する（1年間など）ことも、無制限にすることもできます。制限された定額制サービスの期限を過ぎてKaspersky Security Center Cloudコンソールを利用するには、更新する必要があります。サービスプロバイダーによって期限までに支払いが行われた場合、無制限の定額制サービスは自動的に更新されます。

制限された定額制サービスの期限が過ぎた場合は、更新するまでの猶予期間が与えられ、その期間はアプリケーションが機能し続けます。猶予期間の長さや利用できる機能はサービスプロバイダーによって定義されます。

Kaspersky Security Center Cloud コンソールを定額制サービスの形式で利用するには、サービスプロバイダーが提供するアクティベーションコードを適用する必要があります。

異なる Kaspersky Security Center Cloud コンソールのアクティベーションコードを適用できるのは、定額制サービスの期限の経過後か、定額制サービスのキャンセル時のみです。

サービスプロバイダーによっては、定額制サービスの管理に伴う操作が異なる可能性があります。サービスプロバイダーが定額制サービスの更新のための猶予期間を設定しないこともあり、その場合はアプリケーションを利用できなくなります。

定額制サービスの形式で利用する目的で購入されたアクティベーションコードで Kaspersky Security Center Cloud コンソールの旧バージョンをアクティベートすることはできません。

定額制サービスのもとアプリケーションを使用している場合、Kaspersky Security Center Cloud コンソールは、定額制サービスの有効期間が切れるまで、指定された間隔でアクティベーションサーバーへの接続を自動的に試みます。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。定額制サービスは、サービスプロバイダーの Web サイトで更新することができます。

データ提供

Kaspersky Security Center Cloud コンソールでは、管理対象アプリケーションの機能で、Kaspersky Security Center Cloud コンソールに接続されているデバイス（およびデバイスの所有者）をユーザーが識別してコントロールできます。

データ提供の方法：

1. ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスでデータを入力します。
2. ネットワークエージェントがデータをデバイスから受信して、管理サーバーに送信します。
3. ネットワークエージェントが、管理対象のカスペルスキー製品によって取得されたデータを受信して、管理サーバーに送信する。管理対象のカスペルスキー製品によって処理されるデータ一覧については、該当する製品のヘルプファイルに記載されています。
4. オンプレミスで実行されているセカンダリ管理サーバーからデータが転送されます。

Kaspersky Security Center Cloud コンソールは、試用版ライセンスの有効期間が終了した 30 日後、または製品版ライセンスの有効期間が終了した 90 日後に、ワークスペースを自動的に削除します。

ライセンスの有効期間が終了した後、カスペルスキーはアラートとインシデントに関連するユーザーのデータをユーザーのワークスペースに 30 日間保存します。

現在のライセンスでは、アラートとインシデントの保存期間は 360 日です。この期間が過ぎると、古いアラートと古いインシデントは自動的に削除されます。

このセクションに表示されたデータの最終的な削除には最大 24 時間かかる場合があります。

カスペルスキーのサーバーに送信されるデータ

アクティベーション中に送信されるデータ

ソフトウェアをアクティベートする際にアクティベーションコードを使用すると、ユーザーがソフトウェアを正規の用途で利用していることを確認するために、ユーザーは次の情報を定期的にカスペルスキーに提供することに同意したことになります：

- アクティベーションコード
- 現在のライセンスの一意のアクティベーション識別子

カスペルスキーでは、カスペルスキー製品の配布および使用の状況に関する統計情報を収集するために、この情報を使用する場合もあります。

アップデート中に送信されるデータ

権利者のアップデートサーバーからアップデートを受信することで、アップデートメカニズムの品質を改善するために、ユーザーは次の情報を定期的にカスペルスキーに提供することに同意したものとします：

- ライセンスから取得したソフトウェアの識別子

- ソフトウェアの完全なバージョン
- ソフトウェアのライセンス識別子
- ソフトウェアのインストールの識別子（PCID）
- ソフトウェアアップデートの起動の識別子

カスペルスキーでは、カスペルスキー製品の配布および使用の状況に関する統計情報を収集するために、この情報を使用する場合もあります。

操作中断のない運用、効率的な作業、および Kaspersky Security Center Cloud コンソールの合法的な使用を確認するためのデータ

次の情報が指定された目的で使用されます：

- ワークスペースに接続されているカスペルスキーのセキュリティ製品の名前とバージョン、これらのセキュリティ製品がインストールされているデバイス数。
- すべてのワークスペースに接続されているカスペルスキーのセキュリティ製品がインストールされているデバイスの数と、これらの接続されたデバイスの種別別の分布。
- ワークスペースの識別子、会社の識別子、ワークスペースの国と地域およびワークスペースの作成日。
- ワークスペース内のユーザー数、ワークスペース内での最終認証日。
- 現在使用しているライセンスについての詳細（ライセンス種別、デバイス数のライセンス制限、接続されているデバイスの数、以前使用していたライセンスの有効期限）。

Kaspersky Security Center Cloud コンソールのインターフェイスにあるリンクの使用時に転送されるデータ

管理コンソールまたは Kaspersky Security Center Cloud コンソールのリンクを使用することで、ユーザーは次のデータが自動的に送信されることに同意したものとします：

- Kaspersky Security Center Cloud コンソールの言語版
- ライセンス識別子
- ライセンスが代理店経由で購入されたかどうか

リンクの目的や位置によってリンク経由で提供されたデータのリスト。

ワークスペースが機能するために必要なデータ

Kaspersky Security Center Cloud コンソールは次のデータを処理します：

1. 組織のネットワークで検出されたデバイスの詳細

   ネットワークエージェントが次に記載されているデータをネットワーク接続されたデバイスから受信して、管理サーバーに送信します。

a. デバイスの識別に必要な、検出されたデバイスとそのコンポーネントの技術的な仕様情報（ネットワークのポーリングによって取得）：

- Active Directory のポーリング：

  Active Directory のデバイス：デバイスの識別名、ドメインコントローラーから取得した Windows ドメイン名、Windows 環境でのデバイス名、NetBIOS ドメイン名、デバイスの DNS ドメインと DNS 名、SAM（セキュリティアカウントマネージャー）アカウント（Windows NT 4.0、Windows 95、Windows 98、LAN Manager など、以前のオペレーティングシステムのバージョンを実行しているクライアントやサーバーのサポートに使用するシステムへのログインのための名前）、ドメインの識別名、デバイスが属するグループの識別名、デバイスを管理するユーザーの識別名、デバイスの GUID（グローバル一意識別子）と親 GUID。

  Active Directory ネットワークがポーリングされると、管理対象インフラストラクチャに関する情報の表示と、ユーザーによるこれらの情報の使用の目的（たとえば製品導入時など）で、次のデータ種別も処理されます：

- Active Directory 組織単位：組織単位の識別名、ドメインの識別名、組織単位の GUID と親 GUID

- Active Directory ドメイン：ドメインコントローラーから取得した Windows ドメイン名、DNS ドメイン、ドメインの GUID

- Active Directory ユーザー：ユーザーの表示名、ユーザーの識別名、ドメインの識別名、ユーザーの組織の名前、ユーザーが所属する部門の名前、ユーザーのマネージャーである別のユーザーの識別名、ユーザーの氏名、SAM アカウント、メールアドレス、予備のメールアドレス、メインの電話番号、予備の電話番号、携帯電話番号、ユーザーの役職名、ユーザーが属するグループの識別名、ユーザーの GUID（グローバル一意識別子）、ユーザーの SID（セキュリティ識別子。ユーザーをセキュリティプリンシパルとして識別するために使用する一意のバイナリ値）、UPN（ユーザープリンシパル名。インターネット標準 RFC 822 に基づく、インターネット形式のユーザーログイン名）。UPN は識別名より短く、覚えやすい名前です。規則により、UPN はユーザーのメール名にマッピングされます。

- Active Directory グループ：グループの識別名、メールアドレス、ドメインの識別名、SAM アカウント、グループが属する他のグループの識別名、グループ SID、グループ GUID。

b. Samba ドメインのポーリング：

Samba デバイス：デバイスの識別名、ドメインコントローラーから取得したドメイン名、NetBIOS デバイス名、NetBIOS ドメイン名、デバイスの DNS ドメインと DNS 名、SAM（セキュリティアカウントマネージャー）アカウント、ドメインの識別名、デバイスが属するグループの識別名、デバイスを管理するユーザーの識別名、デバイスの GUID（グローバル一意識別子）と親 GUID。

- Samba 組織単位：組織単位の識別名、ドメインの識別名、組織単位の GUID と親 GUID。

- Samba ドメイン：ドメインコントローラーから取得したドメイン名、DNS ドメイン、ドメインの GUID。

- Samba ユーザー：ユーザーの表示名、ユーザーの識別名、ユーザーの組織の名前、ユーザーが所属する部門の名前、ユーザーのマネージャーである別のユーザーの識別名、ユーザーの氏名、SAM アカウント、メールアドレス、予備のメールアドレス、メインの電話番号、予備の電話番号、携帯電話番号、ユーザーの役職名、ユーザーが属するグループの識別名、ユーザーの GUID（グローバル一意識別子）、ユーザーの SID（セキュリティ識別子。ユーザーをセキュリティプリンシパルとして識別するために使用する一意のバイナリ値）、UPN（ユーザープリンシパル名。インターネット標準 RFC 822 に基づく、インターネット形式のユーザーログイン名）。UPN は識別名より短く、覚えやすい名前です。規則により、UPN はユーザーのメール名にマッピングされます。

- Samba グループ：グループの識別名、メールアドレス、ドメインの識別名、SAM アカウント、グループが属する他のグループの識別名、グループ SID、グループ GUID。

c. Windows ドメインのポーリング：

- Windows ドメインまたはワークグループの名前
- デバイスの NetBIOS 名
- デバイスの DNS ドメインと DNS 名
- デバイス名と説明
- ネットワーク上のデバイス可視性
- デバイスの IP アドレス
- デバイス種別（ワークステーション、サーバー、SQL Server、ドメインコントローラーなど）
- デバイスのオペレーティングシステムの種別
- デバイスのオペレーティングシステムのバージョン
- デバイスについての情報が前回アップデートされた日時
- デバイスが前回ネットワークで検出された日時

d. IP アドレス範囲のポーリング：

- デバイスの IP アドレス
- デバイスの DNS 名または NetBIOS 名
- デバイス名と説明
- デバイスの MAC アドレス
- デバイスが前回ネットワークで検出された日時

2. 管理対象デバイスの詳細情報。

ネットワークエージェントによって、次に記載されたデータがデバイスから管理サーバーに送信されます。ユーザーはデバイスの表示名と説明を Kaspersky Security Center Cloud コンソールのインターフェイスに入力します：

a. デバイスの識別に必要な、管理対象デバイスとそのコンポーネントの技術的な仕様情報：

- デバイスの表示名（NetBIOS 名に基づいて生成され、手動で変更可能）と説明（手動で入力）
- Windows ドメイン名と種別（Windows NT ドメインまたは Windows ワークグループ）
- Windows 環境でのデバイス名
- デバイスの DNS ドメインと DNS 名
- デバイスの IP アドレス
- デバイスのサブネットマスク
- デバイスのネットワークロケーション
- デバイスの MAC アドレス

- デバイスのオペレーティングシステムの種別
- デバイスが仮想マシンかどうかの情報とハイパーバイザーの種別
- デバイスが VDI（仮想デスクトップインフラストラクチャ）の一部としての動的仮想マシンかどうかの情報
- デバイス GUID
- ネットワークエージェントのインスタンス ID
- ネットワークエージェントのインストール ID
- ネットワークエージェントの永続 ID

b. 管理対象デバイスの監査および特定のパッチやアップデートが適用可能かどうかの判断に必要となる、管理対象デバイスとそのコンポーネントのその他の仕様情報：

- WUA（Windows Update エージェント）のステータス
- オペレーティングシステムのアーキテクチャ
- OS 製造元
- OS のビルド番号
- OS のリリース ID
- OS のロケーションフォルダー
- デバイスが仮想マシンの場合、仮想マシンの種別
- デバイスの応答の待ち時間
- ネットワークエージェントがスタンドアロンモードで動作しているかどうかの情報

c. 管理対象デバイスのアクティビティに関する詳細情報：

- 前回のアップデートの日時
- デバイスが前回ネットワークで検出された日時
- 再起動の待機ステータス（「再起動が必要です」）
- デバイスの電源を入れた日時

d. デバイスのユーザーアカウントとその作業セッションの詳細情報

e. デバイスがディストリビューションポイントである場合、ディストリビューションポイントの動作統計情報：

- ディストリビューションポイントが作成された日時
- 作業フォルダー名
- 作業フォルダーのサイズ

- 管理サーバーとの同期回数
- デバイスを管理サーバーと前回同期した日時
- 転送したファイルの数と合計サイズ
- クライアントでダウンロードされたファイルの数と合計サイズ
- TCP を使用してクライアントでダウンロードされたデータのボリューム
- マルチキャストを使用してクライアントに送信されたデータのボリューム
- マルチキャストを使用してクライアントでダウンロードされたデータのボリューム
- マルチキャスト配信数
- マルチキャスト配信の合計ボリューム
- 管理サーバーと前回同期した後のクライアントとの同期回数

f. デバイスを管理する仮想管理サーバーの名前

g. クラウドデバイスの詳細情報：

- クラウドのリージョン
- VPC（仮想プライベートクラウド）
- クラウドのアベイラビリティーゾーン
- クラウドのサブネット
- クラウドのプレイスメントグループ

h. モバイルデバイスの詳細情報。管理対象アプリケーションによって、このデータがモバイルデバイスから管理サーバーに送信されます。データの完全なリストは、管理対象アプリケーションのヘルプで確認できます。

3. デバイスにインストールされたカスペルスキー製品の詳細情報。

管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます：

a. デバイスにインストールされている管理対象のカスペルスキー製品と Kaspersky Security Center Cloud コンソールのコンポーネント

b. 管理対象デバイスにインストールされたカスペルスキー製品の設定：

- カスペルスキー製品の名前とバージョン
- ステータス
- リアルタイム保護のステータス
- 前回のデバイススキャンの日時
- 検知した脅威の数

- 駆除に失敗したオブジェクトの数
- カスペルスキーのセキュリティ製品のタスク
- 製品コンポーネントが利用できるかに関する情報とそのステータス
- 定義データベースの前回のアップデート日時とバージョン
- カスペルスキー製品の設定の詳細情報
- 現在のライセンスに関する情報
- 予備のライセンスに関する情報
- アプリケーションのインストールの日付
- アプリケーションのインストール ID

c. 製品動作の統計情報：管理対象デバイス上のカスペルスキー製品コンポーネントのステータス変化および製品コンポーネントによって開始されたタスクのパフォーマンスに関係するイベント

d. カスペルスキー製品によって定義されたデバイスのステータス

e. カスペルスキー製品によって割り当てられたタグ

f. カスペルスキー製品のインストール済みのアップデートおよび適用可能なアップデート

- アプリケーションの表示名、バージョン、言語
- アプリケーションの内部名
- レジストリキーからの製品名とバージョン
- アプリケーションのインストールフォルダー
- パッチのバージョン
- インストール済みアプリケーションの自動パッチのリスト
- アプリケーションが Kaspersky Security Center Cloud コンソールでサポートされているかどうかの情報
- アプリケーションがクラスターにインストールされているかどうかの情報

g. デバイスにおけるデータ暗号化エラーの詳細：エラー ID、発生時刻、動作の種別（暗号化または復号化）、エラーの説明、ファイルパス、暗号化ルールの説明、デバイス ID、ユーザー名

4. Kaspersky Security Center Cloud コンソールのコンポーネントと管理対象カスペルスキー製品のイベント。

ネットワークエージェントによってデータがデバイスから管理サーバーに送信されます。

イベントの説明には次のデータが含まれる場合があります：

a. デバイス名

b. デバイスのユーザー名

c. デバイスにリモート接続した管理者の名前

d. デバイスにインストールされているアプリケーションの名前、バージョン、製造元

e. デバイス上のアプリケーションのインストールフォルダーのパス

f. デバイス上のファイルパスとファイル名

g. アプリケーションの実行時のアプリケーション名とコマンドラインのパラメータ

h. パッチ名、パッチファイル名、パッチ ID、パッチによって修正された脆弱性の重要度、パッチのインストールエラーの説明

i. デバイスの IP アドレス

j. デバイスの MAC アドレス

k. デバイスの再起動ステータス

l. イベントが発生したタスクの名前

m. デバイスがスタンドアロンモードに切り替えられたかどうかの情報と、切り替えの理由

n. デバイス上のセキュリティ問題に関する情報：セキュリティ問題のタイプ、セキュリティ問題の名前、深刻度、セキュリティ問題の説明、カスペルスキー製品から送信されたセキュリティ問題の詳細

o. デバイスのディスクの空き容量のサイズ

p. カスペルスキー製品が機能制限モードで動作しているかどうかの情報、機能範囲の ID

q. カスペルスキー製品の設定の古い値と新しい値

r. カスペルスキー製品またはその任意のコンポーネントによる操作の実行時に発生したエラーの説明

5. Kaspersky Security Center Cloud コンソールのコンポーネント、およびポリシーとポリシーのプロファイルに示される管理対象カスペルスキー製品の設定。

   ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスでデータを入力します。

6. Kaspersky Security Center Cloud コンソールのコンポーネントおよび管理対象カスペルスキー製品のタスク設定。

   ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスでデータを入力します。

7. 脆弱性とパッチ管理機能によってデータが処理されます。

   ネットワークエージェントによって、次に記載されたデータがデバイスから管理サーバーに送信されます：

   a. 管理対象デバイスにインストールされているアプリケーションおよびパッチの詳細情報（アプリケーションのレジストリ）。アプリケーションは、アプリケーションコントロール機能によって管理対象デバイスで検出された実行ファイルに関する情報に基づいて識別できます。

      - アプリケーション ID またはパッチ ID
      - 親アプリケーション ID（パッチ用）
      - アプリケーション名またはパッチ名、バージョン

- アプリケーションまたはパッチが Windows インストーラーの msi ファイルかどうかの情報
- アプリケーションまたはパッチの製造元
- ローカリゼーション言語 ID
- アプリケーションまたはパッチのインストールの日付
- アプリケーションのインストールパス
- アプリケーションまたはパッチの製造元のテクニカルサポートサイト
- 問い合わせ窓口
- インストール済みアプリケーションのインスタンス ID
- コメント
- アンインストールキー
- サイレントモードのインストールキー
- パッチの分類
- パッチに関する追加情報の URL
- アプリケーションのレジストリキー
- アプリケーションのビルド番号
- ユーザー SID
- オペレーティングシステムの種類（Windows、Unix）

b. 管理対象デバイスで検出されたハードウェアに関する情報（ハードウェアのレジストリ）：

- デバイス ID
- デバイス種別（マザーボード、CPU、RAM、大容量ストレージデバイス、ビデオアダプター、サウンドカード、ネットワークインターフェイスコントローラー、モニター、光ディスクデバイス）
- デバイス名
- 説明
- 製造元
- シリアル番号
- リビジョン
- ドライバーに関する情報：開発元、バージョン、説明、リリース日
- BIOS に関する情報：開発元、バージョン、シリアル番号、リリース日
- チップセット

- クロック周波数
- CPU コア数
- CPU スレッド数
- CPU プラットフォーム
- ストレージデバイスの回転速度
- RAM：種別、パーツ番号
- ビデオメモリ
- サウンドカードのコーデック

c. 管理対象デバイスで検出されたサードパーティ製品の脆弱性に関する詳細情報：

- 脆弱性識別子
- 脆弱性の重要度（警告、高、緊急）
- 脆弱性種別（Microsoft、サードパーティ）
- 脆弱性について説明されているページの URL
- 脆弱性のエントリが作成された日時
- 製造元名
- ローカライズされた製造元名
- 製造元 ID
- アプリケーション名
- ローカライズされたアプリケーション名
- アプリケーションのインストールコード
- アプリケーションのバージョン
- 製品のローカリゼーション言語
- 脆弱性の説明からの CVE ID のリスト
- 脆弱性をブロックしているカスペルスキーのプロテクション技術（ファイル脅威対策、ふるまい検知、ウェブ脅威対策、メール脅威対策、ホスト侵入防止、ZETA シールド）
- 脆弱性が検知されたオブジェクトファイルのパス
- 脆弱性の検知時刻
- 脆弱性の説明からのナレッジベース記事の ID
- 脆弱性の説明からのセキュリティ情報の ID

- 脆弱性に対するアップデートのリスト
- 脆弱性攻撃が存在したかどうかの情報
- 脆弱性に対するマルウェアが存在したかどうかの情報

d. 管理対象デバイスにインストールされているサードパーティ製品で利用できるアップデートの詳細情報：

- アプリケーション名およびバージョン
- 製造元
- 製品のローカリゼーション言語
- オペレーティングシステム
- インストールシーケンスに応じたパッチのリスト
- パッチが適用されたアプリケーションの元のバージョン
- パッチのインストール後のアプリケーションのバージョン
- パッチ ID
- ビルド番号
- インストールフラグ
- パッチの使用許諾契約書
- パッチが、他のパッチのインストールに必須かどうかの情報
- 必要なインストール済みアプリケーションとそのアップデートのリスト
- パッチの情報源
- パッチの追加情報（Web ページのアドレス）
- パッチのダウンロード用 URL、ファイル名、バージョン、リビジョン、SHA-256

e. WSUS 機能によって検出された Microsoft Update の詳細情報：

- アップデートのリビジョン番号
- Microsoft Update の種別（ドライバー、ソフトウェア、カテゴリ、Detectoid）
- MSRC（Microsoft Security Response Center）の情報によるアップデートの重要度（低、中、高、緊急）
- アップデートに関連する MSRC の情報の ID
- MSRC ナレッジベースの記事の ID
- アップデート名（ヘッダー）

- アップデートの説明
- アップデートのインストーラーが対話モードかどうかの情報
- インストールフラグ
- アップデートの分類（重要なアップデート、定義のアップデート、Feature Pack、セキュリティのアップデート、Service Pack、ツール、アップデートロールアップ、アップデート、アップグレード）
- アップデートが適用されたアプリケーションに関する情報
- EULA（使用許諾契約書）ID
- EULA のテキスト
- アップデートのインストールのため、EULA に同意する必要があるかどうかの情報
- 関連付けられたアップデートに関する情報（ID とリビジョン番号）
- アップデート ID（Microsoft Windows Update のグローバル ID）
- より古いアップデートの ID
- アップデートが隠されているかどうかの情報
- アップデートが必須かどうかの情報
- アップデートのインストールステータス（適用不可、インストール未割り当て、割り当て済み、インストール中、インストール済み、失敗、再起動が必要、新しいバージョンのインストール未割り当て）
- アップデートの CVE ID
- アップデートをリリースした会社、または「不明な会社」の値

f. デバイスにインストールする必要のある、WSUS 機能によって検出された Microsoft の更新プログラムのリスト。

8. アプリケーションコントロール機能を使用して管理対象デバイスで検出された、実行ファイルに関する情報（アプリケーションレジストリの情報が関連付けられている場合があります）。データの完全なリストについては、該当するアプリケーションで管理されるデバイスのデータを説明するセクションに記載されています。

   管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。

9. バックアップされたファイルに関する情報。データの完全なリストについては、該当するアプリケーションで管理されるデバイスのデータを説明するセクションに記載されています。

   管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。

10. 詳細分析のためにカスペルスキーの担当者から提出を依頼されたファイルに関する情報。データの完全なリストについては、該当するアプリケーションで管理されるデバイスのデータを説明するセクションに記載されています。

    管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。

11. アダプティブアノマリーコントロールルールのステータスとトリガーに関する情報。データの完全なリストについては、該当するアプリケーションで管理されるデバイスのデータを説明するセクションに記載されています。

    管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。

12. デバイスコントロール機能によって検出された、管理対象デバイスに搭載されているデバイスまたは管理対象デバイスに接続しているデバイス（メモリユニット、情報転送ツール、情報ハードコピーツール、接続バス）に関する情報。データの完全なリストについては、該当するアプリケーションで管理されるデバイスのデータを説明するセクションに記載されています。

    管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます。

13. アラートに関するデータ：

    - アラートのテレメトリイベントの最初のイベントの日時
    - アラートのテレメトリイベントの最後のイベントの日時
    - 適用されたルールの名前（ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスに入力します）
    - アラートのステータス
    - 解決（誤検知、正しい検知、優先度低）
    - アラートに割り当てられたユーザーの識別子および名前
    - Kaspersky Security Center Cloud コンソールのデータベース内の一意な識別子と、アラート発出の元となったイベントに関連するデバイスの名前
    - アラート発出の元となったイベントに関連するデバイスのユーザーの SID と名前
    - アラート発出対象のデータ（アラート発出の元となったイベントに関連するデータ）
        - IP アドレス
        - ファイルとファイルパスの MD5 ハッシュサム
        - URL
        - ドメイン
    - アラートに関連するオブジェクトの追加の詳細（本製品から受け取ったもの）
    - アラートへのコメント：
        - コメントが追加された日時
        - コメントを追加したユーザー
        - コメントの本文
    - アラート変更ログ：
        - 変更の日時

- 変更を行ったユーザー
- 変更の説明

14. セキュリティ問題に関するデータ：

- セキュリティ問題の最初のイベントの日時
- セキュリティ問題の最後のイベントの日時
- セキュリティ問題名（ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスで入力するデータ）
- セキュリティ問題の簡単な説明
- セキュリティ問題の優先度
- セキュリティ問題のステータス
- セキュリティ問題に割り当てられたユーザーの識別子と名前
- 解決（誤検知、正しい検知、優先度低、統合済み）
- セキュリティ問題へのコメント：
  - コメントが追加された日時
  - コメントを追加したユーザー
  - コメントの本文
- セキュリティ問題の変更ログ：
  - 変更の日時
  - 変更を行ったユーザー
  - 変更の説明

15. カスペルスキー製品のデータ暗号化機能で処理されたデータ。

管理対象アプリケーションによって、次のデータがネットワークエージェント経由でデバイスから管理サーバーに送信されます。ユーザーはドライブの説明を Kaspersky Security Center Cloud コンソールのインターフェイスに入力します：

a. デバイスのドライブのリスト：

- ドライブ名
- 暗号化ステータス
- ドライブ種別（起動ドライブ、ディスクドライブ）
- ドライブのシリアル番号
- 説明

b. デバイスのデータ暗号化エラーの詳細：

- エラーが発生した日時
- 動作の種別（暗号化、復号化）
- エラーの説明
- ファイルパス
- ルールの説明
- デバイス ID
- ユーザー名
- エラー ID

c. カスペルスキー製品のデータ暗号化設定。

データの完全なリストについては、該当するアプリケーションで管理されるデバイスのデータを説明するセクションに記載されています。

16. 入力されたアクティベーションコードの詳細情報。

ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスでデータを入力します。

17. ユーザーアカウント。

ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスで次のデータを入力します：

a. 名前

b. 説明

c. 名前

d. メールアドレス

e. 電話番号

f. パスワード

18. Active Directory を使用したユーザー認証に必要なデータ：

a. Active Directory フェデレーションサービス（ADFS）の設定：

- 認証プロバイダーのメイン URL
- ADFS の信頼されたルート証明書
- ADFS で生成されたクライアント ID
- ADFS へのアクセスを保護するための秘密鍵
- トークンの範囲
- 統合が実行されている Active Directory ドメイン

- ユーザー SID を含むトークンフィールドの名前
- ユーザーグループの SID のアレイを含むトークンフィールドの名前

ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスでデータを入力します。

b. Kaspersky Security Center Cloud コンソールが ADFS サーバーから自動的に受信するデータ：

- 発行者（issuer）
- ユーザー認証エンドポイント（authorization_endpoint）
- トークンエンドポイント（token_endpoint）
- JSON Web キーセットの URI（jwks_uri）
- アクセストークンの発行者（access_token_issuer）
- ユーザー情報エンドポイント（userinfo_endpoint）
- セッション終了エンドポイント（end_session_endpoint）
- トークン署名証明書

19. 管理オブジェクトの変更履歴：管理サーバー、管理グループ、ポリシー、タスク、ユーザー / セキュリティグループ、インストールパッケージ。

ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスで次のデータを入力します：

a. 管理サーバー

b. 管理グループ

c. ポリシー

d. タスク

e. ユーザー / セキュリティグループ

f. インストールパッケージ

20. 削除された管理オブジェクトのレジストリ。

ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスでデータを入力します。

21. ファイルから作成されたインストールパッケージとインストール設定。

ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスでデータを入力します。

22. カスペルスキーからの通知の表示を Kaspersky Security Center Cloud コンソールで表示するために必要なデータ：

a. ユーザーが使用している管理対象カスペルスキー製品についての情報：アプリケーション ID、完全なバージョン番号。

b. Kaspersky Security Center Cloud コンソールインターフェイスのユーザーの言語版。

c. デバイスのソフトウェアアクティベーションに関する情報：ソフトウェアライセンス識別子、ソフトウェアライセンスの有効期間、ソフトウェアライセンスの有効期限、使用されているソフトウェアライセンスの種別、ソフトウェア定額制サービスの種別、ソフトウェア定額制サービスの有効期限、ソフトウェア定額制サービスの現在のステータス、ソフトウェア定額制サービスの現在のステータスまたは変更中のステータスの理由、ソフトウェアライセンスが購入された価格リストの項目 ID。

d. ユーザーが同意した、ソフトウェアの使用中の法的契約に関する情報：法的契約の種別、法的契約のバージョン、ユーザーが法的契約の条項に同意したかどうかを示すフラグ。

e. 権利者から受信した通知に関する情報：通知 ID、通知の受信時刻、通知の受信ステータス。

ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスでデータを入力します。

23. Kaspersky Security Center Cloud コンソールのユーザー設定。

ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスで次のデータを入力します：

a. ユーザーインターフェイスのローカリゼーション言語

b. ユーザーインターフェイスのテーマ

c. 監視パネルの表示設定

d. 通知のステータスに関する情報：確認済みまたは未確認

e. スプレッドシートの列のステータス：表示または非表示

f. チュートリアルの進捗状況

24. 管理対象デバイスでリモート診断を使用する時に受信したデータ：トレースファイル、システム情報、デバイスにインストールされているカスペルスキー製品の詳細、ダンプファイル、ログファイル、テクニカルサポートから受信した診断スクリプトの実行結果。

25. ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスで入力するデータ：

a. 管理グループの階層作成時の管理グループ名

b. メール通知設定時のメールアドレス

c. デバイスのタグとタグルール

d. アプリケーションのタグ

e. アプリケーションのユーザーカテゴリ

f. ユーザーへのロール割り当て時のロール名

g. サブネットに関する情報：サブネット名、説明、アドレス、マスク

h. レポートと抽出の設定

i. ユーザーが入力したその他のデータ

26. オンプレミスに導入されているセカンダリ管理サーバーから受信したデータ。

Kaspersky Security Center 管理サーバーで処理されるデータについては、Kaspersky Security Center のオンラインヘルプで説明しています。

オンプレミスに導入されている Kaspersky Security Center 管理サーバーを、Kaspersky Security Center Cloud コンソールとの関連でセカンダリとして接続すると、Kaspersky Security Center Cloud コンソールはセカンダリ管理サーバーからの次のデータ種別を処理します：

a. Active Directory ネットワーク内または Windows ネットワーク内のデバイスの検索または IP 区間のスキャンによって取得した、組織のネットワーク内のデバイスに関する情報

b. Active Directory ネットワークのポーリングによって取得した、Active Directory の組織単位、ドメイン、ユーザー、グループに関する情報

c. 管理対象デバイスとその技術的な仕様情報（デバイスの識別に必要な情報、デバイスのユーザーアカウントとその作業中のセッションに関する情報を含む）

d. Exchange ActiveSync プロトコル経由で送信されるモバイルデバイスに関する情報

e. iOS MDM プロトコル経由で送信されるモバイルデバイスに関する情報

f. デバイスにインストールされたカスペルスキー製品の詳細情報：設定、動作統計情報、製品によって定義済みのデバイスのステータス、インストール済みおよび適用可能なアップデート、タグ

g. Kaspersky Security Center のコンポーネントおよび管理対象のカスペルスキー製品からイベント設定によって送信される情報

h. Kaspersky Security Center のコンポーネント、およびポリシーとポリシーのプロファイルに示される管理対象のカスペルスキー製品の設定

i. Kaspersky Security Center のコンポーネントおよび管理対象のカスペルスキー製品のタスク設定

j. 脆弱性とパッチ管理機能によって処理されるデータ：アプリケーションとパッチの詳細情報、ハードウェアに関する情報、管理対象デバイスで検知されたサードパーティ製ソフトウェアの脆弱性の詳細情報、サードパーティ製品で適用可能なアップデートの詳細情報、WSUS 機能によって検出された Microsoft Update の詳細情報

k. アプリケーションのユーザーカテゴリ

l. アプリケーションコントロール機能を使用して管理対象デバイスで検出された実行ファイルの詳細情報

m. バックアップされたファイルの詳細情報

n. 隔離されたファイルの詳細情報

o. 詳細分析のためにカスペルスキーの担当者から提出を依頼されたファイルの詳細情報

p. アダプティブアノマリーコントロールルールのステータスとトリガーに関する情報

q. アプリケーションコントロール機能によって検出された、管理対象デバイスに搭載されているデバイスまたは管理対象デバイスに接続しているデバイス（メモリユニット、情報転送ツール、情報ハードコピーツール、接続バス）の詳細情報

r. カスペルスキー製品の暗号化設定：暗号化鍵のリポジトリ、デバイスの暗号化ステータス

s. カスペルスキー製品のデータ暗号化機能を使用してデバイス上で実行されたデータ暗号化のエラーに関する情報

t. 管理対象のプログラマブルロジックコントローラー（PLC）のリスト

u. 入力されたアクティベーションコードの詳細情報

v. ユーザーアカウント

w. 管理オブジェクトの変更履歴

x. 削除された管理オブジェクトのレジストリ

y. ファイルから作成されたインストールパッケージとインストール設定

z. Kaspersky Security Center Web コンソールのユーザー設定

aa. ユーザーが管理コンソールまたは Kaspersky Security Center Cloud コンソールのインターフェイスで入力したあらゆるデータ

ab. 管理対象デバイスから Kaspersky Security Center コンポーネントへのセキュアな接続を確立するための証明書

27. リモート診断の使用時に管理対象デバイスからアップロードされた情報：診断ファイル（ダンプファイル、ログファイル、トレースファイルなど）とそれらのファイルに含まれているデータ。

28. イベントのエクスポートのため、Kaspersky Security Center Cloud コンソールと SIEM システムとの統合に必要なデータ：

- 接続と認証に必要なデータ：
  - SIEM システムの接続アドレスとポート
  - SIEM サーバーの認証証明書
  - SIEM システムで Kaspersky Security Center Cloud コンソールのクライアント認証を行うための信頼済み証明書と秘密鍵

  ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスでデータを入力します。
- Kaspersky Security Center Cloud コンソールが SIEM システムから受信するデータ：SIEM サーバー認証のための SIEM サーバー証明書の公開鍵

29. Kaspersky Security Center Cloud コンソールとクラウド環境の対話に必要なデータ：

a. Amazon Web Services（AWS）：

- IAM ユーザーアカウントのアクセスキーの ID
- IAM ユーザーアカウントの秘密鍵

b. Microsoft Azure：

- Azure アプリケーション ID
- Azure サブスクリプション ID
- Azure アプリケーションパスワード
- Azure リポジトリのアカウント名
- Azure リポジトリのアカウントアクセスキー

c. Google Cloud：

- Google クライアントのメール
- プロジェクト ID
- 秘密鍵

ユーザーが Kaspersky Security Center Cloud コンソールのインターフェイスでデータを入力します。

30. サポートされていないカスペルスキー製品から送信されるデータ

Kaspersky Security Center Cloud コンソールでサポートされていないカスペルスキー製品がインストールされているデバイスにネットワークエージェントをインストールしても、このカスペルスキー製品は引き続き Kaspersky Security Center Cloud にデータを送信します（データのリストについては、「データ提供について」セクションに記載）。ただし、Kaspersky Security Center Cloud コンソールでは、サポートされていない製品から送信されるデータを、Kaspersky Security Center Cloud コンソールの基本機能で説明されている処理と同様には処理できません。

サポートされているカスペルスキー製品のリストについては、Kaspersky Security Center Cloud コンソールのオンラインヘルプに記載されています。

管理対象アプリケーションが機能するために必要なデータ

次の管理対象アプリケーションによって、データがネットワークエージェント経由でデバイスから管理サーバーに送信されます：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Agent
- Kaspersky Security for Windows Server
- Kaspersky Security for Mobile
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux

処理されるデータについては、https://ksc.kaspersky.com/Home/LegalDocuments の「Kaspersky Security Center Cloud Console Data Processing Agreement」に記載されています。法的文書の Web ページで「Kaspersky Security Center Cloud Console Agreement」という名前のテキストブロックを見つけ、該当する管理対象アプリケーションで管理されるデバイスのデータについて記載されている部分までテキストブロックをスクロールします。このため、ブラウザーの標準検索機能も使用できます。

ローカル環境で処理されるユーザーデータ

Kaspersky Security Center Cloud コンソールでローカル環境に導入できる Kaspersky Security Center コンポーネントは、ネットワークエージェントのみです。

ローカル環境で処理されるユーザーデータのリスト：

- 「ユーザーデータ」セクションに記載されている、カスペルスキーのフレームワークおよびインフラストラクチャ内で処理されるすべてのデータ（管理者が Kaspersky Security Center Cloud コンソールのインターフェイスで入力したデータを除く）
- ネットワークエージェントの Kaspersky イベントログ
- ネットワークエージェントのトレース
- ログ（ネットワークエージェントのインストーラーと Kaspersky Security Center ユーティリティが作成したログを含む）

ネットワークエージェントのダンプ、ログ、トレースファイルにはランダムなデータが含まれており、個人データが含まれている場合もあります。ファイルは、ネットワークエージェントがインストールされているデバイスに暗号化されずに保存されます。ファイルが自動的にカスペルスキーに送信されることはありません。Kaspersky Security Center の動作の問題を解決するため、テクニカルサポートに依頼された場合に、ユーザーがこのデータをカスペルスキーに手動で送信できます。

個人データを処理する追加の組織

カスペルスキーに加え、Kaspersky Security Center Cloud コンソールのワークスペース関連の個人データを処理する組織は次の通りです：

組織名と所在地：
Microsoft Ireland Operations Limited
One Microsoft Place, South County Business Park, Leopardstown
Dublin 18 D18 P521

サービス：
Microsoft Azure（データホスティング）

データが処理される国については、「Kaspersky Security Center Cloud コンソールの情報の保存に使用するデータセンターの選択」セクションに記載されています。

Kaspersky Security Center Cloud コンソールの法的文書について

Kaspersky Security Center Cloud コンソールを使用するには、Kaspersky Security Center Cloud コンソールの Web サイトで指定される法的文書の条件を読んで同意する必要があります。 AO Kaspersky Lab の Web サイトに関するプライバシーポリシーの条項は、ワークスペースを管理するための Kaspersky Security Center Cloud コンソールへのサインイン時に表示されます。Kaspersky Security Center Cloud コンソールの使用許諾契約書と Kaspersky Security Center Cloud コンソールのデータ処理契約書は、会社のワークスペースの作成時に表示されます。

Kaspersky Security Center Cloud コンソールの使用を開始する前に、すべての法的文書の内容をよくお読みください。

カスペルスキー製品の使用許諾契約書

使用許諾契約書（以後、EULA とも表記）は、ユーザーと AO Kaspersky Lab との間で交わされる契約であり、カスペルスキー製品の使用条件が定められています。

使用許諾契約書の条項は、次の方法で確認できます：

- カスペルスキー製品のインストールパッケージの作成時に表示されるウィンドウ
- 管理対象デバイスにある、カスペルスキー製品のインストールフォルダーの license.txt ファイル

いつでも、使用許諾契約書に対する同意を取り消すことができます。

カスペルスキー製品の使用許諾契約書の条項に同意しない場合、この製品は使用できません。

ハードニングガイド

Kaspersky Security Center Cloud コンソールは、カスペルスキーがホストおよび維持する製品です。ユーザーが Kaspersky Security Center Cloud コンソールをコンピューターまたはサーバーにインストールする必要はありません。Kaspersky Security Center Cloud コンソールにより、管理者はカスペルスキーのセキュリティ製品を企業ネットワークのデバイスにインストールしたり、リモートでスキャンを実行してタスクをアップデートしたり、管理対象アプリケーションのセキュリティポリシーを管理したりできます。

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

Kaspersky Security Center Cloud コンソールは、クライアントデバイスの保護管理に完全にアクセスでき、組織のセキュリティシステムを構成する最も重要なコンポーネントです。したがって、Kaspersky Security Center Cloud コンソールでは、保護方法を強化する必要があります。

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

ハードニングガイドには、次の情報が含まれています：

- Kaspersky Security Center Cloud コンソールにアクセスするためのアカウントの設定
- クライアントデバイスの保護管理
- 管理対象アプリケーションの保護構成
- サードパーティ製品への情報の転送

Kaspersky Security Center Cloud コンソールでの作業を開始する前に、ハードニングガイドの簡易版を読むように要求されます。

ハードニングガイドを読んだことを確認するまでは、Kaspersky Security Center Cloud コンソールを使用することができませんので、ご注意ください。

ハードニングガイドを読むには：

1. Kaspersky Security Center Cloud コンソールを開いてログインします。Kaspersky Security Center Cloud コンソールは、現在のバージョンのハードニングガイドを読んだことを確認したかどうかを確認します。

   ハードニングガイドをまだ読んでいない場合は、ウィンドウが開き、ハードニングガイドの簡易版が表示されます。

2. 次のいずれかの手順を実行します：

   - ハードニングガイドの簡易版をテキストドキュメントとして表示したい場合は、［**新しいウィンドウで開く**］をクリックします。
   - ハードニングガイドの完全版を表示するには、［**オンラインヘルプで「ハードニングガイド」を開く**］をクリックします。

3. ハードニングガイドを読んだ後、［**ハードニングガイドの内容をすべて確認し、理解した上で同意します**］をオンにし、［**同意する**］をクリックします。

これで、Kaspersky Security Center Cloud コンソールを操作できるようになりました。

ハードニングガイドの新しいバージョンが表示されると、Kaspersky Security Center Cloud コンソールはそれを読むように促します。

Kaspersky Security Center Cloud コンソールのアーキテクチャ

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

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

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

- 管理者のワークスペースの組織と Kaspersky Security Center Cloud コンソールへの接続方法
- ネットワークエージェントと保護ソフトウェアの導入方法
- ディストリビューションポイントの使用
- 仮想管理サーバーの使用
- 管理サーバーの階層の使用
- 定義データベースのアップデート方式
- その他の情報の流れ

アカウントおよび認証

Kaspersky Security Center Cloud コンソールでの二段階認証の使用

Kaspersky Security Center Cloud コンソールは、ユーザーに二段階認証を提供します。

二段階認証は、Kaspersky Security Center Cloud コンソールでのアカウントのセキュリティを強化するのに効果的です。この機能を有効にすると、メールアドレスとパスワードを使用して Kaspersky Security Center Cloud コンソールにログインするたびに、追加のワンタイムセキュリティコードの入力が必要になります。ワンタイムセキュリティコードは、SMS で取得するか、認証アプリケーションでこのコードを生成することによって取得できます（設定した二段階認証方法に応じて異なります）。

Kaspersky Security Center Cloud コンソールへの接続が確立されているデバイスと同じデバイスに認証アプリケーションをインストールすることは**強く推奨しません**。モバイルデバイスに認証アプリケーションをインストールすることができます。

管理者パスワード保存の禁止

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

ブラウザーが侵害された場合、侵入者は保存されたパスワードにアクセスできる可能性があります。また、パスワードが保存されているユーザーデバイスが盗難または紛失した場合、侵入者が保護されたデータにアクセスできる可能性があります。

メイン管理者ロールのメンバーシップの制限

メインの管理者ロールのメンバーシップを制限することを推奨します。

既定では、ユーザーがワークスペースを作成すると、メインの管理者ロールがこのユーザーに割り当てられます。これは管理には便利ですが、メイン管理者ロールには広範な権限があるため、セキュリティの観点からは非常に重要です。ロールをユーザーに割り当てることは厳密に規制される必要があります。

Kaspersky Security Center Cloud コンソールの管理用に既に設定済みの権限を持つ定義されたユーザーロールを使用できます。

アプリケーション機能へのアクセス権の設定

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

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

ロールベースのアクセス制御モデルの主な利点：

- 管理の容易さ
- ロール階層
- 最小特権方法
- 職務の分離

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

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

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

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

アプリケーションのリモートインストール用の個別のアカウント

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

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

クライアントデバイスの保護管理

管理グループ間でデバイスを移動するための自動ルール

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

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

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

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

ディストリビューションポイントと接続ゲートウェイのセキュリティ要件

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

- 管理サーバーから受信したアップデートとインストールパッケージをグループ内のクライアントデバイスに配布します。
- クライアントデバイスでサードパーティ製ソフトウェアとカスペルスキー製品のリモートインストールを実行します。
- 新しいデバイスを検出したり既存のデバイスの情報を更新するために、ネットワークを検索します。
- クライアントデバイスの KSN プロキシサーバーとして機能します。

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

管理対象アプリケーションの保護構成

ネットワーク保護の設定

Kaspersky Security Center Cloud コンソールの初期設定シナリオが完了していることを確認してください。このシナリオには、クイックスタートウィザードの手順の実行も含まれます。

クイックスタートウィザードの実行中に、既定のパラメータを含むポリシーとタスクが作成されます。これらのパラメータは最適ではない可能性があり、組織内で禁止されている場合もあります。したがって、作成したポリシーとタスクを設定し、必要に応じて組織ネットワークに追加のポリシーとタスクを作成することを推奨します。

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

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

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

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

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

［**アンインストール用パスワードを使用する**］をオンにすると、Kaspersky Security Center Web コンソールの削除ツール（cleaner.exe）のパスワード保護も有効になります。

Kaspersky Security Network の使用

管理対象アプリケーションのすべてのポリシーと Kaspersky Security Center Cloud コンソールのプロパティで、Kaspersky Security Network（KSN）の使用を有効にし、KSN 声明を受け入れることを推奨します。Kaspersky Security Center Cloud コンソールをアップデートまたはアップグレードする場合、更新された KSN 声明を受け入れることができます。

新しいデバイスの検出

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

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

サードパーティシステムへのイベント転送

監視とレポート

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

SIEM システムへのイベントのエクスポート

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

監査イベントのメール通知

緊急事態にタイムリーに対応するために、公開する監査イベント、重要イベント、障害イベント、および警告に関する通知を送信するように Kaspersky Security Center Cloud コンソールを設定することを推奨します。

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

Kaspersky Security Center Cloud コンソールの初期設定

このセクションでは、Kaspersky Security Center Cloud コンソールの主要な導入シナリオについて、ワークスペースの作成からネットワーク保護ステータスの監視まで説明します。

オンプレミスで実行される Kaspersky Security Center の導入の情報については、Kaspersky Security Center のオンラインヘルプを参照してください。

このシナリオの完了には少なくとも 1 営業日を割り当てることを推奨します。

このシナリオでは、次の内容について説明します：

- 会社のワークスペースで管理者として作業を開始する
- ネットワーク上のデバイスを検出する（必要に応じてディストリビューションポイントを割り当て、配布パッケージを手動でインストールする）
- クライアントデバイスに管理対象カスペルスキー製品を導入する：ネットワーク保護と監視のためのツールの設定、定義データベース、ソフトウェアモジュール、カスペルスキー製品の定期的なアップデート

このシナリオを完了すると、カスペルスキー製品によるネットワーク保護が設定されます。ネットワーク保護ステータスの監視を開始できます。

必須条件

開始する前に：

- Kaspersky Security Center Cloud コンソールのアーキテクチャを確認して、主要な製品コンポーネント間の通信を理解します。
- Kaspersky Security Center Cloud コンソールと管理対象アプリケーションに関する情報を読みます。
- Kaspersky Security Center Cloud コンソールの有効なアクティベーションコードがあることを確認します（製品版のワークスペースを作成する場合）。

実行するステップ

Kaspersky Security Center Cloud コンソールの設定は段階的に進行します：

1. **ポートの設定**

   ネットワークとカスペルスキーのインフラストラクチャ間の通信用に、必要なすべてのポートが開かれていることを確認します。また、管理サーバーの階層を使用する場合は、セカンダリ管理サーバーとクライアントデバイス間の通信用に、必要なすべてのポートが開かれていることを確認します。

2. **会社用のワークスペースの作成**

   アカウントを作成してから、会社のワークスペースを作成します。

3. **クイックスタートウィザードの実行**

   Kaspersky Security Center Cloud コンソールを開いてサインインします。初回のログインでは、クイックスタートウィザードの実行が自動的に要求されます。また、クイックスタートウィザードはいつでも手動で起動できます。

クイックスタートウィザードが完了すると、ネットワークエージェントとセキュリティ製品のインストールパッケージを入手できます。Kaspersky Security Center Cloud コンソールの導入を続行するには、これらのインストールパッケージが必要です。

4. **カスペルスキー製品の導入**

   カスペルスキー製品の初期導入シナリオを実行します。シナリオのステップの1つでは、ネットワークポーリング操作を行います。この操作はネットワーク上のクライアントデバイスを検出するために必要です。ネットワークポーリングとその設定については、ネットワーク接続されたデバイスの検出のシナリオで記載されています。

   Kaspersky Security for Windows Server を導入する場合は、この製品のデータベースが最新であることを確認してください。

5. **カスペルスキーのセキュリティ製品へのライセンス付与**

   管理対象デバイスに対するカスペルスキーのセキュリティ製品の導入時には、各製品にアクティベーションコードを適用して、製品にライセンスを付与する必要があります。管理対象デバイスにインストールされているカスペルスキー製品にアクティベーションコードを展開します。カスペルスキーのセキュリティ製品にライセンスを付与するオプションは、いくつかあります。

6. **ネットワーク保護の設定**

   ネットワーク保護の設定を実行し、クイックスタートウィザードで作成されたポリシーとタスクを調整します。

7. **定義データベース、ソフトウェアモジュール、カスペルスキー製品の定期的なアップデート**

   ウイルスなどの脅威からのネットワークの保護を維持するには、定義データベース、ソフトウェアモジュール、カスペルスキー製品の定期的なアップデートを設定する必要があります。

8. **サードパーティ製ソフトウェアのアップデートと脆弱性の修正（任意）**

   Kaspersky Security Center Cloud コンソールでは、クライアントデバイスにインストールされている Microsoft 製品のアップデートを管理できます。必要なアップデートのインストールにより、Microsoft 製品の脆弱性を修正することもできます。

9. **ネットワーク保護ステータスを監視するツールの設定**

   ネットワーク保護ステータスを監視するためのウィジェットやレポートなどのツールを選択し、設定します。

Kaspersky Security Center Cloud コンソールを導入して設定すると、ネットワーク保護ステータスの監視を開始できます。

ワークスペースの管理

このセクションでは、Kaspersky Security Center Cloud コンソールでアカウントとワークスペースを使用する方法について説明します。

Kaspersky Security Center Cloud コンソールでのワークスペース管理について

Kaspersky Security Center Cloud コンソールを使用して、次のことができます：

- アカウントを作成する。
- アカウントを編集する。
- 会社を登録し、ワークスペースを作成する。
- 会社とワークスペースに関する情報を編集する。
- ワークスペースと会社を削除する。
- アカウントを削除する。

Kaspersky Security Center Cloud コンソールの使用を開始する

このセクションでは、Kaspersky Security Center Cloud コンソールにサインアップして使用を開始する方法について説明します。

Kaspersky Security Center Cloud コンソールにサインアップするには、次の手順があります：

1. アカウントの作成と確認。
2. 会社の登録とワークスペースの作成。

アカウントの作成

Kaspersky Security Center Cloud コンソールでアカウントを作成するには：

1. ブラウザーで、 Kaspersky Security Center Cloud コンソールに移動します。
2. Kaspersky Security Center Cloud コンソールのスタートページで［**アカウントの作成**］をクリックします。
3. **カスペルスキーの法人向け製品やサービスにアクセスするためのアカウントを作成する**ページで、アカウントのメールアドレス、パスワード、パスワードの確認を入力します（下図を参照）。

Kaspersky Security Center Cloud コンソールでのアカウントの作成

4. ［**プライバシーポリシー**］をクリックし、プライバシーポリシーの内容をよく確認します。

5. プライバシーポリシーに記載されている通りにデータが処理されて送信される（第三国を含む）ことを理解して同意し、プライバシーポリシーの内容を確認し理解した場合は、プライバシーポリシーに基づくデータ処理への同意のテキストに隣接するチェックボックスをオンにして［**アカウントの作成**］をクリックします。

   プライバシーポリシーに同意しない場合は、Kaspersky Security Center Cloud コンソールを使用しないでください。

   このボタンは、チェックボックスをオンにしないと使用できません。

   メールの確認を促すページが表示されます。カスペルスキーからのメールが、指定したメールアドレスに送信されます。メールには、アカウント作成手順を完了するためのリンクが記載されています。

6. ページを閉じ、メールボックスのメールを開きます。

7. カスペルスキーから送信されたメールのリンクをクリックして、アカウントページに進みます。

8. ［**ユーザーアカウントの有効化**］ページで［**続行**］をクリックして、アカウントの有効化を完了します。

Kaspersky Security Center Cloud コンソールでのアカウントの作成が完了しました。

会社の登録とワークスペースの作成

アカウントが作成されてすぐに、会社を登録してワークスペースを作成できます。

10,000 台を超えるデバイスを保護する場合、以下に説明するように会社を登録して Kaspersky Security Center Cloud コンソールにワークスペースを作成する必要はありません。代わりに、カスペルスキーテクニカルサポートに問い合わせてください。問い合わせには、作成する会社とワークスペースに関する情報を指定します。

現在、登録できる会社は 1 社、作成できるワークスペースは 1 社のみです。Kaspersky Security Center Cloud コンソールの将来のリリースでは、会社用に追加のワークスペースを作成できるようになる予定です。会社の支店ごとに個別のワークスペースを作成することにより、会社の構造をワークスペースにマッピングするのに役立ちます。

開始する前に、次を確認してください：

- ソフトウェア製品を使用する会社の名前。
- その会社が所在する国。会社がアメリカまたはカナダにある場合、州も確認しておく必要があります。
- 保護する会社のコンピューターとモバイルデバイスの総数。

Kaspersky Security Center Cloud コンソールで会社を登録してワークスペースを作成するには：

1. ブラウザーで、 Kaspersky Security Center Cloud コンソールに移動します。

2. Kaspersky Security Center Cloud コンソールのスタートページで［**ログイン**］をクリックします。

3. アカウントの作成時に指定したメールアドレスとパスワードを入力し、［**ログイン**］をクリックします。
   ワークスペースの作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

4. ウィザードの［**ステップ 01：Kaspersky Security Center Cloud コンソールの利用規約**］ページで、次の手順を実行します：

   a. ソフトウェア製品の使用許諾契約書、プライバシーポリシー、およびデータ処理に関する契約書をよくお読みください。

   b. 使用許諾契約書およびデータ処理に関する契約書の条項に同意し、プライバシーポリシーに記載されている通りにデータが処理されて送信される（第三国を含む）ことを理解して同意した場合、プライバシーポリシーを十分に読んで理解し、一覧表示されている 3 つのドキュメントに隣接するチェックボックスをオンにして、［**同意する**］をクリックします。

   条項に同意しない場合は、Kaspersky Security Center Cloud コンソールを使用しないでください。

［**同意しない**］をクリックすると、Kaspersky Security Center Cloud コンソールのワークスペース作成プロセスが終了します。

5. ウィザードの［**ステップ 02：会社情報**］ページで、会社の主な詳細を指定します。

   次のフィールドに値を入力します：

   - **自分の会社名**（必須）

     ソフトウェア製品を使用する会社の名前を指定します。入力できるのは、255 文字までです。使用できる文字列は、大文字と小文字の英数字、空白、ドット、コンマ、マイナス、ダッシュ、アンダースコアです。指定した会社名が Kaspersky Security Center Cloud コンソールに表示されます。

   - **追加の会社説明**フィールド（省略可能）

     登録する会社に関する追加情報を指定できます。入力できるのは、255 文字までです。使用できる文字列は、大文字と小文字の英数字、空白、ドット、コンマ、マイナス、ダッシュ、アンダースコアです。

6. ウィザードの［**ステップ 03：ワークスペース情報**］ページで、会社用に作成するワークスペースに関する情報を指定します。

   次の必要なフィールドに値を入力します：

   - **ワークスペース名**：ソフトウェア製品を使用するワークスペースの名前を指定します。入力できるのは、255 文字までです。使用できる文字列は、大文字と小文字の英数字、空白、ドット、コンマ、マイナス、ダッシュ、アンダースコアです。指定したワークスペース名が Kaspersky Security Center Cloud コンソールに表示されます。

   - **国**：ドロップダウンリストから、ワークスペースが所在する国を選択します。アメリカまたはカナダを選択した場合、このフィールドの下に表示される［**州**］のドロップダウンリストで州も指定します。

   - **デバイスの数**：このワークスペース内で保護するコンピューターとモバイルデバイスの総数を入力します。

     この入力フィールドでは、300 ～ 10,000 の数値を入力できます。

7. ［**ステップ 04：ウィザードの新しいワークスペースのライセンス**］ページで、次のいずれかを実行します：

   - Kaspersky Security Center Cloud コンソールを試す場合は、［**試用ワークスペースをリクエストする**］をクリックします。

     自分のデバイスを試用ワークスペースに接続し、設定の変更をテストして結果を確認することを推奨します。

     アクティベーションコードを入力して試用ワークスペースを製品版に切り替えることはできません。製品版に切り替えるには、ワークスペースを削除して再度作成する必要があります。

   - Kaspersky Security Center Cloud コンソールを製品版で使用する場合は、アクティベーションコードを入力して［**確認**］をクリックします。

Kaspersky Security Center Cloud コンソールでの会社の登録とワークスペースの作成が完了しました。

ワークスペースの準備が完了すると、ワークスペースにアクセスするためのリンクが記載されたメールが届きます。

Kaspersky Security Center Cloud コンソールのワークスペースを開く

Kaspersky Security Center Cloud コンソールのワークスペースを作成するとすぐに、ワークスペースが自動的に開きます。このセクションの説明に従い、後でワークスペースを開くことができます。

仮想管理サーバーの管理者は、仮想管理サーバーにのみアクセスできます。ログインしてワークスペースを開くと、Kaspersky Security Center Cloud コンソールに仮想管理サーバーのインターフェイスが表示されます。プライマリ管理サーバーまたは他のセカンダリ管理サーバーに切り替えることはできません。

仮想管理サーバーの管理者は、単一の仮想管理サーバーにアクセスできる必要があります。プライマリサーバーへのアクセス権がなく、複数の仮想サーバーへのアクセス権がある場合、 Kaspersky Security Center Cloud コンソールにログインできません。

Kaspersky Security Center Cloud コンソールのワークスペースを開くには：

1. ブラウザーで、 Kaspersky Security Center Cloud コンソールに移動します。
2. ユーザー名とパスワードを指定して、Kaspersky Security Center Cloud コンソールのアカウントにログインします。
3. 二段階認証を設定した場合は、SMS で送信されるか、認証アプリで生成されるワンタイムセキュリティコードを入力します（設定した二段階認証方法によって異なります）。

   ポータルのページに、管理者として登録されている会社とそのワークスペースのリストが表示されます。
4. 必要なワークスペースの名前をクリックするか、［**ワークスペースに移動**］をクリックして、ワークスペースに進みます。

   メンテナンスのため、ワークスペースが使用できない場合があります。この場合、Kaspersky Security Center Cloud コンソールのワークスペースに進むことができません。

   削除対象としてマークされているワークスペースを開くことはできません。
5. Kaspersky Security Center Cloud コンソールの法的文書が、ユーザーが条項に同意した後に変更されている場合、ポータルページに変更された文書が表示されます。

   次の手順に従います：

   a. 表示された文書をよくお読みください。

   b. 表示された文書の条項に同意する場合は、一覧表示されている文書に隣接するチェックボックスをオンにして、［**同意する**］をクリックします。

   条項に同意しない場合は、選択したカスペルスキー製品の使用を中止してください。

   ［**同意しない**］をクリックすると、操作が中止されます。

Kaspersky Security Center Cloud コンソールのワークスペースが開きます。

Kaspersky Security Center Cloud コンソールからログアウトする

作業が終了したら、Kaspersky Security Center Cloud コンソールからサインアウトして、現在のセッションをセキュアに閉じる必要があります。

Kaspersky Security Center Cloud コンソールからログアウトするには：

メインメニューで、アカウント設定に移動して、［**ログアウト**］を選択します。

Kaspersky Security Center Cloud コンソールが終了し、アカウントページが表示されます。このブラウザーページは必要に応じて閉じることができます。ワークスペースのすべてのデータが保存されます。

会社とワークスペースのリストの管理

このセクションでは、会社情報とアカウントに登録されているワークスペースのリストを Kaspersky Security Center Cloud コンソールに表示する方法、会社とワークスペースに関する情報を変更する方法、会社とワークスペースを削除する方法について説明します。

現在、登録できる会社は1社、作成できるワークスペースは1社のみです。Kaspersky Security Center Cloud コンソールの将来のリリースでは、会社用に追加のワークスペースを作成できるようになる予定です。会社の支店ごとに個別のワークスペースを作成することにより、会社の構造をワークスペースにマッピングするのに役立ちます。

会社とワークスペースに関する情報の編集

Kaspersky Security Center Cloud コンソールに会社を追加した時に、指定した会社とワークスペースに関する情報を変更できます。

会社とワークスペースに関する情報を編集するには：

1. ブラウザーで、 Kaspersky Security Center Cloud コンソール に移動します。
2. ユーザー名とパスワードを指定して、Kaspersky Security Center Cloud コンソールのアカウントにログインします。
3. 二段階認証を設定した場合は、SMS で送信されるか、認証アプリで生成されるワンタイムセキュリティコードを入力します（設定した二段階認証方法によって異なります）。
   ポータルのページに、管理者として登録されている会社とそのワークスペースのリストが表示されます。
4. 会社名と説明を編集するには、次の手順を実行します：
   a. 会社情報が示されている領域にある［**編集**］（）アイコンをクリックします。
   b. 必要に応じて、会社名や説明を編集します。
   c. ［**保存**］をクリックします。
      変更を取り消すには、［**キャンセル**］をクリックします。

5. ワークスペースの名前を編集するには、次の手順を実行します：

   a. ワークスペース情報が示されている領域にある［**編集**］（）アイコンをクリックします。

   b. 必要に応じてワークスペース名を変更します。

   c. ［**保存**］をクリックします。
   変更を取り消すには、［**キャンセル**］をクリックします。

変更された情報は、Kaspersky Security Center Cloud コンソールに表示されます。

ワークスペースと会社の削除

会社のワークスペースは、手動または自動で削除できます。最後のワークスペースが削除されると、会社情報も自動的に削除されます。

手動削除

会社がワークスペースの使用停止を決定した場合、その会社のワークスペースを削除できます。

ワークスペースが削除された後、すべてのセキュリティ製品は管理対象デバイスに残ります。そのため、ワークスペースを削除する前に、すべてのセキュリティ製品のパスワード保護を無効にするか、管理対象デバイスからセキュリティ製品をアンインストールしてください。

ワークスペースと会社を削除するには：

1. ブラウザーで、 Kaspersky Security Center Cloud コンソールに移動します。
2. ユーザー名とパスワードを指定して、Kaspersky Security Center Cloud コンソールのアカウントにログインします。
3. 二段階認証を設定した場合は、SMS で送信されるか、認証アプリで生成されるワンタイムセキュリティコードを入力します（設定した二段階認証方法によって異なります）。
   ポータルのページに、管理者として登録されている会社とそのワークスペースのリストが表示されます。
4. 削除するワークスペースを選択します。
5. 右側の、選択したワークスペースを含むセクションで、［**削除**（）］アイコンをクリックします。
   ［**ワークスペースの削除**］ウィンドウが表示されます。
6. ［**ワークスペースの削除**］ウィンドウで、ワークスペースを削除することを確認します。

ワークスペースに削除対象としてマークされます。ワークスペースの情報ブロックが赤い枠で強調表示されます。

ワークスペースの情報ブロックは、ページの下部の［**削除対象としてマーク**］セクションに複製されます。

削除対象としてマークされているワークスペースに移動して管理することはできません。

ワークスペースに削除対象としてマークできなかった場合は、カスペルスキーのテクニカルサポートにお問い合わせください。カスペルスキーのテクニカルサポートエンジニアがお問い合わせを受け取った後、会社とワークスペースが削除されます。

削除対象としてマークされたワークスペースは、マークされてから 7 日間、そのステータスのままになる場合があります。7 日後、それらは自動的に削除されます。

その間、削除対象としてマークされているワークスペースを強制的に削除するか、ワークスペースの削除をキャンセルできます。

ワークスペースを強制的に削除するには：

1. ブラウザーで、 Kaspersky Security Center Cloud コンソールに移動します。
2. ユーザー名とパスワードを指定して、Kaspersky Security Center Cloud コンソールのアカウントにログインします。
3. 二段階認証を設定した場合は、SMS で送信されるか、認証アプリで生成されるワンタイムセキュリティコードを入力します（設定した二段階認証方法によって異なります）。

   ポータルのページに、管理者として登録されている会社とそのワークスペースのリストが表示されます。
4. ［**削除対象としてマーク**］セクションの削除対象としてマークされたワークスペースの情報ブロックで、［**強制削除**］をクリックします。

   ［**ワークスペースの削除**］ウィンドウが表示されます。
5. ［**ワークスペースの削除**］ウィンドウで、削除するワークスペースの ID を入力します。

   誤ってワークスペースを削除しようとしていないことを確認するため、ワークスペースの ID を確認するように要求されます。削除したワークスペースは復元できません。

   ワークスペースの ID は、ワークスペースの名前の下のワークスペース情報セクションに表示されます。
6. ［**ワークスペースの削除**］ウィンドウで、［**OK**］をクリックします。

ワークスペースが削除されます。ユーザー、管理対象デバイス、およびそれらの設定に関するすべてのデータが削除されます。

自動削除

Kaspersky Security Center Cloud コンソールは、次の場合にワークスペースを自動的に削除します：

- 試用版ライセンスの有効期限が切れてから 30 日後
- 管理サーバー リポジトリのすべての製品版ライセンスまたは定額制サービスのライセンスの有効期限が切れてから 90 日後
- リポジトリに手動で追加された最後のライセンス（現在のライセンス、予備のライセンス、または使用されていないライセンス）を削除してから 90 日後

Kaspersky Security Center Cloud コンソールは、削除の 30 日前、7 日前、および 1 日前にワークスペースの管理者に通知します。

ワークスペースの削除のキャンセル

削除対象としてマークされているワークスペースの削除をキャンセルできます。

既に削除されたワークスペースの削除はキャンセルできません。

ワークスペースの削除をキャンセルするには：

1. ブラウザーで、 Kaspersky Security Center Cloud コンソールに移動します。
2. ユーザー名とパスワードを指定して、Kaspersky Security Center Cloud コンソールのアカウントにログインします。
3. 二段階認証を設定した場合は、SMS で送信されるか、認証アプリで生成されるワンタイムセキュリティコードを入力します（設定した二段階認証方法によって異なります）。

   ポータルのページに、管理者として登録されている会社とそのワークスペースのリストが表示されます。
4. ［**削除対象としてマーク**］セクションの、削除対象としてマークされたワークスペースの情報ブロックで、［**削除のキャンセル**］をクリックします。

ワークスペースの削除がキャンセルされました。ワークスペースに移動して作業を続けられます。

会社とそのワークスペースへのアクセスの管理

このセクションでは、会社とそのワークスペースへのアクセスの許可と取り消しに関して説明します。

Kaspersky Security Center Cloud コンソールには、次の 2 つのアクセスレベルがあります。

- **管理者**

  このアクセスレベルを持つユーザーは、会社とそのワークスペースを完全に管理できます。
- **ユーザー**

  このアクセスレベルを持つユーザーは、使用可能なワークスペースのリストを表示し、これらのワークスペースに入ることができます。

会社とそのワークスペースへのアクセス権の付与

別のユーザーが会社にログインして、選択したアクセスレベルに従って会社を管理できるようにするには、会社とそのワークスペースへのアクセスを許可します。

ユーザーにアクセスを許可する前に、ユーザーは Kaspersky Security Center Cloud コンソールでアカウントを作成する必要があります。

会社とそのワークスペースへのアクセス権を付与するには：

1. ブラウザーで、 Kaspersky Security Center Cloud コンソールに移動します。
2. ユーザー名とパスワードを指定して、Kaspersky Security Center Cloud コンソールのアカウントにログインします。

3. 二段階認証を設定した場合は、SMS で送信されるか、認証アプリで生成されるワンタイムセキュリティコードを入力します（設定した二段階認証方法によって異なります）。

   ポータルのページに、管理者として登録されている会社とそのワークスペースのリストが表示されます。

4. ［**アクセス権管理を表示する**］をクリックします。

   会社にアクセス可能なアカウントのリストが展開されます。

5. ［**アクセスの許可**］をクリックします。

6. ［**メールアドレス**］で、アクセスを許可するアカウントのメールアドレスを指定します。

7. **アクセスレベル**で、入力したアカウントに割り当てるアクセスレベルを選択します：

   - **管理者**

     このアクセスレベルを持つユーザーは、会社とそのワークスペースを完全に管理できます。

   - **ユーザー**

     このアクセスレベルを持つユーザーは、使用可能なワークスペースのリストを表示し、これらのワークスペースに入ることができます。

   同じ会社内の同じアカウントに複数のアクセスレベルを付与することはできません。

8. ［**アクセス権を付与**］をクリックします。

指定されたアカウントに会社とそのワークスペースへのアクセスが許可されます。ユーザーは、会社にログインして選択したアクセスレベルに従って会社を管理できます。

アカウントに**ユーザー**アクセスレベルを付与した場合は、追加したユーザーにロールを割り当てる必要があります。ロールを割り当てないと、ユーザーはワークスペースに入ることができません。

会社とそのワークスペースへのアクセスの取り消し

ユーザーが会社にログインして管理できないようにする場合に（たとえば、ユーザーの退職後など）、会社とそのワークスペースへのアクセス権を取り消すことができます。

自分自身の会社へのアクセス権を取り消すことはできません。

会社とそのワークスペースへのアクセス権を取り消すには：

1. ブラウザーで、 Kaspersky Security Center Cloud コンソール に移動します。

2. ユーザー名とパスワードを指定して、Kaspersky Security Center Cloud コンソールのアカウントにログインします。

3. 二段階認証を設定した場合は、SMS で送信されるか、認証アプリで生成されるワンタイムセキュリティコードを入力します（設定した二段階認証方法によって異なります）。

   ポータルのページに、管理者として登録されている会社とそのワークスペースのリストが表示されます。

4. ［**アクセス権管理を表示する**］をクリックします。
   会社にアクセス可能なアカウントのリストが展開されます。

5. アクセスを取り消すアカウントの横にある**取り消し**（）アイコンをクリックします。

6. ［**会社へのアクセス権の取り消し**］ウィンドウで、［**OK**］をクリックして操作を完了します。

選択したアカウントの、会社とワークスペースへのアクセスが取り消されます。ユーザーは会社にログインして管理することはできなくなります。

パスワードのリセット

Kaspersky Security Center Cloud コンソールアカウントのパスワードを忘れた場合は、パスワードをリセットすることで、アカウントへのアクセスを復元できます。

アカウントのパスワードをリセットするには：

1. ブラウザーで、Kaspersky Security Center Cloud コンソールに移動します。

2. ［**ログイン**］をクリックし、［**パスワードをお忘れですか？**］をクリックします。

3. アカウントの作成時に指定したメールアドレスを入力します。

4. ［**パスワードをリセット**］をクリックします。
   パスワードをリセットするためのリンクが記載されたメールが、指定したアドレスに送信されます。

5. メールのリンクをクリックします。

6. 表示されたウィンドウで、新しいパスワードを入力して確認します。

7. 秘密の質問を設定した場合は、その質問に答えてください。
   二段階認証を設定した場合は、SMS で送信されるか、認証アプリで生成されるワンタイムセキュリティコードを入力します（設定した二段階認証方法によって異なります）。

8. ［**続行**］をクリックします。
   Kaspersky Security Center Cloud コンソールにログインするための新しいパスワードが保存されます。

メールを受信しなかった場合は、入力したメールアドレスや迷惑メールフォルダーを確認してから、再度行ってください。再度行ってもメールが受信されない場合は、指定したメールアドレスが Web サイトに登録されていない可能性があります。カスペルスキーのテクニカルサポートにお問い合わせください。

Kaspersky Security Center Cloud コンソールでのアカウント設定の編集

このセクションでは、Kaspersky Security Center Cloud コンソールでアカウントの編集や削除の方法について説明します。

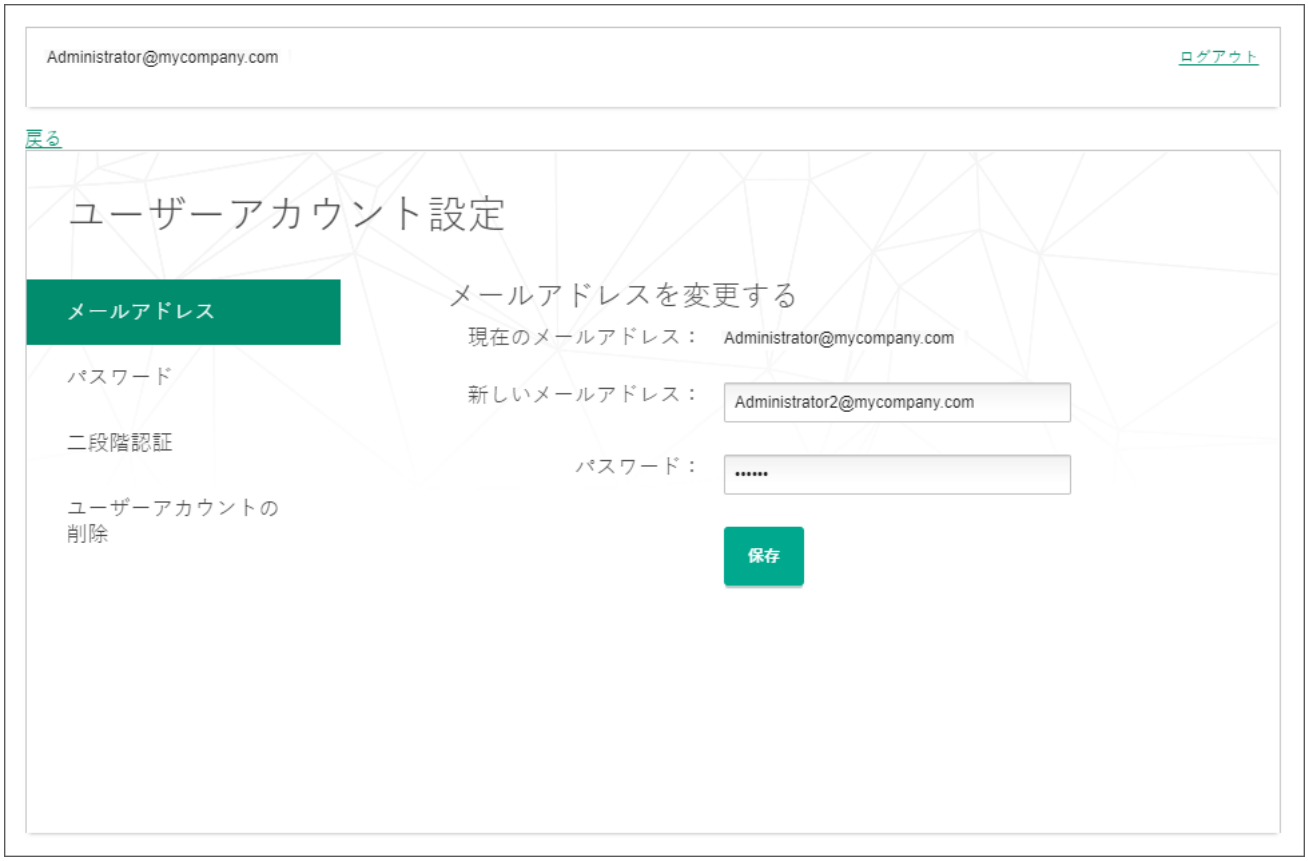
メールアドレスの変更

Kaspersky Security Center Cloud コンソールのアカウントの設定でメールアドレスを変更するには：

1. Kaspersky Security Center Cloud コンソールで、アカウント名を含むリンクをクリックし、［**ユーザーアカウントの管理**］を選択します。

   ［**ユーザーアカウントの設定**］ウィンドウが表示されます。

2. ［**メールアドレス**］セクションを選択します（下図を参照）。



Kaspersky Security Center Cloud コンソールのアカウントの設定でのメールアドレスの変更

［**メールアドレス**］セクションには、現在のメールアドレス、新しいアドレスを入力するための入力フィールド、パスワードを入力するための入力フィールド、および［**保存**］ボタンが表示されます。

3. ［**新しいメールアドレス**］に、新しいメールを入力します。

   アドレスは正しく入力してください。無効なアドレスを入力すると、アカウントに進めず、Kaspersky Security Center Cloud コンソールを使用できなくなります。

4. ［**パスワード**］入力フィールドに、現在のパスワードを入力します。

5. ［**保存**］をクリックします。

6. ［**戻る**］をクリックして Kaspersky Security Center Cloud コンソールに戻るか、［**ログアウト**］をクリックしてポータルを終了します。

これで、Kaspersky Business Hub Kaspersky Security Center Cloud コンソールアカウント設定とマイ カスペルスキー アカウント設定でメールアドレスが変更されました。アカウントアクセス用のメールアドレスが変更されたことを通知するメールが新しいメールアドレスに送信されます。次回の Kaspersky Security Center Cloud コンソールへのログイン時に、新しいメールアドレスを指定する必要があります。

パスワードの変更

Kaspersky Security Center Cloud コンソールアカウントの設定でパスワードを変更するには：

1. Kaspersky Security Center Cloud コンソールで、アカウント名を含むリンクをクリックし、［**ユーザーアカウントの管理**］を選択します。

   ［**ユーザーアカウントの設定**］ウィンドウが表示されます。

2. ［**パスワード**］セクションを選択します（下図を参照）。

Kaspersky Security Center Cloud コンソールでのアカウントのパスワードの変更

   このセクションには、新しいパスワードを入力して確認するためのフィールドと、［**変更の保存**］ボタンが表示されます。

3. 新しいパスワードを入力し、各入力フィールドで確認します。

   パスワード入力フィールドの右側に、パスワードの要件が表示されます。要件に準拠するまで、新しいパスワードを保存できません。

4. ［**パスワードの変更を 180 日 ごとにリクエストする**］をオンまたはオフにします。

   既定では、このチェックボックスはオンです。

5. ［**変更の保存**］をクリックします。

6. ［**戻る**］をクリックして Kaspersky Security Center Cloud コンソールに戻るか、［**ログアウト**］をクリックしてポータルを終了します。

これでパスワードが変更されました。Kaspersky Security Center Cloud コンソールへのログイン時や、マイカスペルスキー へのログイン時に、新しいパスワードを入力する必要があります。

二段階認証の使用

このセクションでは、Kaspersky Security Center Cloud コンソールのアカウントのセキュリティの強化に効果的な二段階認証について説明します。

二段階認証の概要

二段階認証は、Kaspersky Security Center Cloud コンソールでのアカウントのセキュリティを強化するのに効果的です。この機能を有効にすると、メールアドレスとパスワードを使用して Kaspersky Security Center Cloud コンソールにログインするたびに、追加のワンタイムセキュリティコードの入力が必要になります。二段階認証では、犯罪者はパスワードを盗んだり推測したりしても、アカウントにログインできません。携帯電話にもアクセスできなければなりません。また、二段階認証が有効になっている状態でパスワードを忘れた場合は、追加のワンタイムセキュリティコードを入力する必要があります。

二段階認証の設定後は、携帯電話を物理的に安全に保ち、電話番号へアクセスできるようにしておく必要があります。

ワンタイムセキュリティコードを取得するには、次のいずれかの方法で行います：

- セキュリティコードが SMS で携帯電話番号に送信されます。

  この場合、携帯電話にアクセスできなくなった場合、電話番号へのアクセスを復元するまで、Kaspersky Security Center Cloud コンソールでアカウントにサインインすることはできません。

- セキュリティコードは、携帯電話にインストールされている認証アプリで生成されます。

  認証アプリを使用して二段階認証を設定することを、強く推奨します。この場合、携帯電話がインターネットまたはモバイルネットワークに接続されていなくても、アカウントにログインできます。

  Kaspersky Security Center Cloud コンソールとの互換性については、Google Authenticator と Microsoft Authenticator のみをテストしており、これらのアプリケーションはその時点で無料で使用できました。アプリケーションのインターフェイスは、ご希望の言語では使用できない場合があります。アプリケーションを使用する前に、アプリケーションの GDPR コンプライアンスとプライバシーポリシーも確認してください。カスペルスキーは、これらのアプリケーションの所有者による支援や推薦は受けておらず、提携もしておりません。

  > Microsoft Authenticator は、モバイルデバイスにのみインストールできます。

  携帯電話以外のデバイスにも認証アプリをインストールしてください。これにより、携帯電話を紛失したり盗まれたりした場合に、アカウントにログインできます。

  この場合、携帯電話にアクセスできず、別のデバイスに認証システムアプリがない場合、電話番号へのアクセスを復元するまで、Kaspersky Security Center Cloud コンソールでアカウントにサインインすることはできません。その後、SMS で送信されたセキュリティコードを使用します。

> パスワードを紛失した場合にパスワードを復元するために秘密の質問を事前に設定していた場合、二段階認証を設定すると、秘密の質問機能はその後無効になります。

シナリオ：二段階認証の設定

二段階認証は、Kaspersky Security Center Cloud コンソールでのアカウントのセキュリティを強化するのに効果的です。このセクションで説明するシナリオを実行して、アカウントの二段階認証を設定します。

このシナリオは段階的に進行します：

1. **電話番号の追加**

   この段階で、SMS による二段階認証を設定します。

2. **認証アプリのインストールと設定**

   認証アプリをインストールして設定します。

   認証アプリを使用して二段階認証を設定することを、強く推奨します。この場合、携帯電話がインターネットまたはモバイルネットワークに接続されていなくても、アカウントにログインできます。

   携帯電話以外のデバイスにも認証アプリをインストールしてください。これにより、携帯電話を紛失したり盗まれたりした場合に、アカウントにログインできます。

3. **電話番号の変更**

   必要に応じて、二段階認証に使用する電話番号を変更できます。

SMS による二段階認証の設定

SMS による二段階認証を設定するには：

1. Kaspersky Security Center Cloud コンソールで、アカウント名を含むリンクをクリックし、［**ユーザーアカウントの管理**］を選択します。

   ［**ユーザーアカウントの設定**］ウィンドウが表示されます。

2. ［**二段階認証**］セクションを選択します。

3. ［**設定**］ボタンをクリックします。

4. ［**現在のパスワードを入力**］に、Kaspersky Security Center Cloud コンソールのアカウントのパスワードを指定し、［**継続**］をクリックします。

5. ［**携帯電話番号を指定**］で、二段階認証で使用する携帯電話番号を指定し、［**次へ**］をクリックします。

   > 最大 5 つのアカウントに同じ電話番号を使用できます。

   6 桁のセキュリティコードが指定の電話番号に送信されます。

6. ［**電話番号の確認**］で、受信したセキュリティコードを入力します。

二段階認証が設定されます。これで、メールアドレスとパスワードでログインするたび、またはパスワードを忘れた場合に、指定した電話番号に SMS で取得するワンタイムセキュリティコードの入力が必要とされるようになります。

認証アプリのインストールと設定、電話番号の変更、二段階認証の無効化ができるようになりました。

認証アプリを使用した二段階認証の設定

認証アプリは、Kaspersky Security Center Cloud コンソールでスタンドアロンの認証方法として使用することはできません。最初に SMS による二段階認証を設定する必要があります。携帯電話番号による二段階認証を無効にすると、認証アプリによる認証は自動的にオフになります。SMS とアプリの両方による認証を設定すると、ログインページで、またはパスワードを忘れた場合に認証方法を選択できるようになります。

認証アプリによる二段階認証を設定するには：

1. SMS による二段階認証を設定します。

2. 使用する認証アプリをダウンロードしてインストールし、実行します。

   Kaspersky Security Center Cloud コンソールとの互換性については、Google Authenticator と Microsoft Authenticator のみをテストしており、これらのアプリケーションはその時点で無料で使用できました。アプリケーションのインターフェイスは、ご希望の言語では使用できない場合があります。アプリケーションを使用する前に、アプリケーションの GDPR コンプライアンスとプライバシーポリシーも確認してください。カスペルスキーは、これらのアプリケーションの所有者による支援や推薦は受けておらず、提携もしておりません。

   > Microsoft Authenticator は、モバイルデバイスにのみインストールできます。

   必要に応じて、自己責任で他のアプリを使用できます。使用するアプリは、6 桁のセキュリティコードに対応している必要があります。

   携帯電話以外のデバイスにも認証アプリをインストールしてください。これにより、携帯電話を紛失したり盗まれたりした場合に、アカウントにログインできます。

3. Kaspersky Security Center Cloud コンソールで、アカウント名を含むリンクをクリックし、［**ユーザーアカウントの管理**］を選択します。

   ［**ユーザーアカウントの設定**］ウィンドウが表示されます。

4. ［**二段階認証**］セクションを選択します。

5. ［**秘密鍵の取得**］をクリックします。

6. ［**現在のパスワードを入力**］に、Kaspersky Security Center Cloud コンソールのアカウントのパスワードを指定し、［**継続**］をクリックします。

   ポータルページには、16 文字の秘密鍵と QR コードが表示されます。

7. 各デバイスの認証アプリで、アカウントを作成し、表示された秘密鍵を入力します。あるいは、携帯電話で QR コードをスキャンすることもできます。この場合、アカウントは自動的に作成されます。詳細については、アプリのドキュメントを参照してください。

   認証アプリで 6 桁のセキュリティコードが生成されます。

8. アプリで生成されたセキュリティコードが各デバイスで同じであることを確認します。

9. Kaspersky Security Center Cloud コンソールで、生成されたセキュリティコードを入力します。

認証アプリによる二段階認証が設定されました。これで、メールアドレスとパスワードでログインするたびに、またはパスワードを忘れた場合は、認証アプリで生成されるワンタイムセキュリティコードを入力する必要があります。

認証アプリの使用を無効にするか、二段階認証を完全に無効にすることができます。

携帯電話番号の変更

SMS による二段階認証で使用される携帯電話番号を変更するには：

1. Kaspersky Security Center Cloud コンソールで、アカウント名を含むリンクをクリックし、［**ユーザーアカウントの管理**］を選択します。

   ［**ユーザーアカウントの設定**］ウィンドウが表示されます。

2. ［**二段階認証**］セクションを選択します。

3. ［**電話番号**］で、［**電話番号を変更**］をクリックします。

4. ［**携帯電話番号を指定**］で、二段階認証で使用する新しい携帯電話番号を指定し、［**次へ**］をクリックします。

5. ［**現在のパスワードを入力**］に、Kaspersky Security Center Cloud コンソールのアカウントのパスワードを指定し、［**継続**］をクリックします。

   6 桁のセキュリティコードが指定の電話番号に送信されます。

6. ［**電話番号の確認**］で、受信したセキュリティコードを入力します。

携帯電話番号が変更されました。これで、ワンタイムセキュリティコードが新しい電話番号に送信されます。

二段階認証の無効化

二段階認証を使用したくない場合は、二段階認証を無効にすることができます。このセクションでは、その方法を説明します。

二段階認証プロセスを無効にすると、アカウントのセキュリティが低下します。二段階認証を引き続き使用することを強く推奨します。

SMS による二段階認証を設定している場合は、二段階認証を無効にすることができます。認証アプリによる二段階認証を設定している場合、アプリの使用を無効にするか、二段階認証を完全に無効にすることができます。

認証アプリの使用を無効にするには：

1. Kaspersky Security Center Cloud コンソールで、アカウント名を含むリンクをクリックし、［**ユーザーアカウントの管理**］を選択します。

   ［**ユーザーアカウントの設定**］ウィンドウが表示されます。

2. ［**二段階認証**］セクションを選択します。

3. ［**認証アプリ**］で、［**認証アプリの使用を無効にする**］をクリックします。

4. ［**現在のパスワードを入力**］に、Kaspersky Security Center Cloud コンソールのアカウントのパスワードを指定し、［**継続**］をクリックします。

認証アプリの使用が無効になりました。認証アプリによる二段階認証の設定を削除しました。認証アプリのアカウントを削除できるようになりました。

後で、認証アプリによる二段階認証を再度設定することができます。

二段階認証を完全に無効にするには：

1. Kaspersky Security Center Cloud コンソールで、アカウント名を含むリンクをクリックし、［**ユーザーアカウントの管理**］を選択します。

   ［**ユーザーアカウントの設定**］ウィンドウが表示されます。

2. ［**二段階認証**］セクションを選択します。

3. ［**電話番号**］で、［**二段階認証を無効にする**］をクリックします。

4. ［**現在のパスワードを入力**］に、Kaspersky Security Center Cloud コンソールのアカウントのパスワードを指定し、［**継続**］をクリックします。

二段階認証は無効になりました。認証アプリによる二段階認証を使用していた場合、二段階認証の設定は削除されます。認証アプリのアカウントを削除できるようになりました。

後で、二段階認証を再度設定することができます。

Kaspersky Security Center Cloud コンソールでのアカウントの削除

Kaspersky Security Center Cloud コンソールの使用を停止する場合は、アカウントを削除できます。

アカウントを削除すると、そのアカウントに関連付けられているすべてのデータが失われます。

アカウントを削除すると、Kaspersky Endpoint Security Cloud、Kaspersky Security for Microsoft Office 365、および Kaspersky Security Center Cloud コンソールのワークスペースにアクセスできなくなります。削除したアカウントがワークスペースの唯一の管理者であった場合、ワークスペースは削除されます。さらに、マイ カスペルスキーのアカウントにアクセスできなくなります。

Kaspersky Security Center Cloud コンソールでアカウントを削除するには：

1. Kaspersky Security Center Cloud コンソールで、アカウント名を含むリンクをクリックし、［**ユーザーアカウントの管理**］を選択します。

   ［**ユーザーアカウントの設定**］ウィンドウが表示されます。

2. ［**ユーザーアカウントの削除**］セクションを選択します。

   ［**アカウントの削除**］セクションには、アカウントを削除した結果に関する情報と、その情報の下に［**削除**］ボタンが表示されます。

3. アカウントの削除に関する情報を確認し、［**削除**］をクリックしてください。

   ［**ユーザーアカウントのパスワードを入力**］ウィンドウが表示されます。

4. パスワード入力フィールドにパスワードを入力し、［**続行**］ボタンをクリックします。

アカウントが削除されます。

Kaspersky Security Center Cloud コンソールの情報の保存に使用されるデータセンターの選択

Kaspersky Security Center Cloud コンソールのワークスペースは、Microsoft Azure クラウドプラットフォームに基づくグローバルデータセンターのネットワークのサーバーを使用して作成されます。ワークスペースをホスティングするデータセンターの選択は、Kaspersky Security Center Cloud コンソールにワークスペースを登録した時に指定した国によって異なります（以下の表を参照）。セキュリティ製品の配布パッケージは、ワークスペースと同じサーバーにホスティングされます。

会社の場所と Microsoft Azure のリージョンを一致させる

会社が所在する国	Microsoft データセンターのリージョン
アルゼンチン	ブラジル南部
ボリビア	ブラジル南部
ブラジル	ブラジル南部
チリ	ブラジル南部
コロンビア	ブラジル南部
エクアドル	ブラジル南部
ガイアナ	ブラジル南部
ペルー	ブラジル南部
パラグアイ	ブラジル南部
スリナム	ブラジル南部
ウルグアイ	ブラジル南部
ベネズエラ	ブラジル南部
アンティグア・バーブーダ	アメリカ東部
アンギラ	アメリカ東部
アルバ	アメリカ東部
バルバドス	アメリカ東部
サン・バルテルミー島	アメリカ東部
ボネール、シント・ユースタティウスおよびサバ	アメリカ東部
ベリーズ	アメリカ東部
コスタリカ	アメリカ東部
キューバ	アメリカ東部
キュラソー島	アメリカ東部
ドミニカ	アメリカ東部
ドミニカ共和国	アメリカ東部
グレナダ	アメリカ東部
グアドループ	アメリカ東部
グアテマラ	アメリカ東部
ホンジュラス	アメリカ東部
ハイチ	アメリカ東部
ジャマイカ	アメリカ東部
セントクリストファー・ネイビス	アメリカ東部

ケイマン諸島	アメリカ東部
セントルシア	アメリカ東部
セント・マーチン島	アメリカ東部
マルティニーク	アメリカ東部
モントセラト	アメリカ東部
ニカラグア	アメリカ東部
パナマ	アメリカ東部
プエルトリコ	アメリカ東部
シントマールテン	アメリカ東部
トリニダード・トバゴ	アメリカ東部
セントビンセントおよびグレナディーン諸島	アメリカ東部
イギリス領ヴァージン諸島	アメリカ東部
アメリカ領ヴァージン諸島	アメリカ東部
日本	アメリカ東部
カナダ（ニューブランズウィック州）	アメリカ東部
カナダ（ニューファンドランド・ラブラドール州）	アメリカ東部
カナダ（ノバスコシア州）	アメリカ東部
カナダ（オンタリオ州）	アメリカ東部
カナダ（プリンスエドワードアイランド州）	アメリカ東部
カナダ（ケベック州）	アメリカ東部
アメリカ合衆国（アラバマ州）	アメリカ東部
アメリカ合衆国（アーカンソー州）	アメリカ東部
アメリカ合衆国（コネチカット州）	アメリカ東部
アメリカ合衆国（コロンビア特別区）	アメリカ東部
アメリカ合衆国（デラウェア州）	アメリカ東部
アメリカ合衆国（フロリダ州）	アメリカ東部
アメリカ合衆国（ジョージア州）	アメリカ東部
アメリカ合衆国（アイオワ州）	アメリカ東部
アメリカ合衆国（イリノイ州）	アメリカ東部
アメリカ合衆国（インディアナ州）	アメリカ東部
アメリカ合衆国（ケンタッキー州）	アメリカ東部
アメリカ合衆国（ルイジアナ州）	アメリカ東部
アメリカ合衆国（マサチューセッツ州）	アメリカ東部
アメリカ合衆国（メリーランド州）	アメリカ東部
アメリカ合衆国（メイン州）	アメリカ東部
アメリカ合衆国（ミシガン州）	アメリカ東部

アメリカ合衆国（ミネソタ州）	アメリカ東部
アメリカ合衆国（ミズーリ州）	アメリカ東部
アメリカ合衆国（ミシシッピ州）	アメリカ東部
アメリカ合衆国（ノースカロライナ州）	アメリカ東部
アメリカ合衆国（ニューハンプシャー州）	アメリカ東部
アメリカ合衆国（ニュージャージー州）	アメリカ東部
アメリカ合衆国（ニューヨーク州）	アメリカ東部
アメリカ合衆国（オハイオ州）	アメリカ東部
アメリカ合衆国（ペンシルベニア州）	アメリカ東部
アメリカ合衆国（ロードアイランド州）	アメリカ東部
アメリカ合衆国（サウスカロライナ州）	アメリカ東部
アメリカ合衆国（テネシー州）	アメリカ東部
アメリカ合衆国（バージニア州）	アメリカ東部
アメリカ合衆国（バーモント州）	アメリカ東部
アメリカ合衆国（ウィスコンシン州）	アメリカ東部
アメリカ合衆国（ウェストバージニア州）	アメリカ東部
アルバニア	北ヨーロッパ（アイルランド）
ボスニア・ヘルツェゴビナ	北ヨーロッパ（アイルランド）
ブルガリア	北ヨーロッパ（アイルランド）
ベラルーシ	北ヨーロッパ（アイルランド）
チェコ共和国	北ヨーロッパ（アイルランド）
デンマーク	北ヨーロッパ（アイルランド）
エストニア	北ヨーロッパ（アイルランド）
フィンランド	北ヨーロッパ（アイルランド）
イギリス	北ヨーロッパ（アイルランド）
グリーンランド	北ヨーロッパ（アイルランド）
ギリシャ	北ヨーロッパ（アイルランド）
クロアチア	北ヨーロッパ（アイルランド）
ハンガリー	北ヨーロッパ（アイルランド）
アイルランド	北ヨーロッパ（アイルランド）
アイスランド	北ヨーロッパ（アイルランド）
キルギスタン	北ヨーロッパ（アイルランド）
カザフスタン	北ヨーロッパ（アイルランド）
リトアニア	北ヨーロッパ（アイルランド）
ラトビア	北ヨーロッパ（アイルランド）
モルドバ	北ヨーロッパ（アイルランド）

モンテネグロ	北ヨーロッパ（アイルランド）
マケドニア共和国	北ヨーロッパ（アイルランド）
モンゴル	北ヨーロッパ（アイルランド）
ノルウェー	北ヨーロッパ（アイルランド）
ポーランド	北ヨーロッパ（アイルランド）
ルーマニア	北ヨーロッパ（アイルランド）
セルビア	北ヨーロッパ（アイルランド）
ロシア連邦	北ヨーロッパ（アイルランド）
スウェーデン	北ヨーロッパ（アイルランド）
スロベニア	北ヨーロッパ（アイルランド）
スロバキア	北ヨーロッパ（アイルランド）
タジキスタン	北ヨーロッパ（アイルランド）
トルクメニスタン	北ヨーロッパ（アイルランド）
ウズベキスタン	北ヨーロッパ（アイルランド）
カナダ（アルバータ州）	アメリカ西部
カナダ（ブリティッシュコロンビア州）	アメリカ西部
カナダ（マニトバ州）	アメリカ西部
カナダ（ノースウエスト準州）	アメリカ西部
カナダ（ヌナブト準州）	アメリカ西部
カナダ（ユーコン準州）	アメリカ西部
カナダ（サスカチュワン州）	アメリカ西部
メキシコ	アメリカ西部
アメリカ合衆国（アラスカ州）	アメリカ西部
アメリカ合衆国（アリゾナ州）	アメリカ西部
アメリカ合衆国（カリフォルニア州）	アメリカ西部
アメリカ合衆国（コロラド州）	アメリカ西部
アメリカ合衆国（ハワイ州）	アメリカ西部
アメリカ合衆国（アイダホ州）	アメリカ西部
アメリカ合衆国（カンザス州）	アメリカ西部
アメリカ合衆国（モンタナ州）	アメリカ西部
アメリカ合衆国（ノースダコタ州）	アメリカ西部
アメリカ合衆国（ネブラスカ州）	アメリカ西部
アメリカ合衆国（ニューメキシコ州）	アメリカ西部
アメリカ合衆国（ネバダ州）	アメリカ西部
アメリカ合衆国（オクラホマ州）	アメリカ西部
アメリカ合衆国（オレゴン州）	アメリカ西部

アメリカ合衆国（サウスダコタ州）	アメリカ西部
アメリカ合衆国（テキサス州）	アメリカ西部
アメリカ合衆国（ユタ州）	アメリカ西部
アメリカ合衆国（ワシントン州）	アメリカ西部
アメリカ合衆国（ワイオミング州）	アメリカ西部
アメリカ合衆国（その他の行政区分）	アメリカ東部
その他の国	西ヨーロッパ（オランダ）

パブリック DNS サーバーへのアクセス

システム DNS を使用してカスペルスキーのサーバーにアクセスできない場合、Kaspersky Security Center Cloud コンソールでは、以下のパブリック DNS サーバーを次の順序で使用できます：

1. Google Public DNS （8.8.8.8）
2. Cloudflare DNS（1.1.1.1）
3. Alibaba Cloud DNS（223.6.6.6）
4. Quad9 DNS（9.9.9.9）
5. CleanBrowsing（185.228.168.168）

ネットワークエージェントが DNS サーバーへの TCP/UDP 接続を確立されているため、これらの DNS サーバーへの要求にはドメインアドレスとクライアントデバイスのパブリック IP アドレスが含まれる場合があります。Kaspersky Security Center Cloud コンソールがパブリック DNS サーバーを使用している場合、データ処理は関連するサービスのプライバシーポリシーによって管理されます。

シナリオ：Kaspersky Security Center Cloud コンソールで管理される管理サーバーの階層の作成

このシナリオでは、Kaspersky Security Center Cloud コンソールで管理される管理サーバーの階層を作成するために実行する必要がある操作について、プライマリ管理サーバーのロールを想定して説明します。作成後、この階層は Kaspersky Security Center から Kaspersky Security Center Cloud コンソールに管理対象デバイスやオブジェクトを移行するために使用できます。また、Kaspersky Security Center Cloud コンソールによるセカンダリ管理サーバーとデバイスの管理にも使用できます。

Kaspersky Security Center Cloud コンソールはプライマリ管理サーバーとしてのみ動作でき、オンプレミスで実行されている管理サーバーはセカンダリ管理サーバーとしてのみ動作できます。その他の階層スキームは利用できません。

必須条件

開始する前に、次の前提条件が満たされていることを確認してください：

- オンプレミスで実行されている管理サーバーがバージョン 12 以降にアップグレードされている。
- オンプレミスで実行されている管理サーバーに Kaspersky Security Center Web コンソールがインストールされている。
- Kaspersky Security Center Cloud コンソールを使用して管理するアプリケーション用の Web プラグインがインストールされている。
- 管理対象アプリケーションが、Kaspersky Security Center Cloud コンソールでサポートされているバージョンにアップグレードされている。
- オンプレミスで実行されている管理サーバーで、管理サーバーのリポジトリへのアップデートのダウンロードタスクにプライマリ管理サーバーがアップデート元として割り当てられていないことを確認し、必要に応じてタスク設定を変更した。

階層の作成後、Kaspersky Security Center Cloud コンソールで有効なポリシーとタスクがセカンダリ管理サーバーに適用され、既存のポリシーとタスクより優先されます。この動作を避けるには、階層の作成前に、Kaspersky Security Center Cloud コンソールに既存のポリシーとタスクを削除します。または、Kaspersky Security Center Cloud コンソールの各ポリシーの設定でステータスを［**非アクティブ**］に変更し、Kaspersky Security Center Cloud コンソールの各タスクの設定で［**セカンダリまたは仮想管理サーバーに配信**］をオフにします。

必要に応じて、いつでも管理サーバーの階層を削除できます。

階層の作成手順

基本的なシナリオでは、インターネット経由でアクセスできないセカンダリ管理サーバーを指定します。ただし、インターネット経由でセカンダリ管理サーバーにアクセスできる場合は、次に説明するステップの一部に含まれる一連の操作が異なる可能性があります。また、この場合はステップの一部を省略する必要があります。

管理サーバーの階層の作成は、次の手順で構成されます：

1. **セカンダリ管理サーバーの証明書の取得**

   インターネット経由でセカンダリ管理サーバーにアクセスできる場合は、このステップを省略します。

   オンプレミスで実行されている Kaspersky Security Center Web コンソールで、管理サーバーのプロパティを開き、［**全般**］タブで［**全般**］セクションを開きます。［**管理サーバー証明書を表示**］をクリックします。CER 形式の証明書ファイルは、ブラウザーの設定で指定したフォルダーに自動的に保存されます。

2. **Kaspersky Security Center Cloud コンソールからの接続設定と証明書の取得**

   インターネット経由でセカンダリ管理サーバーにアクセスできる場合は、このステップを省略します。

   Kaspersky Security Center Cloud コンソールで管理サーバーのプロパティを開き、［**全般**］タブで［**管理サーバーの階層**］セクションを開きます。次の接続設定が表示されます：

   - **HDS (Hosted Discovery Service) アドレス**

     Hosted Discovery Service（HDS）への接続に使用する URL が表示されます。

   - **HDS (Hosted Discovery Service) ポート**

     HDS への接続に使用するポート番号が表示されます。

   このセクションには次の 2 つのリンクも含まれています：

   - **管理サーバー証明書を表示**

     このリンクをクリックすると、Kaspersky Security Center Cloud コンソールインスタンスの証明書の公開鍵のダウンロードが開始されます。

   - **HDS ルート認証局証明書**

     このリンクをクリックすると、認証局（CA）が発行した信頼されたルート証明書のリストを含む pem 形式のファイルのダウンロードが開始されます。このファイルは、セカンダリ管理サーバーが HDS 証明書の検証に使用するために必要です。

   クリップボードの使用など都合のよい方法で、接続設定を手動でコピーして任意の形式のファイルに保存します。［**管理サーバー証明書を表示**］をクリックして、証明書ファイルがダウンロードされるまで待ちます。［**HDS ルート認証局証明書**］をクリックして、認証局が発行した信頼されたルート証明書のリストを含むファイルがダウンロードされるまで待ちます。2 つのファイルはブラウザー設定で指定されているフォルダーに保存されます。

3. **接続用のセカンダリ管理サーバーの選択**

   管理サーバーのプロパティで、［**管理サーバー**］タブに移動します。管理グループの階層で、セカンダリ管理サーバーとそのすべての管理対象デバイスを含める管理グループの横にあるチェックボックスをオンにします。［**セカンダリ管理サーバーの接続**］をクリックします。

   表示されたページで、階層で表示するセカンダリ管理サーバーの名前を［**セカンダリ管理サーバーの表示名**］に指定します。この名前は使いやすさのためにのみ使用されるため、必要に応じて実際のセカンダリ管理サーバー名と異なる名前を指定できます。［**次へ**］をクリックします。

インターネット経由でセカンダリ管理サーバーにアクセスできる場合は、［**セカンダリ管理サーバーアドレス（任意）**］にセカンダリ管理サーバーのアドレスも指定する必要があります。

次のページで［**参照**］をクリックし、セカンダリ管理サーバーから保存した pem ファイルを指定します。［**次へ**］をクリックします。

4 プロキシサーバーの有効化と設定

このステップで説明されている操作は任意です。接続でプロキシサーバーを使用する必要がある場合のみ実行してください。

［**次へ**］をクリックします。［**セカンダリ管理サーバーをプライマリ管理サーバーに接続する方法の定義**］ページで、必要に応じてプロキシサーバーの使用を有効にして設定できます。［**プロキシサーバーを使用する**］を選択して、次のプロキシ設定を指定します：

- **アドレス**

  プロキシサーバーのアドレス。

- **ユーザー名**

  プロキシサーバーにログインするためのユーザー名。

- **パスワード**

  プロキシサーバーにログインするためのパスワード。

5 認証設定の指定と階層へのセカンダリ管理サーバーの追加

［**次へ**］をクリックします。［**セカンダリ管理サーバーの資格情報**］ページで、次の設定を指定します：

- **ユーザー名**

  セカンダリ管理サーバーにログインするためのユーザー名。

- **パスワード**

  セカンダリ管理サーバーへのログインに使用するパスワード。

［**次へ**］をクリックして、セカンダリ管理サーバーが階層に表示されるまで待ちます。

インターネット経由でセカンダリ管理サーバーにアクセスできる場合、セカンダリ管理サーバーはプライマリ管理サーバーに接続します。

インターネット経由でセカンダリ管理サーバーにアクセスでき、2 つの管理サーバー間の接続が正常に確立されている場合は、以降のステップをすべて省略します。

インターネット経由でセカンダリ管理サーバーにアクセスできない場合、セカンダリ管理サーバーは表示されますが、コントロールできるようにするにはセカンダリ管理サーバーで追加の操作を実行する必要があります。

6 オンプレミスで実行されている Kaspersky Security Center Web コンソールの接続の設定

オンプレミスで実行されている Kaspersky Security Center Web コンソールで、管理サーバーのプロパティを開き、［**全般**］タブで［**管理サーバーの階層**］セクションを開きます。［**この管理サーバーをセカンダリ管理サーバーとして使用する**］をオンにします。［**プライマリ管理サーバーの種別**］リストで［**Kaspersky Security Center Cloud コンソール**］をオンにます。

Kaspersky Security Center Web コンソールで、プライマリ管理サーバーが*管理サーバーのリポジトリへのアップデートのダウンロード*タスクのアップデート元として指定されているかどうかが確認されます。プライマリ管理サーバーがアップデート元として指定されている場合は、対応する警告メッセージとタスク設定へのリンクが表示されます。設定を変更して階層の作成に戻るか、この操作を省略して階層の作成に進むことができます。

［**セカンダリ管理サーバーとプライマリ管理サーバー間の接続を確立するための設定**］グループで、次の設定を指定します：

- **HDS サーバーアドレス（Cloud コンソールのプライマリ管理サーバー）**

  Kaspersky Security Center Cloud コンソールの管理サーバーのプロパティからコピーして保存した HDS サーバーアドレスを、完全修飾ドメイン名（FQDN）形式で入力します。

- **HDS サーバーポート**

  Kaspersky Security Center Cloud コンソールの管理サーバーのプロパティからコピーして保存した HDS サーバーのポート番号を入力します。

7 セカンダリ管理サーバーの証明書の追加

［**プライマリ管理サーバーの証明書を指定する**］をクリックし、Kaspersky Security Center Cloud コンソールの管理サーバーのプロパティから保存した証明書ファイルを指定します。

［**Hosted Discovery Service の証明書を指定する**］をクリックし、Kaspersky Security Center Cloud コンソールから保存した pem ファイルを指定します。

Kaspersky Security Center Cloud コンソールでセカンダリ管理サーバーへの接続にプロキシサーバーの使用を有効にした場合は、［**プロキシサーバーを使用する**］をオンにして、Kaspersky Security Center Cloud コンソールと同じプロキシ設定を指定します。

セカンダリ管理サーバーが非武装地帯（DMZ）にある場合は、［**プライマリ管理サーバーを DMZ 内のセカンダリ管理サーバーに接続する**］をオンにすることもできます。

セカンダリ管理サーバーがプライマリ管理サーバーに接続します。

結果

上記のステップを実行することで、階層が正常に作成されたことを確認できます：

- プライマリ管理サーバーのアクティブポリシーがセカンダリ管理サーバーで有効になります。プライマリ管理サーバーのタスクがセカンダリ管理サーバーに配信されます。［**セカンダリまたは仮想管理サーバーに配信**］がグループタスクの設定でオンになっている場合、そのようなタスクもセカンダリ管理サーバーに配信されます。

- プライマリ管理サーバーで変更がロックされているポリシー設定は、セカンダリ管理サーバーのすべてのポリシーで変更がロックされているとして表示されます。

- プライマリ管理サーバーによって適用されたポリシーが、セカンダリ管理サーバーのポリシーのリストに表示されます（［**アセット（デバイス）**］→［**ポリシーとプロファイル**］）。
- プライマリ管理サーバーによって配信されたグループタスクが、セカンダリ管理サーバーのタスクのリストに表示されます（［**アセット（デバイス）**］→［**タスク**］）。
- プライマリ管理サーバーで作成したポリシーとタスクは、セカンダリ管理サーバーで変更できません。
- Kaspersky Security Center Cloud コンソールの管理グループの構造で、セカンダリ管理サーバーは、この管理サーバーの追加時に選択したグループ内に表示されます。

Kaspersky Security Center Cloud コンソールへの移行

このセクションでは、オンプレミスで実行されているバージョン 12 以降の Kaspersky Security Center Web コンソールから Kaspersky Security Center Cloud コンソールへの移行プロセスについて説明します。

Kaspersky Security Center Cloud コンソールへの移行方法

このセクションでは、オンプレミスで実行されている Kaspersky Security Center から Kaspersky Security Center Cloud コンソールへの移行に使用できる方法について説明します。

移行機能を使用すると、ネットワーク接続されたデバイスを Kaspersky Security Center Cloud コンソールの管理下にある Kaspersky Security Center から転送できます。管理対象デバイスは、管理グループのメンバーシップなどの主要な設定を失うことなく切り替えられます。また、管理対象アプリケーションに関連するポリシーやタスクなどの重要なオブジェクトも保持されます。

管理サーバーを Kaspersky Security Center Cloud コンソールに移行するには、次の 2 つの方法のいずれかを選択できます：

- 管理サーバーの階層を使用しない移行：
  - オンプレミスの管理サーバーが Kaspersky Security Center Cloud コンソールに関してセカンダリではない場合でも、管理対象デバイスと関連オブジェクトを Kaspersky Security Center Cloud コンソールに転送できます。
  - Kaspersky Security Center Web コンソールと Kaspersky Security Center Cloud コンソールが異なる物理デバイスで開かれている場合は、ファイルの転送が必要になる場合があります（リムーバブルドライブ、メール、共有フォルダー、またはその他の簡便な方法を利用）。

  ネットワークに仮想管理サーバーが含まれている場合は、仮想管理サーバーを使用した移行を実行することもできます。

- 管理サーバーの階層を使用した移行：
  - Kaspersky Security Center Cloud コンソールのインターフェイスのみを使用して、管理対象デバイスと関連オブジェクトを Kaspersky Security Center Cloud コンソールに転送できるため、ファイルの物理的な転送は不要です。
  - オンプレミスで実行されている管理サーバーが Kaspersky Security Center Cloud コンソールのセカンダリとして機能する必要があります。移行を開始する前に、このような階層を作成できます。

ディスク全体の暗号化の場合、Kaspersky Security Center Cloud コンソールは BitLocker のみをサポートします。

管理サーバーの階層を使用しない移行

このセクションでは、オンプレミスの Kaspersky Security Center Web コンソールインスタンスで実行されている管理サーバーから Kaspersky Security Center Cloud コンソールで実行されている管理サーバーへの管理対象デバイスとポリシーやタスク、レポートなどの関連オブジェクトの移行について説明します。1 つの管理グループを移行範囲に含めて、Kaspersky Security Center Cloud コンソール内で同じ管理グループを復元できます。

このグループには、単一のオペレーティングシステムの管理対象デバイスが含まれている必要があります。ネットワークに異なるオペレーティングシステムまたは Linux ディストリビューションのデバイスが含まれている場合は、それらを異なる管理グループに割り当ててから、各グループを個別に移行します。

移行が完了すると、移行の対象範囲内にあるすべてのネットワークエージェントが Kaspersky Security Center Cloud コンソールを介してアップグレードおよび管理されます。

このセクションに記載されている手順は、管理サーバーの階層が存在しない場合、つまり、Kaspersky Security Center Cloud コンソールと、オンプレミスで実行されている Kaspersky Security Center Web コンソール間に接続が確立されていない場合に実行される移行プロセスを対象としています。

必須条件

開始する前に、次を実行します：

- オンプレミスで実行されている管理サーバーを次のバージョンにアップグレードします：
  - Windows デバイスの場合 - バージョン 12 以降
  - Linux デバイスの場合 - バージョン 12 パッチ A 以降
- Kaspersky Security Center Web コンソールのバージョン 12.1 以降をインストールします。
- 管理対象デバイスのネットワークエージェントをバージョン 12 以降にアップグレードします。
- Windows デバイスでは、アンインストール用パスワードなしでネットワークエージェントを使用します。
  パスワードが既に設定されている場合は、Kaspersky Security Center Web コンソールで次のいずれかを実行します：
  - ネットワークエージェントのポリシー設定で［**アンインストール用パスワードを使用する**］オプションを無効にします。
  - ［*アプリケーションのリモートアンインストール*］タスクを使用して、ネットワークエージェントをリモートでアンインストールします。タスクの［**アンインストールするアプリケーション**］で **Kaspersky Security Center ネットワークエージェント**を選択します。アンインストール用のパスワードを忘れずに入力してください。
- 管理対象アプリケーションを Kaspersky Security Center Cloud コンソールでサポートされているバージョンにアップグレードします。
- 管理対象アプリケーションの最新バージョンのポリシーがあることを確認してください。古いポリシーを使用している場合は、Kaspersky Security Center Cloud コンソールでサポートされているバージョンのアプリケーション用に新しいポリシーを作成してください。
- 現在のポリシーを使用するには、Kaspersky Security Center Cloud コンソールを使用して管理するアプリケーション用の Web プラグインをアップグレードしてください。

- カスペルスキー製品が Kaspersky Security Center Cloud コンソールでサポートされていない場合は、管理対象デバイスからそのカスペルスキー製品をアンインストールしてから、サポートされている製品に置き換えます。

- Windows オペレーティングシステムを実行している管理対象デバイスで Kaspersky Endpoint Security for Windows によって暗号化されたすべてのデータ（ディスクレベルまたはファイルレベル）を復号化し、アプリケーションポリシーまたはローカルで管理対象デバイスの暗号化機能を無効にします。詳細については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

  Windows デバイスに Kaspersky Endpoint Security for Windows によって暗号化されたファイルまたはフォルダーが保存されていた場合、ネットワークエージェントのアップグレードは移行プロセス中にキャンセルされます。デバイスのすべてのデータを復号化し、暗号化機能を無効にするように指示する通知が表示されます。

Kaspersky Security Center Cloud コンソールで管理可能な管理対象デバイスは、1つの管理サーバーあたり最大 25,000 台です。

移行手順

Kaspersky Security Center Cloud コンソールへの移行は、次の手順で実行します：

1. **移行の範囲を計画し、事前に満たすべき要件（前提条件）を確認**

   移行プロセスの範囲を見積もり（エクスポートする管理グループを確認し）、その中の管理対象デバイスの数を評価します。また、移行の前に満たしておくべき要件（前提条件）としてリストアップされているすべてのアクティビティが正常に完了していることを確認してください。

2. **管理対象デバイス、オブジェクト、および設定を Kaspersky Security Center Web コンソールからエクスポート**

   オンプレミスで実行されている Kaspersky Security Center Web コンソールの移行ウィザードを使用して、管理対象デバイスをそのオブジェクトとともにエクスポートします。

   エクスポートファイルの最大サイズは 4 GB です。

3. **エクスポートファイルを Kaspersky Security Center Cloud コンソールにインポート**

   管理対象デバイスやオブジェクトに関する情報を Kaspersky Security Center Cloud コンソールに転送します。このためには、Kaspersky Security Center Cloud コンソールの移行ウィザードを使用してエクスポートファイルをインポートし、ネットワークエージェントのスタンドアロンインストールパッケージを作成します。

4. **管理対象デバイスにネットワークエージェントを再インストール**

   オンプレミスで実行している Kaspersky Security Center Web コントロールの移行ウィザードに戻り、リモートインストールタスクを作成します。このタスクを（即時または後で）使用して、管理対象デバイスにネットワークエージェントを再インストールし、移行プロセスを完了することができます。

結果

移行の完了後に、移行が成功したことを確認できます：

- ネットワークエージェントは、すべての管理対象デバイスに再インストールされます。

- すべてのデバイスは、Kaspersky Security Center Cloud コンソールによって管理されます。
- 移行前に有効だったオブジェクト設定はすべて維持されます。

移行ウィザード

このセクションでは、Kaspersky Security Center Cloud コンソールとバージョン 12 以降の Kaspersky Security Center Web コンソールの移行ウィザードに関する情報について説明します。

ステップ 1：管理対象デバイス、オブジェクト、および設定を Kaspersky Security Center Web コンソールからエクスポート

管理対象デバイスを Kaspersky Security Center Web コンソールから Kaspersky Security Center Cloud コンソールに移行するには、まず、現在オンプレミスで実行しているお手元の管理サーバー上に存在する管理グループの階層に関する情報を含むエクスポートファイルを作成する必要があります。エクスポートファイルには、オブジェクトとその設定に関する情報も含まれている必要があります。このエクスポートファイルは、続けて実行する Kaspersky Security Center Cloud コンソールへのインポートに使用します。

エクスポートファイルの最大サイズは 4 GB です。

Kaspersky Security Center Web コンソールからオブジェクトやその設定をエクスポートする方法：

1. Kaspersky Security Center Web コンソールのメインメニューで、［**操作**］→［**移行**］の順に移動します。
2. ウィザードの最初のページで、［**次へ**］をクリックします。［**エクスポートする管理対象デバイス**］ページが開き、対応する管理サーバーの管理グループの階層全体が表示されます。
3. ［**エクスポートする管理対象デバイス**］ページで、［**管理対象デバイス**］グループ名の横にあるシェブロンアイコン（>）をクリックして、管理グループの階層を展開します。エクスポートする管理グループを選択します。

   オンプレミスで実行されている Kaspersky Security Center から 2 つの管理グループに対して実行された Kaspersky Security Center Cloud コンソールへの移行後、これらのグループのリモートインストールタスクは同じ名前で表示されます。

4. ポリシーとタスクをグループオブジェクトとともに Kaspersky Security Center Cloud コンソールに転送する必要がある管理対象アプリケーションを選択します。オブジェクトをエクスポートする管理対象アプリケーションを選択するには、リスト内の名前の横にあるチェックボックスをオンにします。

   Kaspersky Security Center 管理サーバーがリストに表示されますが、対応するチェックボックスをオンにしても、ポリシーはエクスポートされません。

   管理対象アプリケーションが Kaspersky Security Center Cloud コンソールでサポートされているかどうかを確認するには、対応するリンクをクリックします。Kaspersky Security Center Cloud コンソールによって管理されるアプリケーションのリストが含まれるオンラインヘルプのトピックにリダイレクトされます。

Kaspersky Security Center Cloud コンソールでサポートされていないアプリケーションを選択すると、これらのアプリケーションのポリシーとタスクはエクスポートされインポートされます。しかしながら専用プラグインが使用できないため、Kaspersky Security Center Cloud コンソールにより管理することはできません。

5. 既定でエクスポートされるグループオブジェクトのリストを確認し、必要に応じて、選択した管理グループと一緒にエクスポートするグループ以外のオブジェクトを指定することができます。グローバルタスク、カスタムデバイスの抽出、レポート、カスタムロール、内部ユーザーとセキュリティグループ、カスタムアプリケーションカテゴリなどの様々なオブジェクトを含めたり除外したりして、エクスポートの範囲を設定できます。このページには以下のセクションがあります：

- **グローバルタスク**

  管理対象アプリケーションのグローバルタスクのリスト、およびネットワークエージェントのグローバルタスクのリスト。

  選択したグローバルタスクが特定のオブジェクト選択に適用される場合、この選択もエクスポートされます。

  管理サーバーのグローバルタスクはリストにありますが、エクスポートすることはできません。これらのタスクをオンにしても、エクスポート範囲は変わりません。リモートインストールタスクも、それぞれのインストールパッケージをエクスポートできないため、エクスポート範囲外のままです。

- **デバイスの抽出**

  カスタムデバイスの抽出のリスト。

- **レポート**

  エクスポートするレポートインスタンスの編集可能なリスト。

  選択したレポートが特定のオブジェクト選択に適用される場合、この選択もエクスポートされます。

  Kaspersky Security Center Cloud コンソールには、Kaspersky Security Center Web コンソールと同じレポートテンプレートが含まれているため、手動で作成または再設定したレポートのみをエクスポートするように選択できます。

- **グループオブジェクト**

既定でエクスポートされるグループオブジェクトのリスト。選択した管理グループに関連する次のオブジェクトは、既定で、完全なかたちでエクスポートされます。

- 管理グループの構造（選択した管理グループのすべてのサブグループ）
- エクスポートする管理グループに含まれているデバイス
- エクスポートするデバイスに割り当てられているタグ

  タグが Kaspersky Security Center Web コンソールで作成されているが、どのデバイスにも割り当てられていない場合、そのタグはエクスポートされません。自動タグ付けルールもエクスポートされません。

- 選択された管理対象アプリケーションのグループポリシー

  管理サーバーポリシーとネットワークエージェントポリシーはエクスポートされません。

- 選択されている管理対象アプリケーションのグループタスク、および、ネットワークエージェントのグループタスク

  管理サーバーのタスクはエクスポートされません。

また、特定のタイプの非グループオブジェクトがエクスポートされないようにすることもできます。

- カスタムロール（ユーザーが作成したロールのみ）のエクスポートをキャンセルするには、［**カスタムロールをエクスポート対象から除外する**］をオンにします。
- 内部ユーザーやセキュリティグループのエクスポートをキャンセルするには、［**内部ユーザーとセキュリティグループをエクスポート対象から除外する**］をオンにします。
- コンテンツを手動で追加したカスタムアプリケーションカテゴリのエクスポートをキャンセルするには、［**カスタムアプリケーションカテゴリをエクスポート対象から除外する**］をオンにします。

様々なオペレーティングシステムのデバイスを Kaspersky Security Center Cloud コンソールに転送する場合、非グループオブジェクトは一度だけ移行する必要があります。

移行ウィザードは、選択した管理グループに含まれる管理対象デバイスの総数をチェックします。この数が 10,000 を超えると、エラーメッセージが表示されます。選択した管理グループ内の管理対象デバイスの数が制限内に収まるまで、［**次へ**］は使用不可（淡色表示）のままです。

6. 移行範囲を設定したら、［**次へ**］をクリックしてエクスポートプロセスを開始します。［**エクスポート用ファイルの作成**］ページが開き、移行範囲に含めた各種別のオブジェクトについて、エクスポートの進行状況をこのページで表示できます。オブジェクトのリスト内の項目の横にある更新アイコン（）がすべて緑色のチェックマーク（）に変わるまで待ちます。エクスポートが完了し、エクスポートファイルは、お手元の Web ブラウザーの設定により決められた、既定のダウンロード場所に自動的にダウンロードされます。エクスポートファイルの名前がブラウザーウィンドウの下部に表示されます。

7. ［**エクスポートが完了しました**］ページが表示されたら、Kaspersky Security Center Cloud コンソールで実行する次の手順に進みます。

Kaspersky Security Center Web コンソールと Kaspersky Security Center Cloud コンソールを異なるデバイスで使用する場合は、エクスポートファイルをリムーバブルドライブにコピーするか、ファイルを転送するその他の方法を選択する必要があります。

ステップ 2：エクスポートファイルを Kaspersky Security Center Cloud コンソールにインポート

管理対象デバイス、オブジェクト、および Kaspersky Security Center Web コンソールからエクスポートした設定に関する情報を転送するには、ワークスペースに展開されている Kaspersky Security Center Cloud コンソールにインポートする必要があります。これにより、スタンドアロンインストールパッケージを作成し、管理対象デバイスへのネットワークエージェントの再インストールに使用できます。

Kaspersky Security Center Cloud コンソールで移行ウィザードを開始する前に、現在のローカリゼーション言語がエクスポートプロセス中の Kaspersky Security Center Web コンソール言語と同じであることを確認してください。必要に応じて言語を切り替えます。

Kaspersky Security Center Cloud コンソールの自身の作業領域でクイックスタートウィザードを以前に完了している場合は、［**管理対象デバイス**］グループには、既定の設定で作成されたポリシーとタスクが含まれます。Kaspersky Security Center Web コンソールからエクスポートしたものをインポートする前に、これらのポリシーとタスクを削除してください。

エクスポートファイルを Kaspersky Security Center Cloud コンソールにインポートする方法：

1. Kaspersky Security Center Cloud コンソールのメインメニューで、［**操作**］→［**移行**］の順にクリックします。
2. ウィザードの最初のページで、［**インポート**］をクリックします。ファイルエクスプローラーのウィンドウが表示されます。保存したフォルダーを参照してエクスポートファイルを選択し、［**開く**］をクリックします。ファイルのアップロードステータスの横にある更新アイコン（）が緑色のチェックマーク（）に変わるまで待ちます。
3. ［**次へ**］をクリックします。次のページが開き、Kaspersky Security Center Cloud コンソールに、管理サーバーの管理グループの階層全体が表示されます。
4. グループオブジェクトを復元するターゲットの管理グループの横にあるチェックボックスをオンにして、［**次へ**］をクリックします。移行ウィザードには、Kaspersky Security Center Cloud コンソールで使用可能なネットワークエージェントのインストールパッケージのリストが表示されます。
5. 含まれているバージョンやネットワークエージェントの言語版が適当なインストールパッケージを選択し、［**次へ**］をクリックします。

お手元の Kaspersky Security Center Cloud コンソールの作業領域でクイックスタートウィザードを以前に完了していて、Windows デバイスで移行を実行している場合にのみ、Kaspersky Network Agent for Windows インストールパッケージをオンにしてください。

移行ウィザードがスタンドアロンインストールパッケージを作成するまで待ちます。ネットワークエージェントのスタンドアロンインストールパッケージの最大ファイルサイズは 200 MB です。

ファイルは解凍され、ブラウザー設定で定義された既定のダウンロード場所に自動的にダウンロードされます。非グループオブジェクトとグループオブジェクトがターゲット管理グループに復元されます。

インポートが完了すると、エクスポートされた管理グループの構造（デバイスの詳細を含む）が、選択したターゲットの管理グループの下に表示されます。復元するオブジェクトの名前が既存のオブジェクトの名前と同じである場合、復元されたオブジェクトには増分サフィックスが追加されます。

［**管理対象デバイス**］グループ全体をインポートした場合、競合を回避するために、新しくインポートしたサブグループの名前を変更することを推奨します：

a. ［**グループ階層構造**］セクションに移動します。

b. グループツリーでサブグループの名前をクリックします。

c. プロパティウィンドウが開くので、［**名前**］に別の名前を入力します（たとえば、「移行されたデバイス」）。

エクスポート範囲に含まれるオブジェクト（ポリシー、タスク、および管理対象デバイス）が Kaspersky Security Center Cloud コンソール に正常にインポートされているかどうかを確認することを推奨します。［**アセット（デバイス）**］セクションに移動し、インポートされたオブジェクトが［**ポリシーとプロファイル**］、［**タスク**］、および［**管理対象デバイス**］サブセクションでリストに表示されているかどうかを確認します。

移行ウィザードを最小化して、インポート中に他の操作を同時に実行することはできません。オブジェクトのリスト内のすべてのアイテムの横にある更新アイコン（🔄）が緑色のチェックマーク（✓）に変わり、インポートが完了するまで待ちます。この後、デバイスは Kaspersky Security Center Cloud コンソールへの切り替えを開始します。

6. ［**終了**］をクリックして移行ウィザードを終了します。

7. スタンドアロンインストールパッケージを再度検索してダウンロードする場合は、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］に移動し、［**スタンドアロンパッケージリストの表示**］をクリックします。表示されるリストから、作成したスタンドアロンインストールパッケージを選択し、［**ダウンロード**］をクリックします。

Kaspersky Security Center Web コンソールと Kaspersky Security Center Cloud コンソールを異なるデバイスで使用する場合は、スタンドアロンインストールパッケージをリムーバブルドライブにコピーするか、その他のファイル転送方法を選択する必要があります。

ステップ 3：Kaspersky Security Center Cloud コンソールにより管理されているデバイスにネットワークエージェントを再インストール

ネットワークエージェントのスタンドアロンインストールパッケージを作成したら、リモートインストールタスクの作成に進むことができます。このタスクを実行すると、すべての管理対象デバイスにネットワークエージェントを再インストールして、これらのデバイスを Kaspersky Security Center Cloud コンソールによる管理に切り替えることができます。

データ損失のリスクを軽減するために、最初は、企業ネットワーク内で最大 20 台の管理対象デバイスを扱い、物理サーバーが含まれない、小規模な管理グループに対してアクションを実行することを推奨します。これらのアクションを完了した後で、再インストールが正常に完了したかどうかを確認し、全範囲を対象とする再インストールに進みます。

リモートインストールタスクを作成してネットワークエージェントを再インストールする方法：

1. オンプレミスで実行されている Kaspersky Security Center Web コンソール内の移行ウィザードに戻ります。

   以下で説明するように、移行ウィザードを使用してリモートインストールタスクを作成し、ネットワークエージェントを再インストールすることを推奨します。カスタムリモートインストールタスクを使用する必要がある場合は、最初にネットワークエージェントスタンドアロンイントールパッケージからカスタムインストールパッケージを手動で作成する必要があります。カスタムインストールパッケージを作成する時は、実行ファイルのコマンドラインで「-s」キーを指定する必要があることに注意してください。そうしないと、このカスタムインストールパッケージからネットワークエージェントを再インストールすると、エラーが発生して完了します。

   移行ウィザードの現在の状態に応じて、次のいずれかを実行できます：

   - エクスポート後に移行ウィザードを閉じておらず、セッションの有効期限が切れていない場合は、［**移行ウィザードのステップ 3 に移動**］をクリックします。［**スタンドアロンインストールパッケージをアップロード**］のチェックボックスをオンにして、［**スタンドアロンインストールパッケージの選択**］をクリックします。開いたブラウザーウィンドウで、ネットワークエージェントのスタンドアロンインストールパッケージを指定します。

   - 何らかの理由で移行ウィザードを再度開始する必要がある場合は、［**スタンドアロンインストールパッケージをアップロード**］をオンにして、［**スタンドアロンインストールパッケージの選択**］をクリックします。開いたブラウザーウィンドウで、ネットワークエージェントのスタンドアロンインストールパッケージを指定します。その後、移行ウィザードには、この管理サーバーの管理グループの階層が再び表示されます。エクスポートファイルを作成したのと同じグループを選択し、［**次へ**］をクリックします。

     移行ウィザードは、選択した管理グループに含まれる管理対象デバイスの総数をあらためて確認します。この数が 10,000 を超えると、エラーメッセージが表示されます。選択した管理グループ内の管理対象デバイスの数が制限内に収まるまで、［**次へ**］は使用不可（淡色表示）のままです。

2. スタンドアロンインストールパッケージがアップロードされるまで待ち、［**次へ**］をクリックします。移行ウィザードが、カスタムのインストールパッケージとそのリモートインストールタスクを作成します。タスク範囲には、［**エクスポートする管理対象デバイス**］ページで選択した管理グループが含まれます。タスクの起動スケジュールは、既定では［**手動**］に設定されます。移行ウィザードに作成の進行状況が表示されます。更新アイコン（）が緑色のチェックマーク（）に変わるまで待ち、［**次へ**］をクリックします。

3. 必要があれば、オンプレミスで実行されている管理サーバーおよびそのすべてのサブグループの、選択した管理グループ内のデバイスの［**新規作成したリモートインストールタスクを実行**］をオンにします（既定ではオフになっています）。この場合、デバイスは Kaspersky Security Center Cloud コンソールの管理下に切り替えられますが、ネットワークエージェントのインストールが完了してからになります。タスクを実行する管理グループへのフルパスが表示されます。

   Kaspersky Security Center Cloud コンソールへのインポートが完了するまでは、このタスクを開始しないでください。そうしないと、リストでデバイス名が重複する可能性があります。

4. ［**終了**］をクリックして移行ウィザードを閉じ、次の目的でリモートインストールタスクを開始します。

   - ネットワークエージェントインスタンスのアップグレード
   - Kaspersky Security Center Cloud コンソールで実行されている管理サーバーの管理下にあるネットワークエージェントインスタンスの切り替え

   ［**新規作成したリモートインストールタスクを実行**］をオフのままにしておき、必要に応じて後で手動でタスクを開始することもできます。

移行されたネットワークエージェントのインスタンスを Kaspersky Security Center Cloud コンソールで管理できるようになったことを確認できます。そうするには、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。［**可視**］、［**ネットワークエージェントがインストール済み**］、および［**ネットワークエージェントが実行中**］列で、移行された管理対象デバイスに確認アイコン（）が表示されていることを確認してください。また、これらのデバイスのステータスの説明に［*長期間接続されていません*］がないことを確認してください。

管理サーバーの階層を使用した移行

このセクションでは、オンプレミスの Kaspersky Security Center Web コンソールインスタンスで実行されている管理サーバーから Kaspersky Security Center Cloud コンソールで実行されている管理サーバーへの管理対象デバイスと関連オブジェクトの移行について説明します。このプロセスには階層が含まれます。つまり、オンプレミスで実行されている Kaspersky Security Center Web コンソールはセカンダリ管理サーバーとして機能し、Kaspersky Security Center Cloud コンソールはプライマリ管理サーバーとして機能します。

Kaspersky Security Center Cloud コンソールに転送するすべての管理グループには、単一のオペレーティングシステムの管理対象デバイスが含まれている必要があります。ネットワークに異なるオペレーティングシステムのデバイスが含まれている場合は、それらを異なる管理グループに割り当ててから、各グループを個別に移行します。

移行が完了すると、移行の対象範囲内にあるグループのすべてのネットワークエージェントが Kaspersky Security Center Cloud コンソールを介してアップグレードおよび管理されます。

開始する前に、次を実行します：

- オンプレミスで実行されている管理サーバーを次のバージョンにアップグレードします：
  - Windows デバイスの場合 - バージョン 12 以降
  - Linux デバイスの場合 - バージョン 12 パッチ A 以降
- Kaspersky Security Center Web コンソールのバージョン 12.1 以降をインストールします。
- 管理対象デバイスのネットワークエージェントをバージョン 12 以降にアップグレードします。
- Windows デバイスでは、アンインストール用パスワードなしでネットワークエージェントを使用します。

  パスワードが既に設定されている場合は、Kaspersky Security Center Web コンソールで次のいずれかを実行します：

  - ネットワークエージェントのポリシー設定で［**アンインストール用パスワードを使用する**］オプションを無効にします。

- ［*アプリケーションのリモートアンインストール*］タスクを使用して、ネットワークエージェントをリモートでアンインストールします。タスクの［**アンインストールするアプリケーション**］で **Kaspersky Security Center ネットワークエージェント**を選択します。アンインストール用のパスワードを忘れずに入力してください。

- 管理対象アプリケーションを Kaspersky Security Center Cloud コンソールでサポートされているバージョンにアップグレードします。

- 管理対象アプリケーションの最新バージョンのポリシーがあることを確認してください。古いポリシーを使用している場合は、Kaspersky Security Center Cloud コンソールでサポートされているバージョンのアプリケーション用に新しいポリシーを作成してください。

- 現在のポリシーを使用するには、Kaspersky Security Center Cloud コンソールを使用して管理するアプリケーション用の Web プラグインをアップグレードしてください。

- カスペルスキー製品が Kaspersky Security Center Cloud コンソールでサポートされていない場合は、管理対象デバイスからそのカスペルスキー製品をアンインストールしてから、サポートされている製品に置き換えます。

- Windows オペレーティングシステムを実行している管理対象デバイスで Kaspersky Endpoint Security for Windows によって暗号化されたすべてのデータ（ディスクレベルまたはファイルレベル）を復号化し、アプリケーションポリシーまたはローカルで管理対象デバイスの暗号化機能を無効にします。詳細については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

  Windows デバイスに Kaspersky Endpoint Security for Windows によって暗号化されたファイルまたはフォルダーが保存されていた場合、ネットワークエージェントのアップグレードは移行プロセス中にキャンセルされます。デバイスのすべてのデータを復号化し、暗号化機能を無効にするように指示する通知が表示されます。

Kaspersky Security Center Cloud コンソールで管理可能な管理対象デバイスは、1つの管理サーバーあたり最大 25,000 台です。

Kaspersky Security Center Cloud コンソールへの移行を行うには：

1. 移行プロセスの範囲を見積もり（エクスポートする管理グループを確認し）、その中の管理対象デバイスの数を評価します。移行の前に満たしておくべき要件（前提条件）としてリストアップされているすべてのアクティビティが正常に完了していることを確認してください。

2. Kaspersky Security Center Cloud コンソールで、移行する管理対象デバイスのセカンダリ管理サーバーに進みます。

3. メインメニューで、［**操作**］→［**移行**］の順に選択します。

   移行ウィザードの最初のページが開きます。

4. ウィザードの最初のページで、［**次へ**］をクリックします。

   ［**エクスポートする管理対象デバイス**］ページが開き、セカンダリ管理サーバーの管理グループの階層全体が表示されます。

5. ［**エクスポートする管理対象デバイス**］ページで、［**管理対象デバイス**］グループ名の横にあるシェブロンアイコン（>）をクリックして、管理グループの階層を展開します。エクスポートする管理グループを選択します。

移行ウィザードは、選択した管理グループに含まれる管理対象デバイスの総数をチェックします。この数が 10,000 を超えると、エラーメッセージが表示されます。選択した管理グループ内の管理対象デバイスの数が制限内に収まるまで、［**次へ**］は使用不可（淡色表示）のままです。

6. ポリシーとタスクをグループオブジェクトとともに Kaspersky Security Center Cloud コンソールに転送する必要がある管理対象アプリケーションを選択します。オブジェクトをエクスポートする管理対象アプリケーションを選択するには、リスト内の名前の横にあるチェックボックスをオンにします。

   Kaspersky Security Center 管理サーバーがリストに表示されますが、対応するチェックボックスをオンにしても、ポリシーはエクスポートされません。

   管理対象アプリケーションが Kaspersky Security Center Cloud コンソールでサポートされているかどうかを確認するには、対応するリンクをクリックします。Kaspersky Security Center Cloud コンソールによって管理されるアプリケーションのリストが含まれるオンラインヘルプのトピックにリダイレクトされます。

   Kaspersky Security Center Cloud コンソールでサポートされていないアプリケーションを選択すると、これらのアプリケーションのポリシーとタスクは移行されますが、専用プラグインが使用できないため、Kaspersky Security Center Cloud コンソールで管理することはできません。

7. 既定でエクスポートされるグループオブジェクトのリストを表示します。必要に応じて、選択した管理グループとともにエクスポートする非グループオブジェクトを指定することもできます。これには、グローバルタスク、カスタムデバイスの選択、レポート、カスタムロール、内部ユーザーとセキュリティグループ、コンテンツが手動で追加されたカスタムアプリケーションカテゴリなどがあります。このページには以下のセクションがあります：

   - **グローバルタスク**

     管理対象アプリケーションのグローバルタスクのリスト、およびネットワークエージェントのグローバルタスクのリスト。

     選択したグローバルタスクが特定のオブジェクト選択に適用される場合、この選択もエクスポートされます。

     管理サーバーのグローバルタスクはリストにありますが、エクスポートすることはできません。これらのタスクをオンにしても、エクスポート範囲は変わりません。リモートインストールタスクも、それぞれのインストールパッケージをエクスポートできないため、エクスポート範囲外のままです。

   - **デバイスの抽出**

     カスタムデバイスの抽出のリスト。

   - **レポート**

エクスポートするレポートインスタンスの編集可能なリスト。

選択したレポートが特定のオブジェクト選択に適用される場合、この選択もエクスポートされます。

Kaspersky Security Center Cloud コンソールには、Kaspersky Security Center Web コンソールと同じレポートテンプレートが含まれているため、手動で作成または再設定したレポートのみをエクスポートするように選択できます。

- **グループオブジェクト**

既定でエクスポートされるグループオブジェクトのリスト。選択した管理グループに関連する次のオブジェクトは、既定で、完全なかたちでエクスポートされます。

- 管理グループの構造（選択した管理グループのすべてのサブグループ）
- エクスポートする管理グループに含まれているデバイス
- エクスポートするデバイスに割り当てられているタグ

  タグが Kaspersky Security Center Web コンソールで作成されているが、どのデバイスにも割り当てられていない場合、そのタグはエクスポートされません。自動タグ付けルールもエクスポートされません。

- 選択された管理対象アプリケーションのグループポリシー

  管理サーバーポリシーとネットワークエージェントポリシーはエクスポートされません。

- 選択されている管理対象アプリケーションのグループタスク、および、ネットワークエージェントのグループタスク

  管理サーバーのタスクはエクスポートされません。

また、特定のタイプの非グループオブジェクトがエクスポートされないようにすることもできます。

- カスタムロール（ユーザーが作成したロールのみ）のエクスポートをキャンセルするには、［**カスタムロールをエクスポート対象から除外する**］をオンにします。
- 内部ユーザーやセキュリティグループのエクスポートをキャンセルするには、［**内部ユーザーとセキュリティグループをエクスポート対象から除外する**］をオンにします。
- コンテンツを手動で追加したカスタムアプリケーションカテゴリのエクスポートをキャンセルするには、［**カスタムアプリケーションカテゴリをエクスポート対象から除外する**］をオンにします。

様々なオペレーティングシステムのデバイスを Kaspersky Security Center Cloud コンソールに転送する場合、非グループオブジェクトは一度だけ移行する必要があります。

8. 移行範囲を設定したら、［**次へ**］をクリックしてエクスポートプロセスを開始します。［**エクスポート用ファイルの作成**］ページが開き、移行範囲に含めた各種別のオブジェクトについて、エクスポートの進行状況をこのページで表示できます。オブジェクトのリスト内の各項目の横にある更新アイコン（）が、緑色のチェックマーク（）に変わるまで待ちます。エクスポートが終了し、エクスポートファイルが一時フォルダーに自動的に保存されます。次のページが開き、プライマリ管理サーバーとして機能する Kaspersky Security Center Cloud コンソールの管理グループの階層全体が表示されます。

9. グループオブジェクトをインポートする必要がある管理グループの横にあるチェックボックスをオンにして、［**次へ**］をクリックします。ファイルが解凍され、非グループオブジェクトとグループオブジェクトがターゲットの管理グループに復元されます。

   復元するオブジェクトの名前が既存のオブジェクトの名前と同じである場合、復元されたオブジェクトには増分サフィックスが追加されます。

   インポートが完了すると、エクスポートされた管理グループの構造（デバイスの詳細を含む）が、選択したターゲットの管理グループの下に表示されます。非グループオブジェクトもインポートされます。

   移行ウィザードを最小化して、インポート中に他の操作を同時に実行することはできません。オブジェクトのリスト内の各項目の横にある更新アイコン（）が、緑色のチェックマーク（）に変わり、インポートが完了するまで待ちます。この後、デバイスは Kaspersky Security Center Cloud コンソールへの切り替えを開始します。

10. インポートが完了すると、移行ウィザードには適切なオペレーティングシステム向けの Kaspersky Security Center Cloud コンソールで使用可能なネットワークエージェントのインストールパッケージのリストが表示されます。含まれているバージョンやネットワークエージェントの言語版が適当なインストールパッケージを選択します。

    お手元の Kaspersky Security Center Cloud コンソールの作業領域でクイックスタートウィザードを以前に完了していて、Windows デバイスで移行を実行している場合にのみ、Kaspersky Network Agent for Windows インストールパッケージをオンにしてください。

11. ［**次へ**］をクリックします。

    移行ウィザードは、新しいスタンドアロンインストールパッケージ（または既存のインストールパッケージを使用）とそれに基づくカスタムインストールパッケージ、および対応するリモートインストールタスクを作成します。タスクの対象範囲には、［**エクスポートする管理対象デバイス**］ページで選択した管理グループが含まれます。既定では、タスクの起動スケジュールが［**手動**］に設定されています。移行ウィザードに作成の進行状況が表示されます。

12. 各更新アイコン（）が緑色のチェックマーク（）に変わるまで待ち、［**次へ**］をクリックします。

13. 必要に応じて、オンプレミスで実行されている Kaspersky Security Center Web コンソールで選択した管理グループとそのすべてのサブグループのデバイスに対して、［**新規作成したリモートインストールタスクを実行**］をオンにします（既定ではオフになっています）。ネットワークエージェントのインストールが完了すると、Kaspersky Security Center Cloud コンソールを介して選択したデバイスを管理できます。タスクを実行する管理グループへの完全パスが表示されます。

    Kaspersky Security Center Cloud コンソールへのインポートが完了するまでは、リモートインストールタスクを開始しないでください。これに反すると、デバイスが重複する可能性があります。

14. ［**終了**］をクリックして移行ウィザードを閉じ、次の目的でリモートインストールタスクを開始します。

- ネットワークエージェントインスタンスのアップグレード
- Kaspersky Security Center Cloud コンソールを使用したネットワークエージェントインスタンスの管理

［**リモートインストールタスクを実行する**］をオフのままにしておき、必要に応じて後で手動でタスクを開始することもできます。

移行されたネットワークエージェントのインスタンスを Kaspersky Security Center Cloud コンソールで管理できるようになったことを確認できます。そうするには、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。［**可視**］、［**ネットワークエージェントがインストール済み**］、および［**ネットワークエージェントが実行中**］列で、移行された管理対象デバイスに確認アイコン（）が表示されていることを確認してください。また、これらのデバイスのステータスの説明に［*長期間接続されていません*］がないことを確認してください。

シナリオ：Linux または macOS オペレーティングシステムのデバイスの移行

このセクションでは、Linux または macOS オペレーティングシステムのデバイスを、オンプレミスで実行中の Kaspersky Security Center Web コンソールから Kaspersky Security Center Cloud コンソールへ移行する方法について説明します。管理サーバーの階層を使用しない移行と、管理サーバーの階層を使用した移行の基本的なシナリオでは、すべてのデバイスと関連オブジェクトを Kaspersky Security Center Cloud コンソールに転送できます。ただし、ネットワークに Windows だけでなく、Linux または macOS を実行しているデバイスが含まれている場合は、各オペレーティングシステム種別のデバイスを個別に転送する必要があります。つまり、移行を数回実行する必要があります。

必須条件

開始する前に、次を実行します：

- オンプレミスで実行されている管理サーバーをバージョン 12 以降にアップグレードします。
- Kaspersky Security Center Web コンソールのバージョン 12.1 以降をインストールします。
- 管理対象デバイスのネットワークエージェントをバージョン 12 以降にアップグレードします。
- 管理対象アプリケーションを Kaspersky Security Center Cloud コンソールでサポートされているバージョンにアップグレードします。
- 管理対象アプリケーションの最新バージョンのポリシーがあることを確認してください。古いポリシーを使用している場合は、Kaspersky Security Center Cloud コンソールでサポートされているバージョンのアプリケーション用に新しいポリシーを作成してください。
- 現在のポリシーを使用するには、Kaspersky Security Center Cloud コンソールを使用して管理するアプリケーション用の Web プラグインをアップグレードしてください。
- カスペルスキー製品が Kaspersky Security Center Cloud コンソールでサポートされていない場合は、管理対象デバイスからそのカスペルスキー製品をアンインストールしてから、サポートされている製品に置き換えます。

Kaspersky Security Center Cloud コンソールで管理可能な管理対象デバイスは、1つの管理サーバーあたり最大 25,000 台です。

移行手順

Kaspersky Security Center Cloud コンソールへの移行は、次の手順で実行します：

1. **オペレーティングシステムごとの管理対象デバイスのグループ化**

   ネットワークに異なるオペレーティングシステム（Windows、Linux、または macOS）を実行しているデバイスが含まれている場合は、Kaspersky Security Center Web コンソールの個別の管理グループにある各オペレーティングシステムにデバイスを配置します。また、Linux ディストリビューションごとに管理グループを作成します。たとえば、Debian デバイスと Red Hat Linux デバイスがある場合は、異なる管理グループに割り当てます。様々なオペレーティングシステムには異なるネットワークエージェントインストールパッケージが必要になるため、この操作により移行を正常に実行できます。

2. **すべての管理グループとそのアプリケーションオブジェクトの移行を個別に実行する**

   ポリシーとタスクを含めるには、各オペレーティングシステムの管理対象デバイスを個別に移行する必要があります。たとえば、Windows、macOS、Ubuntu、CentOS デバイスを使用している場合は、最初に Windows オペレーティングシステムを実行しているデバイスを Kaspersky Security Center Cloud コンソールに転送し、次に macOS、次に Ubuntu、最後に CentOS を転送します。管理対象デバイスは任意の順序で転送できます。

   そのためには、ネットワークにセカンダリ管理サーバーが含まれているかどうかに応じて、管理サーバーの階層を使用しない移行か、管理サーバーの階層を使用した移行を実行します。移行中は、転送されたデバイスのオペレーティングシステムに対応するネットワークエージェントのインストールパッケージを使用してください。たとえば、移行を正常に実行するには、Linux デバイス向けの Kaspersky Security Center 13.2 Network Agent を選択します。

   > グローバルタスク、カスタムデバイスの抽出、レポートなどの非グループオブジェクトは1度だけ移行する必要があることに注意してください。

結果

移行の完了後に、移行が成功したことを確認できます：

- 適切なバージョンのネットワークエージェントが、Linux または macOS オペレーティングシステムの各管理対象デバイスに再インストールされます。
- すべての Linux または macOS デバイスは、Kaspersky Security Center Cloud コンソールによって管理されます。
- 移行前に有効だったオブジェクト設定はすべて維持されます。

シナリオ：Kaspersky Security Center Cloud コンソールから Kaspersky Security Center への逆移行

Kaspersky Security Center Cloud コンソールから Kaspersky Security Center 管理サーバーに管理対象デバイスを移行する必要がある場合があります。たとえば、この処理を使用して Kaspersky Security Center Cloud コンソールへの移行をロールバックできます。

必須条件

開始する前に、次の前提条件が満たされていることを確認してください：

- Kaspersky Security Center Cloud コンソールが利用可能で、管理対象デバイスが接続されている。
- Kaspersky Security Center 14.2 以降の管理サーバーが使用可能で、バージョン 13 以降のネットワークエージェントのインストールパッケージが存在します。

逆移行の手順

逆移行は次の手順で構成されます：

1. **オンプレミスの Kaspersky Security Center 管理サーバーでのネットワークエージェントのスタンドアロンインストールパッケージの作成**

   オンプレミスで実行されている Kaspersky Security Center 管理サーバーで、ネットワークエージェントのスタンドアロンインストールパッケージを作成します。

   作成処理中、［**未割り当てデバイスをこのグループへ移動**］を選択してインストール後にネットワークエージェントを移動する管理グループを指定できます。管理グループを指定した場合、このスタンドアロンインストールパッケージにインストールされているすべてのネットワークエージェントをターゲットの管理グループに移動する自動移動ルールが作成されます。

   > 正確な逆移行のためには、Kaspersky Security Center Cloud コンソールで使用されているバージョン以降のネットワークエージェントを選択する必要があります。

2. **Kaspersky Security Center Cloud コンソールでのカスタムインストールパッケージの作成**

   オンプレミスで実行されている Kaspersky Security Center 管理サーバーから作成して保存したスタンドアロンインストールパッケージに基づいて、Kaspersky Security Center Cloud コンソールでカスタムインストールパッケージを作成します。

   サイレントモードのパッケージのインストールを有効にするには、［**実行ファイルのコマンドライン**］で -s キーを指定します。

3. **リモートインストールタスクの作成**

   Kaspersky Security Center Cloud コンソールで、作成したカスタムインストールパッケージを使用してリモートインストールタスクを作成します。

4. **リモートインストールタスクの実行**

   作成したリモートインストールタスクを開始します。タスクによって、指定した管理グループ内のすべてのネットワークエージェントの再インストールが開始されます。また、接続アドレスとその他の接続設定の変更により、オンプレミスで実行されている Kaspersky Security Center 管理サーバーで管理されているネットワークエージェントが切り替えられます。

   > スタンドアロンインストールパッケージの作成中にターゲットの管理グループを指定しなかった場合、すべてのデバイスが［**未割り当てデバイス**］グループに移動されます。

結果

移行の完了後に、移行が成功したことを確認できます：

- 以前は Kaspersky Security Center Cloud コンソールで管理されていた、リモートインストールタスクの範囲内のすべてのデバイスが、オンプレミスで実行されている Kaspersky Security Center 管理サーバーで管理されます。
- デバイスが、インストールパッケージの設定で指定されいる管理グループに自動的に移動されます。

すべての対象デバイスの接続設定が変更されて対象デバイスがなくなるため、Kaspersky Security Center Cloud コンソールのリモートインストールタスクは完了できません。移行範囲に含まれるすべてのデバイスの管理対象デバイスリストの［**可視**］列に、エラーアイコン（  ）が表示されたことを確認してから、手動でタスクを停止する必要があります。

仮想管理サーバーがある場合の移行

既存の Kaspersky Security Center のオンプレミスインフラストラクチャに仮想管理サーバーがある場合は、移行ウィザードを使用して、オンプレミスの Kaspersky Security Center から Kaspersky Security Center Cloud コンソールに移行することができません。また、移行できるのは顧客のデバイスのみです。ポリシー、タスク、およびレポートは手動で作成する必要があります。

次の移行シナリオのいずれかを実行できます：

- 仮想管理サーバーからプライマリ管理サーバーにクライアントデバイスを移動する
- 仮想管理サーバーから手動で移行する

シナリオ：デバイスの移動による仮想管理サーバーがある場合の移行

オンプレミスで実行されている Kaspersky Security Center Webコンソールから Kaspersky Security Center Cloud コンソールへの移行を実行するには、デバイスを仮想管理サーバーからプライマリ管理サーバーに移動します。

必須条件

移行する前に、オンプレミスで実行されている管理サーバーをバージョン 12 以降にアップグレードし、Kaspersky Security Center Cloud コンソールでサポートされるバージョンに管理対象アプリケーションをアップグレードするなど、いくつかの処理を実行する必要があります。

移行のシナリオ

このシナリオは段階的に進行します：

1. **各仮想管理サーバーに管理グループを作成**

   オンプレミスで実行されている Kaspersky Security Center でグループを作成します。

2. **顧客のデバイスの移動**

   オンプレミスで実行されている Kaspersky Security Center で、各仮想管理サーバーから、前の手順で作成したそれぞれの管理グループに顧客のデバイスを移動します。

3. **移行**

   管理サーバーの階層を使用しないネットワークの説明に従って移行を実行します。

4. **仮想管理サーバーで管理されているデバイスを移動（任意のステップ）**

   仮想管理サーバーで顧客を管理する場合は、仮想管理サーバーで管理されている管理グループからデバイスを移動します。

5. **ポリシー、タスク、レポートを作成**

   必要に応じて、ポリシー、タスク、レポートを作成します。

結果

移行の完了後に、移行が成功したことを確認できます：

- ネットワークエージェントは、すべての管理対象デバイスに再インストールされます。
- すべてのデバイスは、Kaspersky Security Center Cloud コンソールによって管理されます。
- 移行前に有効だったオブジェクト設定はすべて維持されます。

シナリオ：仮想管理サーバーがある場合の手動での移行

オンプレミスで実行されている Kaspersky Security Center Webコンソールから Kaspersky Security Center Cloud コンソールに手動で移行できます。

必須条件

移行する前に、オンプレミスで実行されている管理サーバーをバージョン 12 以降にアップグレードし、Kaspersky Security Center Cloud コンソールでサポートされるバージョンに管理対象アプリケーションをアップグレードするなど、いくつかの処理を実行する必要があります。

移行のシナリオ

このシナリオは段階的に進行します：

1. **各仮想管理サーバーに管理グループを作成**

   Kaspersky Security Center Cloud コンソールで、各仮想管理サーバーに対応する管理グループを作成します。

2. **ネットワークエージェントのスタンドアロンインストールパッケージの作成**

   ネットワークエージェントのスタンドアロンインストールパッケージを作成します。作成時に、前のステップで作成した管理グループを指定します。したがって、各管理グループに個別のスタンドアロンインストールパッケージを作成する必要があります。

   このステップは Kaspersky Security Center Cloud コンソールで実行します。

3. **スタンドアロンインストールパッケージのダウンロード**

前のステップで作成したスタンドアロンインストールパッケージをダウンロードします。このステップは Kaspersky Security Center Cloud コンソールで実行します。

4. **各スタンドアロンインストールパッケージのアーカイブの作成**

   使用可能なアーカイブ種別は ZIP、CAB、TAR、または TAR.GZ です。

5. **ネットワークエージェントのカスタムインストールパッケージの作成**

   ネットワークエージェントのカスタムインストールパッケージを作成します。作成時に、前のステップで作成したアーカイブを使用します。

   このステップは、オンプレミスで実行されている Kaspersky Security Center で実行します。

6. **リモートインストールタスクの作成**

   作成したカスタムインストールパッケージからネットワークエージェントをインストールするリモートインストールタスクを作成します。

   タスクの作成時に、対応する管理グループを指定します。

   このステップは、オンプレミスで実行されている Kaspersky Security Center で実行します。

7. **作成したリモートインストールタスクの実行**

   ネットワークエージェントがアップデートされます。Kaspersky Security Center Cloud コンソール管理サーバーがそれらの管理を引き継ぎます。

   すべてのデバイスが Kaspersky Security Center Cloud コンソールに移行され、ネットワークエージェントのスタンドアロンインストールパッケージの作成時に指定した管理グループに配置されます。

8. **仮想管理サーバーで管理されているデバイスを移動（任意のステップ）**

   仮想管理サーバーで顧客を管理する場合は、仮想管理サーバーで管理されている管理グループからデバイスを移動します。

9. **ポリシー、タスク、レポートを作成**

   必要に応じて、ポリシー、タスク、レポートを作成します。

結果

移行の完了後に、移行が成功したことを確認できます：

- ネットワークエージェントは、すべての管理対象デバイスに再インストールされます。
- すべてのデバイスは、Kaspersky Security Center Cloud コンソールによって管理されます。

  移行前に有効だったオブジェクト設定はすべて維持されます。

シナリオ：仮想サーバーで管理されている管理グループからのデバイスの移動

仮想管理サーバーでの顧客の管理が必要になる場合があります。オンプレミスの Kaspersky Security Center から Kaspersky Security Center Cloud コンソールにデバイスとその他の項目を移行した場合、デバイスは管理グループに配置されます。仮想管理サーバーを使用して顧客のデバイスを管理するには、管理グループから仮想管理サーバーの管理下にデバイスを移動する必要があります。

必須条件

各顧客に仮想管理サーバーを作成した。

各顧客のすべてのデバイスが個別の管理グループに配置されている。

実行するステップ

このシナリオは段階的に進行します：

1. **ネットワークエージェントのスタンドアロンインストールパッケージの作成**

   作成した各仮想管理サーバーに切り替えて、ネットワークエージェントのスタンドアロンインストールパッケージを作成します。メインメニューで現在の管理サーバー名の右側にあるシェブロンアイコン（  ）をクリックして、必要な管理サーバーを選択すると、管理サーバーを切り替えることができます。

2. **スタンドアロンインストールパッケージのダウンロード**

   前のステップで作成したスタンドアロンインストールパッケージをダウンロードします。

3. **各スタンドアロンインストールパッケージのアーカイブの作成**

   使用可能なアーカイブ種別は ZIP、CAB、TAR、または TAR.GZ です。

4. **ネットワークエージェントのカスタムインストールパッケージの作成**

   ネットワークエージェントのカスタムインストールパッケージを作成します。作成時に、前のステップで作成したアーカイブを使用します。

   このステップはプライマリ管理サーバーで実行します。

5. **リモートインストールタスクの作成**

   作成したカスタムインストールパッケージからネットワークエージェントをインストールするリモートインストールタスクを作成します。

   タスクの作成時に、対応する管理グループを指定します。

   このステップはプライマリ管理サーバーで実行します。

6. **作成したリモートインストールタスクの実行**

   ネットワークエージェントがアップデートされます。デバイスが仮想管理サーバーの管理下に移動されます。

7. **ポリシー、タスク、レポートを作成**

   必要に応じて、ポリシー、タスク、レポートを作成します。

結果

仮想管理サーバーを使用して、移行された顧客のデバイスを管理できるようになりました。

クイックスタートウィザード

このセクションでは、Kaspersky Security Center Cloud コンソールのクイックスタートウィザードについて説明します。

クイックスタートウィザードの概要

Kaspersky Security Center Cloud コンソールのクイックスタートウィザードでは、必要最小限のタスクとポリシーを作成し、設定を最小限に調整して、カスペルスキー製品のインストールパッケージの作成を開始できます。ウィザードを使用すると、Kaspersky Security Center Cloud コンソールで次のような変更を実行できます：

- 管理対象のカスペルスキー製品のインストールパッケージのダウンロードを開始します。
- Windows、Linux、または macOS を実行しているデバイス用に、ネットワークエージェントのスタンドアロンインストールパッケージを作成します。
- Kaspersky Security Center ネットワークエージェントのポリシーを作成します。
- *ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを作成します。
- 管理対象のカスペルスキー製品のポリシーとタスクを作成します。
- Kaspersky Security Network（KSN）との対話を設定します。

クイックスタートウィザードの完了後、［**検出と製品の導入**］→［**導入と割り当て**］の順に選択すると、［**インストールパッケージ**］のリストにネットワークエージェントのインストールパッケージと管理対象のカスペルスキー製品が表示されます。

［管理対象デバイス］グループで該当するポリシーが作成されている場合を除き、クイックスタートウィザードでは Kaspersky Endpoint Security for Windows などの管理対象アプリケーションのポリシーが作成されます。クイックスタートウィザードでは、［管理対象デバイス］グループに同じ名前のタスクが作成されていない場合にタスクを作成します。

会社のワークスペースの作成後、Kaspersky Security Center Cloud コンソールの初回の起動時に、Kaspersky Security Center Cloud コンソールからクイックスタートウィザードを実行するよう自動的に要求されます。また、クイックスタートウィザードはいつでも手動で起動できます。

クイックスタートウィザードの起動

会社のワークスペースの作成後、Kaspersky Security Center Cloud コンソールの初回の起動時に、Kaspersky Security Center Cloud コンソールからクイックスタートウィザードを実行するよう自動的に要求されます。また、クイックスタートウィザードはいつでも手動で起動できます。

クイックスタートウィザードを再度起動した場合、ウィザードの前回の実行で作成されたタスクとポリシーは再び作成されません。

クイックスタートウィザードを手動で起動するには：

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**全般**］セクションを選択します。

3. ［**クイックスタートウィザードを開始**］をクリックします。

   または、［**検出と製品の導入**］→［**導入と割り当て**］→［**クイックスタートウィザード**］の順に選択して、クイックスタートウィザードを起動できます。

ウィザードにより、Kaspersky Security Center Cloud コンソールの初期設定を実行するよう要求されます。ウィザードの指示に従ってください。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。ウィザードで前のステップに戻るには、［**戻る**］を使用します。

ステップ1：ダウンロードするインストールパッケージの選択

リストの中で、クライアントデバイスにインストールするカスペルスキー製品を選択します。Kaspersky Security Center Cloud コンソールにより、選択した製品のインストールパッケージが作成されます。後程、作成されたインストールパッケージは製品のインストールに使用します。

ダウンロードするインストールパッケージの選択時は、言語に注意してください。インストールパッケージには複数の言語版があります。

次の製品を選択します：

- Kaspersky Security Center ネットワークエージェント

  ネットワークエージェントのインストールパッケージの選択時は、以下を考慮します：

  - ネットワークエージェントは各クライアントデバイスにインストールされている必要があります。したがって、クライアントデバイスで実行されている各オペレーティングシステムに適切なネットワークエージェントを選択します。

  - ディストリビューションポイントとして機能するように選択したデバイスでは、スタンドアロンインストールパッケージを使用してネットワークエージェントを手動でインストールする必要があります。ディストリビューションポイントは、ネットワークポーリングや、クライアントデバイスに対するカスペルスキーのセキュリティ製品のリモートインストールを実行するために必要です。そのため、ネットワークエージェントのインストールパッケージを1つ以上選択する必要があります。ウィザードで次のステップに進むと、Kaspersky Security Center Cloud コンソールによってネットワークエージェントのスタンドアロンインストールパッケージが作成されます。

    Windows ベースのディストリビューションポイントと比較して、Linux ベースおよび macOS ベースのディストリビューションポイントは機能が制限されています。Windows ベースのコンピューターをディストリビューションポイントにすることを強く推奨します。

    Windows、Linux、macOS 用のネットワークエージェントを選択できます。1つのオペレーティングシステム（たとえば macOS）用にのみネットワークエージェントを選択すると、スタンドアロンインストールパッケージは選択したオペレーティングシステム用に作成されます。複数のオペレーティングシステム用にネットワークエージェントを選択すると、Windows、Linux、macOS の順の優先度で、Kaspersky Security Center Cloud コンソールによってスタンドアロンインストールパッケージが1つのみ作成されます。たとえば、Linux と macOS 用にネットワークエージェントを選択すると、Kaspersky Security Center Cloud コンソールによって Linux 用のネットワークエージェントのスタンドアロンインストールパッケージが作成されます。これらのオペレーティングシステム用に、いつでもネットワークエージェントのスタンドアロンインストールパッケージを作成できます。

- カスペルスキーのセキュリティ製品

  組織のクライアントデバイスにインストールされているオペレーティングシステムに適切なインストールパッケージを選択します。

ステップ 2：プロキシサーバーの設定

インターネット接続にプロキシサーバーを組織が使用している場合、ウィザードのこのステップでプロキシサーバー設定を指定します。これらの設定はネットワークエージェントのインストールパッケージに追加されます。インストール後、ネットワークエージェントはこれらの設定を各クライアントデバイスで自動的に使用します。

プロキシサーバーの接続には、次の設定を行います：

- **プロキシサーバーを使用する**
- **アドレス**
- **ポート番号**
- **プロキシサーバー認証**

  このオプションをオンにすると、入力フィールドでプロキシサーバー認証の資格情報を指定できます。

  プロキシサーバー認証に必要な最小限の権限が付与されているアカウントの資格情報を指定することを推奨します。

  既定では、このオプションはオフです。

- **ユーザー名**

  プロキシサーバーへの接続の確立に使用されるアカウントのユーザー名。

  プロキシサーバー認証に必要な最小限の権限が付与されているアカウントの資格情報を指定することを推奨します。

- **パスワード**

  プロキシサーバーへの接続の確立に使用されるアカウントのパスワード。

  プロキシサーバー認証に必要な最小限の権限が付与されているアカウントの資格情報を指定することを推奨します。

ステップ 3：Kaspersky Security Network の設定

ウィザードの最初のステップで Kaspersky Endpoint Security for Windows のインストールパッケージをダウンロードした場合は、次の製品の KSN に関する声明の内容が表示されます：

- Kaspersky Endpoint Security for Windows
- ローカルデバイスにインストールされている Kaspersky Security Center
- クラウド環境にインストールされている Kaspersky Security Center Cloud コンソール

Kaspersky Endpoint Security for Windows をダウンロードしなかった場合、この製品の KSN に関する声明は表示されません。

試用モードでは、Kaspersky Endpoint Security for Windows の KSN に関する声明のみ表示されます。

Kaspersky Security Network に関する声明をよくお読みください。次のいずれかのオプションをオンにします：

- **Kaspersky Security Network への参加に同意する**

  Kaspersky Security Center Cloud コンソールとクライアントデバイスにインストールされている管理対象製品は、自動的に動作情報を Kaspersky Security Network に送信します。Kaspersky Security Network への参加により、ウイルスなどの脅威に関する情報を含んだデータベースのアップデートをより迅速に入手できるため、セキュリティへの緊急の脅威にすぐに対応できます。

- **Kaspersky Security Network への参加に同意しない**

  Kaspersky Security Center Cloud コンソールと管理対象製品は、Kaspersky Security Network に対して情報を提供しません。

  このオプションをオンにすると、Kaspersky Security Network の使用がオフになります。

既定では、KSN への参加はオフです。後で KSN への参加について変更する場合は、管理サーバーのプロパティウィンドウの［**KSN 設定**］セクションで、該当するオプションをオン（またはオフ）にできます。

ステップ 4：サードパーティ製品のアップデート管理設定

［*脆弱性とアプリケーションのアップデートの検索*］タスクが既に存在する場合、このステップは表示されません。

管理対象デバイスにインストールされているアプリケーションのアップデートのリスト、および検知された脆弱性とそれに対して推奨される修正のリストを取得する場合は、［**サードパーティ製品のアップデートと脆弱性修正プログラムの検索**］をオンにします。このオプションをオンにすると、Kaspersky Security Center Cloud コンソールによって［*脆弱性とアプリケーションのアップデートの検索*］タスクが作成されます。

ステップ 5：基本的なネットワーク保護の設定情報の作成

ウィザードのこのステップで、［**作成**］をクリックして、クライアントデバイスの初期保護に必要なオブジェクトを作成します。

Kaspersky Security Center Cloud コンソールによって 2 つの処理が実行されます：

- 既定の設定の基本的なポリシーとタスクの作成

  次のポリシーが作成されます：

  - Kaspersky Security Center ネットワークエージェントのポリシー

- 管理対象のカスペルスキー製品のポリシー

次のタスクが作成されます：

- *ディストリビューションポイントのリポジトリにアップデートをダウンロードタスク*
- *脆弱性とアプリケーションのアップデートの検索タスク*
  ウィザードの前のステップで［**サードパーティ製品のアップデートと脆弱性修正プログラムの検索**］をオンにした場合のみ、このタスクが作成されます。
- 管理対象のカスペルスキー製品のタスク

- ネットワークエージェントのスタンドアロンインストールパッケージの作成

  このパッケージを使用して、ディストリビューションポイントにネットワークエージェントをインストールします。ウィザードの前のステップで選択したネットワークエージェントのインストールパッケージに基づいて、Kaspersky Security Center Cloud コンソールによってスタンドアロンインストールパッケージが作成されます。パッケージの作成時、ネットワークエージェントの EULA の条項を読んで同意する必要があります。スタンドアロンインストールパッケージが作成されると、その時使用しているデバイスにダウンロードするよう要求されます。

  ネットワークエージェントのスタンドアロンインストールパッケージの作成には時間がかかる場合があります。ウィザードで次のステップに進むことができます。プロセスはバックグラウンドモードで続行します。プロセスは、［**インストールパッケージ**］セクション（［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］）の［**実行中（）**］タブで追跡できます。

  認証のため、各スタンドアロンインストールパッケージは証明書を使用して署名されています。証明書は定期的に再発行されます。証明書の再発行の各手順後、作成されたすべてのスタンドアロンインストールパッケージの署名が Kaspersky Security Center Cloud コンソールによって自動的にアップデートされます。ダウンロードしたスタンドアロンインストールパッケージに対しては、署名の自動アップデートを実行できません。したがって、証明書の有効期間が終了し、スタンドアロンインストールパッケージからの製品のインストール中に証明書エラーが発生する場合があります。この場合は、スタンドアロンインストールパッケージを再びダウンロードしてください。

ステップ 6：クイックスタートウィザードの終了

クイックスタートウィザードの完了ページで、カスペルスキーのセキュリティ製品をクライアントデバイスに導入するために実行する必要がある追加の操作について確認します。カスペルスキー製品の初期導入のシナリオに記載されている手順に従います。

カスペルスキー製品の初期導入

このセクションでは、組織のクライアントデバイスに対するカスペルスキー製品の初期導入について説明します。

シナリオ：カスペルスキー製品の初期導入

このシナリオでは、Kaspersky Security Center Cloud コンソールでクライアントデバイスにカスペルスキー製品をインストールする方法について説明します。最初に、ディストリビューションポイントをネットワークに導入する必要があります。続いて、ディストリビューションポイントを使用し、ネットワークポーリングを実行してネットワーク接続されたデバイスを検出する必要があります。その後、ネットワーク接続されたデバイスにカスペルスキー製品を導入できます。

シナリオを完了すると、組織ネットワーク内の選択したクライアントデバイスにカスペルスキー製品が導入されます。カスペルスキー製品をインストールしたすべてのデバイスを管理できます。

必須条件

開始する前に、次の前提条件が満たされていることを確認してください：

- クイックスタートウィザードが終了した。
- ネットワークエージェントとセキュリティ製品のインストールパッケージが作成された。
- 管理対象デバイスのファイアウォールの例外に、アドレス https://aes.s.kaspersky-labs.com/endpoints/ が含まれている。
- 組織のクライアントデバイスのインターネット設定に関する情報、ゲートウェイに関する情報、プロキシサーバー設定について把握している。

実行するステップ

カスペルスキー製品の初期導入は、以下の手順で進みます：

1. **ディストリビューションポイントとして動作するデバイスの選択**

   Kaspersky Security Center Cloud コンソールで、ディストリビューションポイントは以下の目的で使用されます：

   - ネットワークポーリングとデバイスの検索
   - クライアントデバイスに対するネットワークエージェントのリモートインストール
   - 管理サーバーへのクライアントデバイスの接続（ディストリビューションポイントが接続ゲートウェイとして動作する場合）

   管理グループのディストリビューションポイントとして動作するデバイスを、組織のネットワークで選択します。選択したデバイスはディストリビューションポイントの要件を満たしている必要があります。組織のネットワークにあるクライアントデバイスの数に応じて、正しい数のディストリビューションポイントとして動作するデバイスを選択します。

2. **ネットワークエージェントのスタンドアロンインストールパッケージの作成**

ディストリビューションポイントにインストールする、ネットワークエージェントのスタンドアロンインストールパッケージを作成します。

クライアントデバイスがインターネットを介して管理サーバーに直接アクセスできない場合、ネットワークエージェントのインストールパッケージの設定で、接続ゲートウェイとプロキシサーバー設定を設定します。

3. **選択したディストリビューションポイントとして動作するデバイスへのネットワークエージェントのインストール**

任意の方法で、ネットワークエージェントのスタンドアロンインストールパッケージを選択したデバイスに配布します。たとえば、スタンドアロンインストールパッケージをリムーバブルドライブ（フラッシュドライブなど）にコピーしたり、共有フォルダーに配置したりできます。

スタンドアロンインストールパッケージファイルの［**プロパティ**］ウィンドウで、ネットワークエージェントのスタンドアロンインストールパッケージがカスペルスキーによって署名されていることを確認します。

選択したデバイスで、ネットワークエージェントのスタンドアロンインストールパッケージのインストールを実行します。ネットワークエージェントのインストールパッケージの設定に応じてネットワークエージェントがインストールされ、管理サーバーに接続されます。ネットワークエージェントのスタンドアロンインストールパッケージの作成時に指定した管理グループに、ネットワークエージェントをインストールしたデバイスが配置されます。

Microsoft Windows XP Professional for Embedded Systems の 32 ビットを実行しているデバイスに、スタンドアロンインストールパッケージを使用してネットワークエージェントをインストールすると、インストールは失敗します。この問題を解決するには、Microsoft の Web サイト（https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626）から WindowsXP 用の更新プログラム KB2868626 を事前にインストールしてください。

4. **ネットワークエージェントをインストールしたデバイスのディストリビューションポイントとしての割り当て**

ネットワークエージェントをインストールしたデバイスをディストリビューションポイントとして割り当てます。

5. **ディストリビューションポイントでのネットワークポーリングの設定と実行**

ネットワークエージェントをインストールしたディストリビューションポイントでネットワークポーリングを設定します。オプションとして、ネットワークエージェントのポリシーでネットワークポーリングを設定できます。

スケジュールに応じたネットワークポーリングの完了後、組織のネットワークに接続されているクライアントデバイスが検出され、［**未割り当てデバイス**］グループに配置されます。

6. **ネットワークエージェントと管理対象のカスペルスキー製品のインストールパッケージの作成**

クイックスタートウィザードを起動しなかった、またはインストールパッケージを作成するステップを省略した場合は、カスペルスキー製品のインストールパッケージを作成します。組織のネットワークのクライアントデバイスにインストールされているオペレーティングシステムに適したインストールパッケージを、ネットワークエージェントと管理対象のカスペルスキー製品の両方に作成する必要があります。

7. **サードパーティのセキュリティ製品の削除**

組織のネットワークのクライアントデバイスにサードパーティのセキュリティ製品がインストールされている場合は、カスペルスキー製品をインストールする前に削除します。

8. **クライアントデバイスへのカスペルスキー製品のインストール**

組織のネットワークのクライアントデバイスに、ネットワークエージェントと管理対象のカスペルスキー製品をインストールするためのタスクを作成します。タスクの作成時は、［**アプリケーションのリモートインストール**］のタスク種別を使用します。ネットワークエージェントをインストールするタスクには、［**ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**］を使用します。管理対象のカスペルスキー製品をインストールするタスクには、［**ネットワークエージェントを使用する**］を使用します。タスクの作成後、それらの設定を構成できます。各タスクのスケジュールが要件に合致しているかを確認します。最初に、ネットワークエージェントをインストールするタスクを実行する必要があります。続いて、クライアントデバイスへのネットワークエージェントのインストール後、管理対象のカスペルスキー製品をインストールするタスクを実行する必要があります。

オプションとして、組織のネットワークのクライアントデバイスにネットワークエージェントと管理対象のカスペルスキー製品をインストールするためのリモートインストールタスクを1つ作成することができます。この場合は、［**インストールパッケージ**］セクションで［**インストールパッケージの選択**］と［**ネットワークエージェントの選択**］をオンにし、［**インストールパッケージの強制ダウンロード**］セクションで［**ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**］をオンにします。

異なる管理グループや異なるデバイスの抽出を対象に、管理対象のカスペルスキー製品をインストールするための複数のリモートインストールタスクを作成することもできます。

ディストリビューションポイントを割り当てたネットワークに含まれないクライアントデバイスがある場合（リモートユーザーのノート PC など）、それらのクライアントデバイスにネットワークエージェントのスタンドアロンインストールパッケージを任意の方法で配布する必要があります。ネットワークエージェントのスタンドアロンインストールパッケージをクライアントデバイスのローカルにインストールします。その後、ディストリビューションポイントで検出されたその他のデバイスの場合と同じ手順で、それらのリモートユーザーのデバイスに管理対象のカスペルスキー製品をインストールできます。

リモートインストールタスクを実行します。

オプションとして、製品導入ウィザードを起動してカスペルスキー製品をインストールできます。

9. **Kaspersky Security for Mobile のインストール**

   企業のモバイルデバイスを管理する場合は、Kaspersky Security for Mobile のヘルプ の手順に従って Kaspersky Endpoint Security for Android を導入してください。

10. **カスペルスキー製品の初期導入の確認**

    カスペルスキー製品バージョンレポートを生成して表示します。管理対象のカスペルスキー製品が組織のすべてのクライアントデバイスにインストールされていることを確認します。

ディスク全体の暗号化の場合、Kaspersky Security Center Cloud コンソールは BitLocker のみをサポートします。

カスペルスキー製品のインストールパッケージの作成

カスペルスキー製品を組織のネットワーク接続されたデバイスに導入するには、Kaspersky Security Center Cloud コンソールでカスペルスキー製品のインストールパッケージを作成する必要があります。

カスペルスキー製品のインストールパッケージを作成するには：

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に選択します。
   - メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

画面表示による通知のリストでも、新しいパッケージに関する通知を確認できます。新しいパッケージに関する通知が表示されている場合、通知に隣接するリンクをクリックし、使用可能なインストールパッケージのリストを表示できます。

管理サーバーで使用可能なインストールパッケージのリストが表示されます。

2. ［**追加**］をクリックします。

新規パッケージウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ウィザードの最初のページで、［**カスペルスキー製品のインストールパッケージを作成する**］を選択します。

カスペルスキーの Web サーバーで使用可能な配布パッケージのリストが表示されます。

4. 配布パッケージの名前（たとえば「**Kaspersky Endpoint Security for Windows (<バージョン番号>)**」など）をクリックします。

配布パッケージに関する情報を確認できるウィンドウが表示されます。

5. 情報を確認し、［**ダウンロードしてインストールパッケージを作成**］をクリックします。

配布パッケージをインストールパッケージに自動的に変換できない場合、［**ダウンロードしてインストールパッケージを作成**］の代わりに［**配布パッケージをダウンロード**］が表示されます。この場合、配布パッケージをダウンロードして、ダウンロードしたファイルを使用してカスタムインストールパッケージを作成します。

インストールパッケージのダウンロードが開始されます。ウィザードのウィンドウを閉じるか、手順の次のステップに進むことができます。ウィザードのウィンドウを閉じると、ダウンロードプロセスはバックグラウンドモードで続行されます。

インストールパッケージのダウンロードプロセスを追跡する場合：

a. メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］→［**実行中（）**］の順に選択します。

b. 操作の進捗状況を表の［**ダウンロードの進行状況**］列と［**ダウンロード状況**］列で追跡します。

プロセスが完了すると、インストールパッケージが［**ダウンロード済み**］タブのリストに追加されます。ダウンロードプロセスが停止し、ダウンロードの状況が［**使用許諾契約書に同意する**］に切り替わったら、インストールパッケージ名をクリックして、手順の次のステップに進みます。

Kaspersky Security Center Cloud コンソールに Kaspersky Security Center Web コンソールから移行する計画があり、組織のセキュリティ規則で企業ネットワークへのアクセスにプロキシの使用が必要とされている場合は、移行プロセスに影響がある可能性があります。ネットワークエージェントのインストールパッケージの作成後、Kaspersky Security Center Cloud コンソールのワークスペースと管理対象デバイスのネットワークエージェントのインスタンスとの間で確実に接続できるように、プロキシ設定を指定する必要があります。

a. インストールパッケージ名をクリックします。

b. インストールパッケージのプロパティウィンドウで、［**設定**］タブに移動します。

c. ［**接続**］セクションを開きます。

d. ［**プロキシサーバーを使用する**］をオンにして、［**プロキシサーバーアドレス**］と［**プロキシサーバーのポート**］に入力します。

6. 一部のカスペルスキー製品では、ダウンロードプロセスの途中で［**使用許諾契約書を表示**］が表示されます。この場合は、次の操作を実行します：

a. ［**使用許諾契約書を表示**］をクリックし、使用許諾契約書（EULA）の内容を確認します。

b. 画面に表示された EULA の内容を確認し、［**同意する**］をクリックします。

EULA に同意するとダウンロードを進めることができます。［**同意しない**］をクリックすると、ダウンロードが中止されます。

7. ダウンロードが完了したら、［**閉じる**］（×）をクリックして、配布パッケージに関する情報が表示されているウィンドウを閉じます。

インストールパッケージが作成されます。インストールパッケージがインストールパッケージのリストに表示されます。

セカンダリ管理サーバーへのインストールパッケージの配布

セカンダリ管理サーバーにインストールパッケージを配布するには：

1. 目的のセカンダリ管理サーバーを制御する管理サーバーとの接続を確立します。

2. 次のいずれかの方法で、セカンダリ管理サーバーへのインストールパッケージの配布タスクを作成します：

   - 選択した管理グループ内でセカンダリ管理サーバー用のタスクを作成する場合は、そのグループのグループタスクを作成します。

   - 特定のセカンダリ管理サーバー用のタスクを作成するには、デバイスを指定してタスクを作成します。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。

   タスク追加ウィザードの［**新規タスク**］ウィンドウで、［**タスク種別**］に［**インストールパッケージの配布**］を選択します。［**タスク名**］でタスクの既定の名前を編集することもできます。

   次のステップで、タスク範囲のセカンダリ管理サーバーを指定し、新規タスクウィザードの指示に従います。完了すると、選択したインストールパッケージを特定のセカンダリ管理サーバーに配布するタスクが新規タスクウィザードによって作成されます。

   > オンプレミスで実行されているセカンダリ管理サーバーに対するインストールパッケージの配布タスクを作成すると、［**すべてのインストールパッケージ**］または［**選択されたインストールパッケージ**］のどちらの配布オプションを選択した場合も、配布の範囲（カスタムインストールパッケージは除く）には、オンプレミスで実行されている Kaspersky Security Center Web コンソールでサポートされているカスペルスキー製品のインストールパッケージのみが含まれます。

3. 手動でタスクを実行するか、タスク設定で指定したスケジュールに基づいてタスクが起動するのを待ちます。

選択したインストールパッケージが指定のセカンダリ管理サーバーにコピーされます。

ネットワークエージェントのスタンドアロンイントールパッケージの作成

組織内の管理者とユーザーは、デバイスのローカルにネットワークエージェントをインストールするために、スタンドアロンインストールパッケージを使用できます。Windows、Linux、または macOS を実行するデバイス用にスタンドアロンインストールパッケージを作成できます。

Kaspersky Security Center Cloud コンソールでは、ネットワークエージェント用のスタンドアロンインストールパッケージのみ作成できます。

スタンドアロンインストールパッケージは実行ファイル形式で、メールなどを利用してクライアントデバイスに送信できます。受信した実行ファイルはクライアントデバイスのローカルで実行でき、Kaspersky Security Center Cloud コンソールを使用せずにネットワークエージェントをインストールできるようになります。

Linux 用のネットワークエージェントと macOS 用のネットワークエージェントの場合、スタンドアロンインストールパッケージは拡張子が sh のスクリプトファイルです。このファイルを実行すると、インストールパッケージとその設定を含む添付のアーカイブがスクリプトによって解凍され、インストールが開始されます。

Microsoft Windows XP Professional for Embedded Systems の 32 ビットを実行しているデバイスに、スタンドアロンインストールパッケージを使用してネットワークエージェントをインストールすると、インストールは失敗します。この問題を解決するには、Microsoft の Web サイト（https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626）から WindowsXP 用の更新プログラム KB2868626 を事前にインストールしてください。

認証のため、各スタンドアロンインストールパッケージは証明書を使用して署名されています。証明書は定期的に再発行されます。証明書の再発行の各手順後、作成されたすべてのスタンドアロンインストールパッケージの署名が Kaspersky Security Center Cloud コンソールによって自動的にアップデートされます。ダウンロードしたスタンドアロンインストールパッケージに対しては、署名の自動アップデートを実行できません。したがって、証明書の有効期間が終了し、スタンドアロンインストールパッケージからの製品のインストール中に証明書エラーが発生する場合があります。この場合は、スタンドアロンインストールパッケージを再びダウンロードしてください。

スタンドアロンインストールパッケージを作成するには：

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に選択します。
   - メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

   インストールパッケージのリストが表示されます。ネットワークエージェントのインストールパッケージがリストにない場合、手動でこのインストールパッケージを作成します。

2. インストールパッケージのリストで、ネットワークエージェントのインストールパッケージの名前をクリックします。

   ネットワークエージェントのインストールパッケージのプロパティウィンドウが表示されます。

3. 必要に応じてネットワークエージェントのインストールパッケージの設定を構成し、ネットワークエージェントのインストールパッケージのプロパティウィンドウを閉じます。

4. インストールパッケージのリストでインストールパッケージを選択し、リストの上にある［**製品の導入**］をクリックします。

5. ［**スタンドアロンパッケージを使用**］を選択します。

   スタンドアロンインストールパッケージ作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

6. 選択したアプリケーションとネットワークエージェントを合わせてインストールする場合、ウィザードの最初のページで［**このアプリケーションと同時にネットワークエージェントをインストールする**］がオンであることを確認します。

既定では、このオプションはオンです。デバイスにネットワークエージェントがインストール済みかどうかが不明な場合は、このオプションをオンにすることを推奨します。ネットワークエージェントがデバイスにインストールされている場合、ネットワークエージェントを含めたインストールパッケージがインストールされた時にネットワークエージェントが新しいバージョンにアップデートされます。

このオプションがオフの場合、デバイスにはネットワークエージェントはインストールされず、デバイスは管理対象外のデバイスになります。

選択したアプリケーションのスタンドアロンインストールパッケージが既に管理サーバー上に存在する場合、ウィザードに通知が表示されます。この場合、次のいずれかのオプションを選択する必要があります：

- **スタンドアロンインストールパッケージの作成**：新しいバージョンのアプリケーションのスタンドアロンインストールパッケージを新規に作成し、なおかつ旧バージョンのアプリケーションで作成したスタンドアロンインストールパッケージも保持する場合などにこのオプションを選択します。新しいスタンドアロンインストールパッケージは別のフォルダーに配置されます。

- **既存のスタンドアロンインストールパッケージを使用**：既存のスタンドアロンインストールパッケージを使用する場合は、このオプションをオンにします。パッケージの作成プロセスは開始されません。

- **既存のスタンドアロンインストールパッケージを再構築**：同じアプリケーションのインストールパッケージを再作成する場合、このオプションを選択します。スタンドアロンインストールパッケージは、同じフォルダーに保存されます。

7. ウィザードの［**管理対象デバイスのリストへ移動**］ページで、既定では［**デバイスを移動しない**］が選択されています。ネットワークエージェントのインストール後にクライアントデバイスをどの管理グループにも移動したくない場合は、オプションの選択を変更しないでください。

   ネットワークエージェントのインストール後にクライアントデバイスを移動したい場合は、［**未割り当てデバイスをこのグループへ移動**］を選択し、クライアントデバイスの移動先の管理グループを指定します。既定では、デバイスは［**管理対象デバイス**］グループに移動されます。

8. ウィザードの終了後にスタンドアロンインストールパッケージのリストを表示する場合は、ウィザードの次のページで［**スタンドアロンパッケージのリストを開く**］をオンにします。

9. ［**終了**］をクリックします。

   スタンドアロンインストールパッケージ作成ウィザードが閉じます。

ネットワークエージェントのスタンドアロンインストールパッケージが作成されます。作成されたスタンドアロンインストールパッケージが、スタンドアロンインストールパッケージのリストに表示されます。

スタンドアロンインストールパッケージのリストの表示

スタンドアロンインストールパッケージのリストを表示し、それぞれのスタンドアロンインストールパッケージのプロパティを確認できます。

すべてのインストールパッケージについて、対応するスタンドアロンインストールパッケージのリストを表示するには：

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に選択します。

   - メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

インストールパッケージのリストが表示されます。

2. リストの上にある［**スタンドアロンパッケージリストの表示**］をクリックします。

スタンドアロンインストールパッケージのリストが表示されます。

スタンドアロンインストールパッケージのリストで、パッケージのプロパティが次のように表示されます。

- **パッケージ名**：パッケージに含まれるアプリケーション名とバージョン番号を組み合わせて自動的に作成されるスタンドアロンインストールパッケージの名前。
- **ネットワークエージェントのインストールパッケージ名**。
- **ネットワークエージェントのバージョン**。
- **サイズ**：ファイルのサイズ（MB 単位）。
- **グループ**：ネットワークエージェントのインストール後にクライアントデバイスが移動する管理グループの名前。
- **作成日時**：スタンドアロンインストールパッケージが作成された日時。
- **変更日時**：スタンドアロンインストールパッケージが変更された日時。
- **ファイルのハッシュ**：このプロパティは、スタンドアロンインストールパッケージが第三者による改竄を受けておらず、管理者が作成してユーザーに送信したのと同じファイルがユーザーの手元にあるかどうかを検証するために使用します。

特定のインストールパッケージについて、対応するスタンドアロンインストールパッケージのリストを表示するには：

リストからインストールパッケージを選択し、リストの上にある［**スタンドアロンパッケージリストの表示**］をクリックします。

スタンドアロンインストールパッケージのリストを使用して、次の操作を実行できます：

- ［**ダウンロード**］をクリックして、スタンドアロンインストールパッケージを操作中のデバイスにダウンロードする。

  認証のため、各スタンドアロンインストールパッケージは証明書を使用して署名されています。証明書は定期的に再発行されます。証明書の再発行の各手順後、作成されたすべてのスタンドアロンインストールパッケージの署名が Kaspersky Security Center Cloud コンソールによって自動的にアップデートされます。ダウンロードしたスタンドアロンインストールパッケージに対しては、署名の自動アップデートを実行できません。したがって、証明書の有効期間が終了し、スタンドアロンインストールパッケージからの製品のインストール中に証明書エラーが発生する場合があります。この場合は、スタンドアロンインストールパッケージを再びダウンロードしてください。

- ［**削除**］をクリックして、スタンドアロンインストールパッケージを削除する。

カスタムインストールパッケージの作成

以下のような用途でカスタムインストールパッケージを使用できます：

- Kaspersky Security Center Cloud コンソールを使用して（たとえばタスクにより）、サードパーティ製を含む任意のアプリケーション（テキストエディターなど）をクライアントデバイスにインストールするため。

- スタンドアロンインストールパッケージを作成するため。

カスタムインストールパッケージは、実行ファイルなどの複数のファイルを含んだフォルダーです。カスタムインストールパッケージは、圧縮ファイルを元に作成します。圧縮ファイルには、カスタムインストールパッケージに含める必要のあるファイルが含まれているようにします。カスタムインストールパッケージの作成時には、コマンドラインオプションを指定できます（例：製品をサイレントモードでインストールするオプション）。

カスタムインストールパッケージを作成するには：

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に選択します。

   - メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

   管理サーバーで使用可能なインストールパッケージのリストが表示されます。

2. ［**追加**］をクリックします。

   新規パッケージウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ウィザードの最初のページで、［**インストールパッケージをファイルから作成する**］を選択します。

4. ウィザードの次のページで、インストールパッケージ名を入力して［**参照**］をクリックします。

   標準の［**開く**］ウィンドウで、インストールパッケージを作成するための圧縮ファイルを選択できます。

5. 事前に準備しておいた圧縮ファイルを選択します。

   ZIP、CAB、TAR、または TAR.GZ ファイルをアップロードできます。インストールパッケージを SFX ファイル（自己解凍型の圧縮ファイル）から作成することはできません。

   ファイルは Kaspersky Security Center Cloud コンソール管理サーバーにダウンロードされます。

   圧縮ファイルにカスペルスキー製品が含まれていることが管理サーバーによって検出されると、エラーメッセージが表示されます。カスペルスキー製品のインストールパッケージは、カスペルスキーの Web サーバーからダウンロードできます。この操作は、［**操作**］→［**カスペルスキー製品**］→［**現在入手可能な製品バージョン**］の順に選択することで実行できます。

6. 選択した圧縮ファイルに複数の実行ファイルが含まれている場合、ウィザードの次のページで、作成したインストールパッケージを使用して製品をインストールするために実行する必要がある実行ファイルを1つ選択します。

7. 必要に応じて、実行ファイルにコマンドラインのパラメータを指定できます。

   インストールパッケージから製品をサイレントモードでインストールするためのコマンドラインのパラメータを指定できます。コマンドラインのパラメータの詳細については、製品の開発元のガイドを参照してください。

   インストールパッケージの作成が開始されます。

   プロセスが終了すると、ウィザードで通知されます。

   インストールパッケージが作成されなかった場合は、エラーメッセージが表示されます。

Kaspersky Security Center Cloud コンソールでは、管理サーバーのインストールパッケージの合計サイズは 500 MB が上限です。インストールパッケージの作成プロセスで合計サイズの上限を超えた場合は、以前作成したインストールパッケージを削除します。インストールパッケージのサイズはそのプロパティに表示されます。

8. ［**終了**］をクリックしてウィザードを終了します。

作成されたカスタムインストールパッケージが管理サーバーにダウンロードされます。ダウンロード後、インストールパッケージがインストールパッケージのリストに表示されます。

インストールパッケージのリストで、カスタムインストールパッケージの次のプロパティを確認できます：

- **名前**：カスタムインストールパッケージの名前。
- **ソース**：アプリケーションの開発元の名前。
- **アプリケーション**：カスタムインストールパッケージに含まれるアプリケーションの名前。
- **バージョン**：アプリケーションのバージョン。
- **言語**：カスタムインストールパッケージに含まれるアプリケーションの言語。
- **サイズ（MB）**：カスタムインストールパッケージのサイズ。
- **オペレーティングシステム**：カスタムインストールパッケージが作成されたオペレーティングシステム。
- **作成**：インストールパッケージの作成日時。
- **変更**：インストールパッケージの変更日時。
- **種別**：カスペルスキー製品またはサードパーティ製品。

インストールパッケージのリストでカスタムインストールパッケージの名前のリンクをクリックすると、コマンドラインのパラメータとカスタムインストールパッケージ名を変更できます。

ディストリビューションポイントの要件

10,000 台以下のクライアントデバイスでディストリビューションポイントを使用する場合、次の最小要件を満たしている必要があります（テストスタンドでの設定値）：

- CPU：Intel® Core™ i7-7700 CPU（3.60 GHz 4 コア）
- メモリ：8 GB
- 空きストレージ容量：120 GB

また、ディストリビューションポイントではインターネット接続が確保され、デバイスが常時接続されている必要があります。

管理サーバー上でリモートインストールタスクが実行を待っている場合、ディストリビューションポイントがあるデバイスには、インストール対象となるインストールパッケージの合計サイズと同等の空き容量が必要です。

管理サーバー上でアップデート（パッチ）のインストールタスクと脆弱性の修正タスクが1つ以上保留されている場合、ディストリビューションポイントが動作しているデバイスには、インストールするすべてのパッチの合計サイズの2倍の空きディスク容量が追加で必要です。

ネットワークエージェントのポリシー設定

ネットワークエージェントのポリシーを設定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. ネットワークエージェントポリシーの名前をクリックします。
   ネットワークエージェントポリシーのプロパティウィンドウが表示されます。

Windows、macOS、および Linux ベースのデバイスでは、様々な設定が使用可能であることを考慮してください。

［全般］タブ

このタブでは、ポリシーステータスを変更したり、継承ポリシーを設定したりすることができます：

- ［**ポリシーのステータス**］セクションで、ポリシーのステータスを選択します：
  - **アクティブ**
  - **非アクティブ**

    このオプションをオンにすると、ポリシーは非アクティブになりますが［**ポリシー**］フォルダーに保持されます。必要に応じて、ポリシーをアクティブにすることができます。

- ［**設定の継承**］セクションでは、ポリシーの継承を設定できます。
  - **親ポリシーから設定を継承する**

    このオプションをオンにすると、ポリシーの設定値は上位レベルグループのポリシーから継承されるため、ロックされます。

    既定では、このオプションはオンです。

  - **設定を子ポリシーへ強制的に継承させる**

    このオプションをオンにすると、ポリシーの変更を適用した後に次の処理が実行されます：
    - 管理サブグループのポリシー（子ポリシー）に、ポリシーの設定値が継承されます。
    - 各子ポリシーのプロパティウィンドウの［**全般**］セクションにある［**設定の継承**］ブロックで、［**親ポリシーから設定を継承する**］が自動的にオンになります。

    このオプションをオンにすると、子ポリシーの設定はロックされます。

    既定では、このオプションはオフです。

［イベントの設定］タブ

このタブでは、イベントの記録と通知を設定できます。イベントは、［**イベントの設定**］タブの次のセクションの重要度に応じて配信されます：

- **機能エラー**
- **警告**
- **情報**

それぞれのセクションのイベント種別リストには、イベントの種別と、管理サーバーでイベントが保存される既定の日数が表示されます。［**プロパティ**］をクリックすると、リストで選択したイベントについてのイベントログとイベント通知を設定できます。既定では、すべてのイベント種別で、管理サーバー全体を対象に指定された共通の通知設定が使用されます。しかしながら、目的のイベント種別の特定の設定を変更できます。

［アプリケーション設定］タブ

設定

［**設定**］セクションでは、ネットワークエージェントのポリシーを設定できます。

- **ディストリビューションポイント経由でのみファイルを配信する**

  このオプションをオンにすると、クライアントデバイスはアップデートサーバーからではなくディストリビューションポイントからのみアップデートを受信します。

  このオプションをオフにすると、クライアントデバイスは、様々なアップデート元から（アップデートサーバーから直接、ローカルまたはネットワークフォルダーから）アップデートを受信できます。

  既定では、このオプションはオフです。

- **イベントキュー最大サイズを MB で指定**
- **アプリケーションがポリシーの拡張データをデバイスから取得可能である**

  管理対象デバイスにインストールされたネットワークエージェントは、適用されたセキュリティ製品のポリシーに関する情報をセキュリティ製品（たとえば、Kaspersky Endpoint Security for Windows）に転送します。転送された情報は、セキュリティ製品のインターフェイスで表示できます。

  ネットワークエージェントは次の情報を転送します：

  - 管理対象デバイスへのポリシー導入の時間
  - 管理対象デバイスへポリシー導入の時点でのアクティブポリシーまたはモバイルユーザーポリシーの名前
  - 管理対象デバイスへポリシー導入の時点で管理対象デバイスが含まれていた管理グループの名前とフルパス
  - アクティブポリシーのプロファイルのリスト

    情報を使用して、デバイスに正しいポリシーが適用されていることを確認し、トラブルシューティングを行うことができます。既定では、このオプションはオフです。

- **ネットワークエージェントを不正な削除・停止から保護し、設定の変更を防止する**

  このオプションをオンにすると、管理対象デバイスにネットワークエージェントのインストールされた後、必要な権限がない場合はコンポーネントの削除や再設定が行えなくなります。また、ネットワークエージェントサービスを停止できなくなります。このオプションはドメインコントローラーに影響しません。

  ローカル管理者権限で操作されているワークステーション上のネットワークエージェントを保護するには、このオプションをオンにします。

  既定では、このオプションはオフです。

- **アンインストール用パスワードを使用する**

  このオプションをオンにすると、［**変更**］をクリックして、klmover ユーティリティおよびネットワークエージェントのリモートアンインストール時に使用するパスワードを指定できます。

  既定では、このオプションはオフです。

リポジトリ

［**リポジトリ**］セクションでは、情報ネットワークエージェントから管理サーバーに詳細が送信されるオブジェクトの種別を選択できます。このセクションの設定の一部を変更することがネットワークエージェントのポリシーで禁止されている場合、それらの設定を変更することはできません。［**リポジトリ**］セクションの設定は、Windows を実行しているデバイスでのみ使用できます：

- **インストール済みアプリケーションの詳細**
- **パッチの情報を含める**

  クライアントデバイスにインストールされたアプリケーションのパッチに関する情報が管理サーバーに送信されます。このオプションをオンにすると、データベースに保存されるデータの容量が増えるとともに管理サーバーと DBMS での負荷が増大します。

  既定では、このオプションはオンです。Windows でのみ使用できます。

- **Windows Update 更新プログラムの詳細**

  このオプションをオンにすると、クライアントデバイスにインストールする必要のある Microsoft Windows 更新プログラムに関する情報が管理サーバーに送信されます。

  このオプションをオフにしても、［**適用なアップデート**］セクションのデバイスのプロパティに更新プログラムが表示されることがあります。たとえば、組織のデバイスにこれらの更新プログラムによって修正できる脆弱性がある場合などに、こうしたことが起こる可能性があります。

  既定では、このオプションはオンです。Windows でのみ使用できます。

- **ソフトウェアの脆弱性と対応するアップデートの詳細**

このオプションをオンにすると、管理対象デバイスで検出されたサードパーティソフトウェア（Microsoft ソフトウェアを含む）の脆弱性に関する情報、およびサードパーティの脆弱性（Microsoft ソフトウェアを含まない）を修正するソフトウェアアップデートに関する情報が、管理サーバーに送信されます。

このオプション（**ソフトウェアの脆弱性と対応するアップデートの詳細**）を選択すると、ネットワーク負荷、管理サーバーのディスク負荷、およびネットワークエージェントのリソース消費が増加します。

既定では、このオプションはオンです。Windows でのみ使用できます。

Microsoft ソフトウェアのソフトウェアアップデートを管理するには、［**Windows Update 更新プログラムの詳細**］を使用します。

- **ハードウェアレジストリの詳細**

ソフトウェアのアップデートと脆弱性

［**ソフトウェアのアップデートと脆弱性**］セクションでは、Windows アップデートの検索を設定し、実行ファイルの脆弱性のスキャンを有効化できます。［**ソフトウェアのアップデートと脆弱性**］セクションの設定は、Windows を実行しているデバイスでのみ使用できます：

- ［**Kaspersky Security Center 11 がインストールされた管理サーバーデバイスが WSUS サーバーとして使用されている場合に、バージョン 11 以降のネットワークエージェントがインストールされたデバイス上で、Windows Update 更新プログラムのインストールをユーザーが管理することを許可する**］の設定で、Windows Update を使用してデバイスに手動でインストールできる Windows 更新プログラムを制限できます。

  Windows 10 を実行しているデバイスで、デバイスに適用可能な更新プログラムが Windows Update 内で既に検出されている場合、［**Kaspersky Security Center 11 がインストールされた管理サーバーデバイスが WSUS サーバーとして使用されている場合に、バージョン 11 以降のネットワークエージェントがインストールされたデバイス上で、Windows Update 更新プログラムのインストールをユーザーが管理することを許可する**］は、検出された更新プログラムがインストールされた後に適用されます。

  ドロップダウンリストからオプションを選択します：

  - **Windows Update のすべての適用可能な更新プログラムのインストールをユーザーに許可する**

    ユーザーは、デバイスに適用可能な Microsoft Windows Update のすべての更新プログラムをインストールできます。

    アップデートのインストールをブロックしない場合は、このオプションを選択します。

    ユーザーが Microsoft Windows Update の更新プログラムを手動でインストールする時、更新プログラムを管理サーバーからではなく Microsoft サーバーからダウンロードする場合があります。これは、管理サーバーが対象の更新プログラムをまだダウンロードしていない場合に起こります。Microsoft サーバーから更新プログラムをダウンロードすると、トラフィック量が増加します。

  - **Windows Update の承認された更新プログラムのみのインストールをユーザーに許可する**

ユーザーは、デバイスに適用可能で管理者に承認された Microsoft Windows Update のすべての更新プログラムをインストールできます。

たとえば、最初にテスト環境にアップデートをインストールしてデバイスのオペレーティングシステムとの互換性の問題が生じないかを確認してから、クライアントデバイスへの承認されたアップデートのインストールを許可することができます。

ユーザーが Microsoft Windows Update の更新プログラムを手動でインストールする時、更新プログラムを管理サーバーからではなく Microsoft サーバーからダウンロードする場合があります。これは、管理サーバーが対象の更新プログラムをまだダウンロードしていない場合に起こります。Microsoft サーバーから更新プログラムをダウンロードすると、トラフィック量が増加します。

- **Windows Update 更新プログラムのインストールをユーザーに許可しない**

  ユーザーは、デバイスに Microsoft Windows Update の更新プログラムを手動でインストールできません。すべての適用可能な更新プログラムは、管理者の設定に従ってインストールされます。

  アップデートのインストールを一元的に管理する場合は、このオプションをオンにします。

  たとえば、ネットワークの過負荷を避けるために、アップデートのスケジュールを最適化したい場合などです。ユーザーの業務に支障をきたさないように、業務時間外にアップデートをスケジュールすることができます。

- ［**Windows Update 検索モード**］で、更新プログラムの検索モードを選択できます：

  - **アクティブ**

    このオプションをオンにすると、管理サーバーがネットワークエージェントのサポートにより、クライアントデバイス上の Windows Update エージェントからアップデート元である Windows Update Server または WSUS への要求を開始します。次に、ネットワークエージェントが、Windows Update エージェントから受け取った情報を管理サーバーに渡します。

    このオプションは、*脆弱性とアプリケーションのアップデートの検索*タスクで［**アップデートサーバーに接続してアップデートを取得**］が選択されている場合にのみ有効になります。

    既定では、このオプションがオンです。

  - **パッシブ**

    このオプションをオンにすると、ネットワークエージェントは、Windows Update エージェントとアップデート元との前回の同期で取得した更新プログラムの情報を定期的に管理サーバーに渡します。Windows Update エージェントとアップデート元が同期されない場合、管理サーバー上のアップデートの情報が最新ではなくなります。

    アップデート元のメモリキャッシュからアップデートを取得する場合は、このオプションを選択します。

  - **無効**

    このオプションをオンにすると、管理サーバーは更新プログラムに関する情報を要求しません。

    このオプションは、たとえば手元のローカルデバイスで最初にアップデートをテストしたい場合などに選択します。

- **実行ファイルの開始時に脆弱性をスキャンする**

  このオプションをオンにすると、実行ファイルが実行時にスキャンされ、脆弱性がないかチェックされます。

  既定では、このオプションはオフです。

再起動の設定

［**再起動の設定**］セクションでは、アプリケーションの正しい使用、インストール、またはアンインストールのために管理対象デバイスのオペレーティングシステムの再起動が必要な場合に行う動作を指定できます。
［**再起動の設定**］セクションの設定は、Windows を実行しているデバイスでのみ使用できます：

- **OS を再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **必要に応じて自動的に OS を再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

  - **通知の繰り返し間隔（分）**

    このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

    既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

    このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

  - **次の時間経過後に強制的に再起動する（分）**

    ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

    既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

Windows デスクトップ共有

［**Windows デスクトップ共有**］セクションでは、デスクトップアクセスの共有時にリモートデバイスで実行される管理者の処理の監査を有効にしたり、設定したりできます。［**Windows デスクトップ共有**］セクションの設定は、Windows を実行しているデバイスでのみ使用できます：

- **監査を有効にする**

  このオプションをオンにすると、リモートデバイスにおける管理者の処理の監査が有効になります。リモートデバイスにおける管理者の処理の記録は次に保存されます：

  - リモートデバイスのイベントログ
  - リモートデバイス上のネットワークエージェントのインストールフォルダーにある、拡張子が syslog のファイル
  - Kaspersky Security Center Cloud コンソールのイベントデータベース

  管理者の処理の監査が使用可能である条件は次の通りです：

  - 脆弱性とパッチ管理のライセンスが使用されている
  - 管理者がリモートデバイスのデスクトップに対する共有アクセスを開始する権限を持っている

  このオプションをオフにすると、リモートデバイスにおける管理者の処理の監査が無効になります。

  既定では、このオプションはオフです。

- **読み取り時に監視する必要のあるファイルのマスク**

  リストにはファイルマスクが含まれます。監査が有効になると、マスクと一致する管理者の読み取りファイルが監視され、ファイルの読み取りに関する情報が保存されます。リストは、［**監査を有効にする**］がオンの場合に使用できます。ファイルマスクを編集し、新しいマスクをリストに追加できます。新しいファイルマスクは、新しい行のリストに指定する必要があります。

  既定では、*.txt、*.rtf、*.doc、*.xls、*.docx、*.xlsx、*.odt、*.pdf のファイルマスクが指定されます。

- **変更時に監視する必要のあるファイルのマスク**

リストには、リモートデバイス上のファイルのマスクが含まれます。監査が有効になると、マスクと一致するファイルで管理者によって行われた変更が監視され、その変更に関する情報が保存されます。リストは、［**監査を有効にする**］がオンの場合に使用できます。ファイルマスクを編集し、新しいマスクをリストに追加できます。新しいファイルマスクは、新しい行のリストに指定する必要があります。

既定では、*.txt、*.rtf、*.doc、*.xls、*.docx、*.xlsx、*.odt、*.pdf のファイルマスクが指定されます。

パッチとアップデートの管理

［**パッチとアップデートの管理**］セクションでは、管理対象デバイスでのアップデートのダウンロードと配信や、パッチのインストールを設定できます。［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオンまたはオフにします。

接続

［**接続**］セクションには 3 つのサブセクションが含まれます：

- **ネットワーク**
- **接続プロファイル**
- **接続スケジュール**

［**ネットワーク**］サブセクションでは、管理サーバーからクライアントコンピューターへの接続を設定したり、UDP ポートの使用を有効化したり、UDP ポート番号を定義したりできます。

- ［**管理サーバーへの接続**］設定グループでは、次の設定を指定できます：
  - **ネットワークトラフィックを圧縮する**

    このオプションをオンにすると、送信される情報量が減ることでネットワークエージェントによるデータ送信速度が向上し、これにより管理サーバーの負荷が軽減されます。

    クライアントコンピューターの CPU の負荷は増加する可能性があります。

    既定では、このチェックボックスはオンです。

  - **Microsoft Windows ファイアウォールにネットワークエージェントのポートを開ける**

    このオプションをオンにすると、ネットワークエージェントの動作に必要な UDP ポートが Microsoft Windows ファイアウォールの除外リストに追加されます。

    既定では、このオプションはオンです。

  - **既定の接続設定でディストリビューションポイントの接続ゲートウェイを使用する（使用可能な場合）**

このオプションをオンにすると、ディストリビューションポイントの接続ゲートウェイが、管理グループのプロパティで指定された設定で使用されます。

既定では、このオプションはオンです。

- **UDP ポートを使用する**

  UDP ポートを経由して KSN プロキシサーバーと管理対象デバイスを接続する場合は、［**UDP ポートを使用**］をオンにして、［**UDP ポート**］でポート番号を指定します。既定では、このオプションはオンです。KSN プロキシサーバーに接続する既定の UDP ポートは 15111 です。

- **UDP ポート番号**

  このフィールドに、UDP ポート番号を入力できます。既定のポート番号は 15000 です。

  レコードには 10 進法が使用されます。

  Windows XP Service Pack 2 で稼働するクライアントデバイスでは、UDP ポート 15000 が OS のファイアウォールによりブロックされます。このポートを手動で開く必要があります。

- **ディストリビューションポイントを使用して管理サーバーへ強制的に接続する**

  ［**プッシュサーバーを実行**］をディストリビューションポイントの設定ウィンドウでオンにする場合、このオプションをオンにします。オンにしないと、ディストリビューションポイントはプッシュサーバーとして動作しません。

［**接続プロファイル**］設定グループでは、［**管理サーバー接続プロファイル**］に新しい項目は追加できないため、［**追加**］は無効になっています。設定済みの接続プロファイルも変更できません。

［**接続スケジュール**］サブセクションでは、ネットワークエージェントから管理サーバーにデータを送信する時間間隔を指定できます。

- **要求時に接続**
- **指定の時間間隔で接続**

［**接続スケジュール**］サブセクションでは、ネットワークエージェントから管理サーバーにデータを送信する時間間隔を指定できます。

- **要求時に接続**

  このオプションをオンにすると、ネットワークエージェントが管理サーバーへのデータ送信を要求された時に、接続が確立されます。

  既定では、このオプションがオンです。

- **指定の時間間隔で接続**

  このオプションをオンにすると、ネットワークエージェントは指定した時間に管理サーバーへ接続します。複数の接続時間帯を追加できます。

ディストリビューションポイント別のネットワークポーリング

［**ディストリビューションポイント別のネットワークポーリング**］セクションでは、ネットワークの自動ポーリングを設定できます。ポーリングの設定は、Windows を実行しているデバイスでのみ使用できます。次のオプションを使用してポーリングを有効にしたり、頻度を設定できます：

- **Windows ネットワーク**

  このオプションをオンにすると、［**簡易ポーリングのスケジュールを設定する**］と［**完全ポーリングのスケジュールを設定する**］をクリックして設定したスケジュールに従って、ディストリビューションポイントによってネットワークが自動的にポーリングされます。

  このオプションをオフにすると、管理サーバーはネットワークをポーリングしません。

  既定では、このオプションはオンです。

- **IP アドレス範囲**

  このオプションをオンにすると、［**ポーリングのスケジュールを設定する**］をクリックして設定したスケジュールに従って、ディストリビューションポイントによって IP アドレス範囲が自動的にポーリングされます。

  このオプションをオフにすると、ディストリビューションポイントは IP アドレス範囲をポーリングしません。

  既定では、このオプションはオフです。

- **ドメインコントローラー**

  このオプションをオンにすると、［**ポーリングのスケジュールを設定する**］をクリックして設定したスケジュールに従って、ディストリビューションポイントによって Active Directory が自動的にポーリングされます。

  このオプションをオフにすると、ディストリビューションポイントはドメインコントローラーをポーリングしません。

  10.2 より前のバージョンのネットワークエージェントドメインコントローラーのポーリング頻度は、［**ポーリング間隔（分）**］で設定できます。このフィールドは、このオプションをオンにすると使用可能になります。

  既定では、このオプションはオフです。

ディストリビューションポイントのネットワーク設定

［**ディストリビューションポイントのネットワーク設定**］セクションで、インターネットアクセス設定を指定できます：

- **プロキシサーバーを使用する**
- **アドレス**
- **ポート番号**
- **ローカルアドレスにプロキシサーバーを使用しない**

このオプションをオンにすると、ローカルネットワークのデバイスへの接続にプロキシサーバーが使用されません。

既定では、このオプションはオフです。

- **プロキシサーバー認証**

  このチェックボックスをオンにすると、入力フィールドでプロキシサーバーの資格情報を指定できます。

  既定では、このチェックボックスはオフです。

- **ユーザー名**
- **パスワード**

KSN プロキシ（ディストリビューションポイント）

［**KSN プロキシ（ディストリビューションポイント）**］セクションでは、ディストリビューションポイントを使用して管理対象デバイスからの KSN リクエストを転送するようにアプリケーションを設定できます：

- **ディストリビューションポイントで KSN プロキシを有効にする**

  ディストリビューションポイントとして使用しているデバイス上で KSN プロキシサービスが実行されます。この機能を使用することで、ネットワーク上でトラフィックを分配しなおし、最適化できます。

  この機能は、Linux または macOS を実行するディストリビューションポイントデバイスでサポートされていません。

  ディストリビューションポイントは、Kaspersky Security Network に関する声明に記載されている KSN の統計情報をカスペルスキーに送信します。既定では、KSN 声明は「%ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula」にあります。

  既定では、このオプションはオフです。管理サーバーのプロパティウィンドウで、［**Kaspersky Security Network への参加に同意する**］がオンになっている場合にのみ使用できます。

  アクティブ / パッシブモードのクラスターのノードをディストリビューションポイントに割り当て、ノード上で KSN プロキシサーバーを有効にできます。

- **ポート**

  管理対象デバイスが KSN プロキシサーバーへの接続に使用する TCP ポートの番号。既定のポート番号は 13111 です。

- **UDP ポート**

  UDP ポートを経由して KSN プロキシサーバーと管理対象デバイスを接続する場合は、［**UDP ポートを使用**］をオンにして、［**UDP ポート**］でポート番号を指定します。既定では、このオプションはオンです。KSN プロキシサーバーに接続する既定の UDP ポートは 15111 です。

ネットワークエージェントのポリシー設定のオペレーティングシステム別の比較

次の表は、特定のオペレーティングシステムでネットワークエージェントの設定に使用できるネットワークエージェントのポリシー設定を示しています。

ネットワークエージェントのポリシー設定：オペレーティングシステムによる比較

［ポリシー］セクション	Windows	macOS	Linux
全般	✓	✓	✓
イベントの設定	✓	✓	✓
設定	✓	✓ ［**アンインストール用パスワードを使用する**］チェックボックスを除く。	✓ ［**アンインストール用パスワードを使用する**］チェックボックスを除く。
リポジトリ	✓	–	✓ 次のオプションを使用できます： • インストール済みアプリケーションの詳細 • ハードウェアレジストリの詳細
ソフトウェアのアップデートと脆弱性	✓	–	–
再起動の設定	✓	–	–
Windows デスクトップ共有	✓	–	–
パッチとアップデートの管理	✓	–	–
［**接続**］→［**ネットワーク**］	✓	✓ ［**Microsoft Windows ファイアウォールにネットワークエージェントのポートを開ける**］以外。	✓ ［**Microsoft Windows ファイアウォールにネットワークエージェントのポートを開ける**］以外。
［**接続**］→［**接続スケジュール**］	✓	✓	✓
ディストリビューションポイント別のネットワークポーリング	✓ 次のオプションを使用できます： • **Windows ネットワーク** • **IP アドレス範囲**	–	✓ 次のオプションを使用できます： • **IP アドレス範囲** • ［**ドメインコントローラー**］（Microsoft Active Directory、Active

	• ［**ドメインコントローラー**］（Microsoft Active Directory）		Directory としての Samba）
ディストリビューションポイントのネットワーク設定	✓	✓	✓
KSN プロキシ（ディストリビューションポイント）	✓	–	✓

ネットワークエージェントのインストールパッケージ設定

ネットワークエージェントのインストールパッケージを設定するには：

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に選択します。
   - メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。

   管理サーバーで使用可能なインストールパッケージのリストが表示されます。

2. ネットワークエージェントのインストールパッケージの名前のリンクをクリックします。

   ネットワークエージェントのインストールパッケージのプロパティウィンドウが開きます。ウィンドウでは、タブとセクションに情報がグループ化されています。

全般

［**全般**］セクションには、インストールパッケージに関する全般的な情報が表示されます：

- インストールパッケージ名
- インストールパッケージでインストールされるアプリケーションの名前とバージョン
- インストールパッケージのサイズ
- インストールパッケージの作成日
- インストールパッケージのフォルダーのパス

設定

このセクションには、ネットワークエージェントをインストール後すぐに正常に機能させるのに必要な設定が示されます。このセクションの設定は、Windows を実行しているデバイスでのみ使用できます。

［**インストール先フォルダー**］設定グループでは、ネットワークエージェントがインストールされるクライアントデバイスのフォルダーを選択できます。

- **既定のフォルダーにインストールする**

  このオプションをオンにすると、ネットワークエージェントは、フォルダー <ドライブ名>:\Program Files\Kaspersky Lab\NetworkAgent にインストールされます。このフォルダーがない場合は、フォルダーが自動的に作成されます。

  既定では、このオプションがオンです。

- **指定したフォルダーにインストールする**

  このオプションをオンにすると、ネットワークエージェントは、入力フィールドで指定したフォルダーにインストールされます。

次の設定グループでは、ネットワークエージェントのリモートアンインストールタスク用のパスワードを設定できます：

- **アンインストール用パスワードを使用する**

  このオプションをオンにすると、［**変更**］をクリックしてアンインストール用パスワード（Windows オペレーティングシステム実行中のデバイスのネットワークエージェントのみに使用可能）を入力できます。

  既定では、このオプションはオフです。

- **ステータス**

- **ネットワークエージェントを不正な削除・停止から保護し、設定の変更を防止する**

  このオプションをオンにすると、管理対象デバイスにネットワークエージェントのインストールされた後、必要な権限がない場合はコンポーネントの削除や再設定が行えなくなります。また、ネットワークエージェントサービスを停止できなくなります。このオプションはドメインコントローラーに影響しません。

  ローカル管理者権限で操作されているワークステーション上のネットワークエージェントを保護するには、このオプションをオンにします。

  既定では、このオプションはオフです。

- **コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**

  このチェックボックスをオンにすると、ネットワークエージェント用にダウンロードされたすべてのアップデートとパッチが自動的にインストールされます。

  このチェックボックスをオフにすると、ダウンロードされたすべてのアップデートとパッチは、アップデートとパッチのステータスを［*承認*］に変更した後にインストールされます。［*未定義*］ステータスのアップデートとパッチはインストールされません。

  既定では、このチェックボックスはオンです。

接続

このセクションでは、ネットワークエージェントから管理サーバーへの接続を設定できます：

- **UDP ポートを使用する**

  UDP ポート番号

  このフィールドでは、UDP プロトコル経由で管理サーバーがネットワークエージェントに接続するポートを指定できます。

  既定の UDP ポート番号は 15000 です。

- **Microsoft Windows ファイアウォールにネットワークエージェントのポートを開ける**

  このオプションをオンにすると、ネットワークエージェントによって使用される UDP ポートが Microsoft Windows ファイアウォールの除外リストに追加されます。

  既定では、このオプションはオンです。

- **プロキシサーバーを使用しない**

- **プロキシサーバーを使用する**

  プロキシサーバーアドレス

  プロキシサーバーのポート

- **プロキシサーバー認証**

  このオプションをオンにすると、入力フィールドでプロキシサーバー認証の資格情報を指定できます。

  プロキシサーバー認証に必要な最小限の権限が付与されているアカウントの資格情報を指定することを推奨します。

  既定では、このオプションはオフです。

  ユーザー名

  プロキシサーバーへの接続の確立に使用されるアカウントのユーザー名。

  プロキシサーバー認証に必要な最小限の権限が付与されているアカウントの資格情報を指定することを推奨します。

  パスワード

  プロキシサーバーへの接続の確立に使用されるアカウントのパスワード。

  プロキシサーバー認証に必要な最小限の権限が付与されているアカウントの資格情報を指定することを推奨します。

詳細

［**詳細**］セクションでは、接続ゲートウェイの使用方法を設定できます：

- **接続ゲートウェイを使用して管理サーバーに接続する**

- **接続ゲートウェイアドレス**
- **VDI 向け動的モードを有効にする**

  このオプションをオンにすると、仮想マシンにインストールされたネットワークエージェントで仮想デスクトップインフラストラクチャ（VDI）向け動的モードが有効になります。

  既定では、このオプションはオフです。

- **VDI 向けに設定を最適化する**

  このオプションをオンにすると、ネットワークエージェントの設定で次の機能が無効にされます：
  - インストールされたソフトウェアに関する情報の取得
  - ハードウェアに関する情報の取得
  - 検知された脆弱性に関する情報の取得
  - 必要なアップデートに関する情報の取得

  既定では、このオプションはオフです。

追加コンポーネント

このセクションでは、ネットワークエージェントと同時にインストールする追加コンポーネントを選択できます。

タグ

［**タグ**］セクションには、ネットワークエージェントのインストール後にクライアントデバイスに追加できるキーワード（タグ）のリストが表示されます。リストへのタグの追加、リストからのタグの削除、タグの名前の変更を行うことができます。

タグの横のチェックボックスがオンの場合、そのタグは、ネットワークエージェントのインストール時に、管理対象デバイスに自動的に追加されます。

タグに隣接するチェックボックスをオフにすると、ネットワークエージェントのインストール時に、管理対象デバイスに自動的には追加されません。タグは手動でデバイスに追加できます。

リストからタグを削除すると、そのタグは、そのタグが追加されたすべてのデバイスから自動的に削除されます。

変更履歴

このセクションでは、インストールパッケージのリビジョンの履歴を確認できます。リビジョンの比較、リビジョンの表示、リビジョンのファイル保存、リビジョンの説明の追加と編集ができます。

次の表に、各オペレーティングシステムで利用できるネットワークエージェントのインストールパッケージ設定を示します。

ネットワークエージェントのインストールパッケージ設定

プロパティセ	Windows	Mac	Linux

クション			
全般	✓	✓	✓
設定	✓	–	–
接続	✓	✓ * ［**Microsoft Windows ファイアウォールにネットワークエージェントのポートを開ける**］を除く	✓ * ［**Microsoft Windows ファイアウォールにネットワークエージェントのポートを開ける**］を除く
詳細	✓	✓	✓
追加コンポーネント	✓	✓	✓
タグ	✓	✓ * ただし、自動タグルールを除く	✓ * ただし、自動タグルールを除く
変更履歴	✓	✓	✓

仮想インフラストラクチャ

Kaspersky Security Center Cloud コンソールでは仮想マシンの使用をサポートします。仮想インフラストラクチャを保護するには、各仮想マシンにネットワークエージェントをインストールする必要があります。

仮想マシンの負荷を軽減するヒント

Kaspersky Security Center Cloud コンソールの一部の機能は、仮想マシンに対してはそれほど有効性がないと考えられます。ネットワークエージェントを仮想マシンにインストールする場合は、それらの機能の無効化を検討することが推奨されます。

ネットワークエージェントを仮想マシンまたは仮想マシンの生成を目的とするテンプレートにインストールする場合、以下の操作を実行してください：

- リモートインストールを実行している場合、ネットワークエージェントのインストールパッケージのプロパティウィンドウの［**詳細**］セクションで、［**VDI 向けに設定を最適化する**］をオンにします。
- ウィザードを使用して対話型インストールを実行している場合、ウィザードウィンドウで［**ネットワークエージェントの設定を仮想インフラストラクチャ用に最適化します**］をオンにします。

これらのオプションを選択すると、ネットワークエージェントの設定が変更されるため、以下の機能は（ポリシーを適用する前に）既定で引き続き無効化されます：

- インストールされたソフトウェアに関する情報の取得
- ハードウェアに関する情報の取得
- 検知された脆弱性に関する情報の取得
- 必要なアップデートに関する情報の取得

これらの機能は同一のソフトウェアと仮想ハードウェアを使用しているため、通常は仮想マシンでは必須ではありません。

機能の無効化は取り消すことができます。無効にした機能が必要になった場合、ネットワークエージェントのポリシーを使用して、またはネットワークエージェントのローカル設定を使用して有効にすることができます。ネットワークエージェントのローカル設定は、管理コンソールで関連デバイスのコンテキストメニューからアクセスできます。

動的仮想マシンのサポート

Kaspersky Security Center Cloud コンソールは動的仮想マシンをサポートしています。仮想インフラストラクチャが組織ネットワークに導入されている場合、動的（一時）仮想マシンを特定の条件下で使用できます。動的仮想マシンは、管理者が準備したテンプレートに基づき、一意の名前で作成されます。ユーザーがしばらくの間仮想マシンで作業して、仮想マシンの電源をオフにすると、その仮想マシンは仮想インフラストラクチャから削除されます。ネットワークエージェントがインストールされた仮想マシンも、管理サーバーデータベースに追加されます。この仮想マシンの電源をオフにした後は、対応するエントリも管理サーバーのデータベースから削除する必要があります。

仮想マシンのエントリの自動削除機能を活用するには、動的仮想マシンのテンプレートにネットワークエージェントをインストールする際に、次の場所で［**VDI 向け動的モードを有効にする**］をオンにします：

- リモートインストールの場合 – ネットワークエージェントのインストールパッケージのプロパティウィンドウで（［**詳細**］セクション）
- 対話型インストールの場合 – ネットワークエージェントのインストールウィザードで

ネットワークエージェントを物理デバイスにインストールする場合は、［**VDI 向け動的モードを有効にする**］をオンにしないでください。

動的仮想マシンのイベントを、それらの仮想マシンを削除した後もしばらくの間管理サーバーに保存したい場合、管理サーバーのプロパティウィンドウの［**イベントリポジトリ**］セクションで、［**デバイスの削除後にイベントを保管する**］をオンにし、イベントの最大保管時間（日数）を指定します。

仮想マシンのコピーのサポート

Kaspersky Security Center Cloud コンソールは、ネットワークエージェントがインストールされた仮想マシンのコピー、またはネットワークエージェントがインストールされたテンプレートからの仮想マシンの作成をサポートしています。

ネットワークエージェントは、次の場合に仮想マシンのコピーを自動的に検出できます：

- ネットワークエージェントのインストール時に［**VDI 向け動的モードを有効にする**］をオンにした場合：オペレーティングシステムを再起動するたびに、この仮想マシンは、コピーされたかどうかに依存せず、新しいデバイスとして認識されます。
- VMware™、HyperV®、Xen® のいずれかのハイパーバイザーが使用されている場合：ネットワークエージェントでは、変更された仮想ハードウェアの ID によって、仮想マシンのコピーが検出されます。

仮想ハードウェアにおける変更の分析機能は、完全に信頼できるわけではありません。この方法を広く採用する前に、組織が現在使用しているハイパーバイザーのバージョンを用いて、小規模な仮想マシンのプールでテストする必要があります。

Windows 用、macOS 用、Linux 用ネットワークエージェントの用途：比較

Windows 用ネットワークエージェントと比較して、macOS および Linux 用ネットワークエージェントにはいくつかの機能制限があります。ネットワークエージェントのポリシーの設定とインストールパッケージの設定も、オペレーティングシステムによって異なります。次の表は、Windows、macOS、および Linux オペレーティングシステムで使用可能なネットワークエージェントの機能と使用シナリオを比較したものです。

ネットワークエージェントの機能の比較

ネットワークエージェントの機能	Windows	Linux	macOS
インストール			
ネットワークエージェントのアップデートとパッチの自動インストール	✓	–	–
ライセンスの自動配信	✓	✓	✓
デバイスでアプリケーションインストーラーを実行しての手動インストール	✓	✓	✓
強制同期	✓	✓	✓
ディストリビューションポイント			
ネットワークポーリング	✓ • IP アドレス範囲のポーリング • Windows ネットワークのポーリング • ドメインコントローラーのポーリング（Microsoft Active Directory）	✓ • IP アドレス範囲のポーリング • ドメインコントローラーのポーリング（Microsoft Active Directory、Active Directory としての Samba）	–
ディストリビューション	✓	–	–

ポイントでの KSN プロキシサービスの実行			
管理対象デバイスにアップデートを配布するディストリビューションポイントリポジトリに、カスペルスキーのアップデートサーバー経由でアップデートをダウンロードする	✓	✓	– macOS を実行しているディストリビューションポイントデバイスでは、カスペルスキーのアップデートサーバーからアップデートをダウンロードできません。 *ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクの対象範囲に macOS を実行しているデバイスが1台以上含まれている場合、すべての Windows デバイスでタスクが正常に完了した場合でも、タスクには「*失敗*」ステータスが付与されます。
アプリケーションのプッシュインストール	✓	制限あり：Linux ディストリビューションポイントを使用して Windows デバイスにプッシュ インストールを実行することはできません。	
サードパーティ製品の取り扱い			
デバイスへのアプリケーションのリモートインストール	✓	–	–
ソフトウェアのアップデート	✓	–	–
ネットワークエージェントポリシーでのオペレーティングシステムのアップデートの設定	✓	–	–
ソフトウェアの脆弱性に関する情報の表示	✓	–	–
アプリケーションの脆弱性スキャン	✓	–	–
デバイスにインストールされたソフトウェアのインベントリ	✓	–	–
仮想マシン			
仮想マシンへのネットワークエージェントのインストール	✓	✓	✓
仮想デスクトップインフ	✓	✓	✓

ラストラクチャ（VDI）に合わせた設定の最適化			
動的仮想マシンのサポート	✓	✓	✓
その他			
リモートクライアントデバイスでの Windows デスクトップ共有を使用した操作の監査	✓	–	–
デバイスの再起動の管理	✓	–	–
接続マネージャー	✓	✓	✓
クライアントデバイスのデスクトップへのリモート接続	✓	–	–

ディストリビューションポイントのプロパティには次のセクションが表示されますが、macOS 用ネットワークエージェントでは該当する機能がサポートされません：

- アップデート元
- KSN プロキシサーバー
- Windows ドメイン
- Active Directory
- IP アドレス範囲
- 詳細
- 統計

Unix デバイスのリモートインストールを設定する

リモートインストールタスクを使用して Unix デバイスにアプリケーションをインストールする際、タスクに Unix 固有の設定を指定することができます。これらの設定はタスクが作成された後にタスクのプロパティで利用できるようになります。

Unix 固有の設定をリモートインストールタスクで指定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. Unix 固有の設定を指定するリモートインストールタスクの名前をクリックします。
   タスクのプロパティウィンドウが開きます。
3. ［**アプリケーション設定**］→［**Unix 固有の設定**］の順に移動します。
4. 次の設定を指定します：

- **root アカウントのパスワードを設定する（SSH での導入時のみ）**

  パスワードを指定しないと対象のデバイスで sudo コマンドが使用できない場合、このオプションを選択してルートアカウントのパスワードを指定します。Kaspersky Security Center Cloud コンソールは対象デバイスにパスワードを暗号化して転送し、復号化してからこのパスワードを使用してルートアカウントに代わってインストール手順を開始します。

  Kaspersky Security Center Cloud コンソールは SSH 接続を作成するためにユーザーアカウントや指定したパスワードを使用しません。

- **ターゲットデバイスへの実行権限がある一時ディレクトリへのパスを指定する（SSH での導入時のみ）**

  対象デバイスの /tmp ディレクトリに実行権限がない場合、このオプションを選択してから実行権限のあるディレクトリへのパスを指定します。Kaspersky Security Center Cloud コンソールは SSH 経由でアクセスする一時ディレクトリとして指定されたディレクトリを使用します。アプリケーションはインストールパッケージをそのディレクトリに配置し、インストールプロセスを実行します。

5. ［**保存**］をクリックします。

指定したタスク設定が保存されます。

サードパーティのセキュリティ製品からの移行とアンインストールの実施

カスペルスキーのセキュリティ製品を Kaspersky Security Center Cloud コンソールを使用してインストールする場合、インストールするアプリケーションと競合するサードパーティ製ソフトウェアを削除しなければならない場合があります。Kaspersky Security Center Cloud コンソールでは、サードパーティ製品を削除する複数の方法が用意されています。

競合するアプリケーションの削除をアプリケーションのリモートインストールの設定時に指定

セキュリティ製品のリモートインストールの設定時に［**競合アプリケーションを自動的にアンインストールする**］をオンにできます。このオプションは製品導入ウィザードで使用できます。このオプションをオンにすると、Kaspersky Security Center Cloud コンソールは、管理対象デバイスにセキュリティ製品をインストールする前に競合アプリケーションを削除します。

専用タスクを使用した競合アプリケーションの削除

タスクを使用して競合アプリケーションを削除するには、**アプリケーションのリモートアンインストール**タスクを使用します。このタスクは、セキュリティ製品のインストールタスクの前にデバイスで実行する必要があります。たとえば、インストールタスクのスケジュール種別として［**他のタスクが完了次第**］を選択し、条件の対象となるタスクとして［**アプリケーションのリモートアンインストール**］を指定できます。

このアンインストール方法は、セキュリティ製品のインストーラーでは競合アプリケーションを適切に削除できない場合に有用です。

アプリケーションの手動インストールのオプション

Kaspersky Security Center Cloud コンソールを使用せずに、デバイスにネットワークエージェントをローカルにインストールできます。これを行うには、トピック「スタンドアロンインストールパッケージの作成」の説明に従って、ネットワークエージェントのスタンドアロンインストールパッケージを作成します。パッケージをクライアントデバイスに転送してインストールします。ネットワークエージェントのインストールが完了すると、デバイスをディストリビューションポイントとして使用できます。

製品導入ウィザード

カスペルスキー製品をインストールするには、製品導入ウィザードを使用できます。製品導入ウィザードにより、専用に作成されたインストールパッケージを使用するか、または配布パッケージから直接、アプリケーションをリモートインストールすることができます。

製品導入ウィザードにより、次の操作が実行できます：

- アプリケーションをインストールするためのインストールパッケージをダウンロードします（まだ作成されていない場合）。［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動すると、インストールパッケージにアクセスできます。今後アプリケーションをインストールする時に、このインストールパッケージを使用できます。
- 特定のデバイスまたは管理グループに対するリモートインストールタスクを作成して実行します。新しく作成されたリモートインストールタスクは、［**タスク**］セクションに保存されます。このタスクは後から手動で開始できます。タスクの種別は［**アプリケーションのリモートインストール**］になります。

製品導入ウィザードの開始

製品導入ウィザードを手動で起動するには：

メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**製品導入ウィザード**］の順に移動します。

製品導入ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

ステップ1：インストールパッケージの選択

インストールする製品のインストールパッケージを選択します。

目的の製品のインストールパッケージがリストに含まれていない場合、［**追加**］をクリックしてリストから製品を選択します。

ステップ2：ネットワークエージェントのバージョンの選択

ネットワークエージェント以外の製品のインストールパッケージを選択した場合でも、各製品と Kaspersky Security Center 管理サーバーとを接続するために、ネットワークエージェントのインストールが必要になります。

最新バージョンのネットワークエージェントを選択してください。

ステップ 3：デバイスの選択

アプリケーションをインストールするデバイスを指定します。

- **管理対象デバイスにインストール**

  このオプションをオンにすると、デバイスのグループに対してリモートインストールタスクが作成されます。

- **インストールするデバイスの選択**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

ステップ 4：リモートインストールタスクの設定

［**リモートインストールタスク設定**］ウィンドウで、製品のリモートインストール設定を指定します。

［**インストールパッケージの強制ダウンロード**］セクションで、製品のインストールに必要なファイルをクライアントデバイスに配布する方法を指定します。

- **ネットワークエージェントを使用する**

  このオプションをオンにすると、インストールパッケージのクライアントデバイスへの配布は、クライアントデバイスにインストールされたネットワークエージェントによって行われます。

  このオプションをオフにすると、インストールパッケージはクライアントデバイスのオペレーティングシステムのツールを使用して配信されます。

  ネットワークエージェントがインストールされたデバイスにタスクが割り当てられている場合は、このチェックボックスをオンにすることを推奨します。

  既定では、このオプションはオンです。

- **ディストリビューションポイントを通じてオペレーティングシステムの共有フォルダーを使用する**

このオプションをオンにすると、ディストリビューションポイントがオペレーティングシステムのツールを使用してインストールパッケージをクライアントデバイスに送信します。この機能が使用できるのは、ネットワークに少なくとも1つのディストリビューションポイントがある場合です。

［**ネットワークエージェントを使用する**］をオンにすると、ネットワークエージェントのツールが使用できない場合に限り、ファイルがオペレーティングシステムのツールで配布されます。

既定では、仮想管理サーバーで作成されたリモートインストールタスクに対して、このオプションはオンです。

詳細設定を行います：

アプリケーションが既にインストールされている場合再インストールしない

このオプションをオンにすると、選択したアプリケーションがクライアントデバイスに既にインストールされていた場合、インストールされません。

このオプションをオフにすると、アプリケーションは常にインストールされます。

既定では、このオプションはオンです。

ステップ5：再起動の設定

アプリケーションの使用中、インストール中、アンインストール中にオペレーティングシステムの再起動が必要になった場合に行う動作を指定します。

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

  - **通知の繰り返し間隔（分）**

このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

既定では、このオプションはオンです。既定の間隔は 5 分です。1分から 1,440 分までの値を指定できます。

このオプションをオフにすると、確認メッセージは1回だけ表示されます。

- **再起動するまでの時間（分）**

  ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

  既定では、このオプションはオンです。既定の間隔は 30 分です。1分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

ステップ 6：インストール前に競合アプリケーションを削除する

この手順の実施ウィンドウは、インストール対象の製品に既知の競合アプリケーションが存在する場合にのみ表示されます。

インストール対象の製品と互換性がないアプリケーションを自動的に削除するには、オプションをオンにします。

互換性がない競合アプリケーションのリストも表示されます。

このオプションをオフにした場合、インストール対象の製品は、競合アプリケーションがインストールされていないデバイスにのみインストールされます。

ステップ 7：管理対象デバイスへのデバイスの移動

ネットワークエージェントのインストール後に、デバイスを管理グループに移動するかどうかを指定します。

- **デバイスを移動しない**

デバイスは、現在配置されているグループから移動しません。どのグループにも割り当てられていないデバイスは、未割り当てのままとなります。

- **未割り当てデバイスをグループへ移動**

  指定した管理グループにデバイスが移動されます。

既定では［**デバイスを移動しない**］がオンになっています。セキュリティ上の理由のため、場合によってはデバイスを手動で移動する必要があります。

ステップ 8：デバイスにアクセスするアカウントの選択

必要に応じて、リモートインストールタスクの開始に使用するアカウントを追加できます：

- **アカウントが不要（ネットワークエージェントインストール済み）**

  このオプションをオンにすると、アプリケーションのインストーラーを実行するアカウントを指定する必要はありません。タスクは管理サーバーのサービスを実行しているアカウントで実行されます。

  クライアントデバイスにネットワークエージェントがインストールされていない場合、このオプションは使用できません。

- **アカウントが必要（ネットワークエージェントの使用なし）**

  リモートインストールタスクを割り当てるデバイスにネットワークエージェントがインストールされていない場合は、このオプションをオンにします。この場合、ユーザーアカウントを指定して、アプリケーションをインストールできます。

  アプリケーションインストーラーを実行するユーザーアカウントを指定するには、［**追加**］をクリックし、［**ローカルアカウント**］を選択して、ユーザーアカウントの資格情報を指定します。

  タスクを割り当てるすべてのデバイスで必要なすべての権限をどのアカウントも持たない場合などのために、複数のユーザーアカウントを追加できます。この場合、追加されたすべてのアカウントが上から下へ順番に使用され、タスクが実行されます。

ステップ 9：インストールの開始

このウィンドウがこのウィザードでの最後のステップです。このステップを完了すると、**リモートインストールタスク**の作成と設定が完了します。

既定では、［**ウィザードの終了後にタスクを実行**］はオフになっています。このオプションをオンにすると、ウィザードの完了後すぐに**リモートインストールタスク**が開始されます。このオプションをオフにすると、**リモートインストールタスク**は開始されません。このタスクは後から手動で開始できます。

製品導入ウィザードを完了するには、［**OK**］をクリックします。

外部サービスとの相互対話のためのネットワーク設定

Kaspersky Security Center Cloud コンソールは、外部サービスと対話するために次のネットワーク設定を使用します。

ネットワーク設定

ネットワーク設定	アドレス	説明
ポート：443 プロトコル：HTTPS	activation-v2.kaspersky.com/activationservice/activationservice.svc	アプリケーションのアクティベーション。
ポート：443 プロトコル：HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデート。
ポート：443 プロトコル：HTTPS	https://www.kaspersky.co.jp/downloads	• 定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデート。 • カスペルスキーサーバーにアクセスできるかどうかを確認しています。

		Kaspersky Security Center Cloud コンソールは、定義データベースとソフトウェアをダウンロードする前にカスペルスキーのサーバーがアクセス可能かどうかをチェックします。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。
ポート：80 プロトコル：HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデート
ポート：443	ds.kaspersky.com	Kaspersky Security Network の使用。

プロトコル：HTTPS		
ポート：443、1443 プロトコル：HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Kaspersky Security Network の使用。
プロトコル：HTTPS	click.kaspersky.com redirect.kaspersky.com	インターフェイスからリンクをたどります。
ポート：80 プロトコル：HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	公開鍵基盤（PKI）。
ポート：443 プロトコル：HTTPS	https://ipm-klca.kaspersky.com	マーケティング関連告知。

ネットワークエージェントをインストールするために、閉鎖ソフトウェア環境モードで Astra Linux を実行しているデバイスを準備します

閉鎖ソフトウェア環境モードで Astra Linux を実行しているデバイスにネットワークエージェントをインストールする前に、2 つの準備手順を実行する必要があります。1 つは以下の手順にある手順、もう 1 つは Linux デバイスの一般的な準備手順です。

事前準備：

- Linux 用ネットワークエージェントをインストールするデバイスで、サポート対象の Linux ディストリビューションを使用していることを確認します。
- 必要なネットワークエージェントインストールファイルをカスペルスキーの Web サイトからダウンロードします。

ルート権限を持つアカウントを使用してこの手順にあるコマンドを実行します。

ネットワークエージェントをインストールするために、閉鎖ソフトウェア環境モードで Astra Linux を実行しているデバイスを準備するには：

1. /etc/digsig/digsig_initramfs.conf ファイルを開き、次の設定を指定します：

   ```
   DIGSIG_ELF_MODE=1
   ```

2. コマンドラインで次のコマンドを実行して、適合パッケージをインストールします：

   ```
   apt install astra-digsig-oldkeys
   ```

3. 製品のライセンスにディレクトリを作成します：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. 前の手順で作成したディレクトリに製品のライセンス /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg を配置します：

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   > Kaspersky Security Center Cloud コンソール配布キットに kaspersky_astra_pub_key.gpg ライセンスが含まれていない場合は、以下のリンクをクリックしてダウンロードできます：https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg。

5. RAM ディスクをアップデートします：

   ```
   update-initramfs -u -k all
   ```

   システムを再起動します。

6. すべての Linux デバイスに共通の準備手順を実行します。

デバイスが準備されました。これで、ネットワークエージェントのインストールに進むことができます。

Linux デバイスの準備と Linux デバイスへのネットワークエージェントのリモートインストール

ネットワークエージェントのインストールは、次の 2 つの手順で実行されます：

- Linux デバイスの準備
- ネットワークエージェントのリモートインストール

Linux デバイスの準備

Linux で動作するデバイスにネットワークエージェントをリモートインストールのために準備するには：

1. 対象となる Linux デバイスに次のソフトウェアがインストールされていることを確認します：
   - Sudo
   - Perl 言語インタープリターのバージョン 5.10 以降
2. デバイスの構成をテストします：
   a. デバイスに SSH クライアント（PuTTY など）で接続できることを確認します。
   デバイスに接続できない場合、/etc/ssh/sshd_config ファイルを開き、次の設定をそれぞれの値に変更します：

   ```
   PasswordAuthentication no
   ChallengeResponseAuthentication yes
   ```

デバイスに問題なく接続できる場合は、/etc/ssh/sshd_config ファイルを変更しないでください。そうしないと、リモートインストールタスクの実行時に SSH 認証エラーが発生する可能性があります。

必要に応じてファイルを保存し、`sudo service ssh restart` コマンドを使用して SSH サービスを再起動します。

b. デバイスへの接続に使用するユーザーアカウントで sudo パスワードを無効にします。

c. sudo で `visudo` コマンドを使用し、sudoers 構成ファイルを開きます。

開いたファイルで、`%sudo`（CentOS オペレーティングシステムを使用している場合は、`%wheel`）で開始される行を探します。該当の行で、次を指定します：`<username> ALL = (ALL) NOPASSWD: ALL` この場合、`<username>` は、SSH を経由してデバイスを接続するために使用するユーザーアカウントです。Astra Linux オペレーティングシステムを使用している場合は、ファイル /etc/sudoers の最後の行に次のテキストを追加します：`%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

d. sudoers ファイルを保存して閉じます。

e. SSH を使用して再度デバイスに接続し、sudo サービスがパスワードの入力を要求しないことを確認します。そのためには `sudo whoami` コマンドを使用できます。

3. /Etc/systemd/logind.conf ファイルを開き、次のいずれかを実行します：

- KillUserProcesses 設定の値として「no」を指定します：`KillUserProcesses=no`
- KillExcludeUsers の設定にリモートインストールを実行するアカウントのユーザー名を入力します。例：`KillExcludeUsers=root`

対象デバイスが Astra Linux を実行している場合は、`export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` 文字列をファイル `/home/<ユーザー名>/.bashrc` に追加します。`<ユーザー名>`は、SSH を使用したデバイス接続に使用されるユーザーアカウントです。

変更した設定を適用するには、Linux デバイスを再起動するか、次のコマンドを実行してください：

```
$ sudo systemctl restart systemd-logind.service
```

4. SUSE Linux Enterprise Server 15 オペレーティングシステムを搭載したデバイスにネットワークエージェントをインストールする場合は、ネットワークエージェントの設定前に、insserv-compat パッケージをインストールします。

5. Astra Linux オペレーティングシステムが閉鎖ソフトウェア環境モードで実行されているデバイスにネットワークエージェントをインストールする場合は、追加の手順を実行して Astra Linux デバイスを準備します。

ネットワークエージェントのリモートインストール

Linux デバイスにネットワークエージェントをリモートインストールするには、次の手順に従います：

1. インストールパッケージをダウンロードして作成します：

a. パッケージのインストール前に、このパッケージが依存するプログラムやライブラリのすべてがデバイスにインストールされていることを確認してください。

パッケージの依存関係は、パッケージのインストール先の Linux ディストリビューションに含まれるユーティリティで確認できます。それらのユーティリティについて詳しくは、オペレーティングシステムのマニュアルを参照してください。

b. アプリケーションインターフェイスを使用するか、カスペルスキー Web サイトからネットワークエージェントインストールパッケージをダウンロードします。

c. リモートインストールパッケージを作成するには、次のファイルを使用します：

- klnagent.kpd
- akinstall.sh
- ネットワークエージェントの DEB または RPM パッケージ

2. 次の設定でリモートインストールタスクを作成します：

- 新規タスクウィザードの［**設定**］ページで、［**管理サーバーを通じてオペレーティングシステムの共有フォルダーを使用する**］をオンにします。それ以外のチェックボックスはすべてオフにします。
- ［**タスクを実行するアカウントの選択**］ページで、SSH でデバイスに接続するために使用するユーザーアカウントの設定を指定します。

3. リモートインストールタスクを実行します。`su` コマンドのオプションを使用して、環境を保持します: `-m, -p, --preserve-environment`。

バージョン 20 より前の Fedora で動作しているデバイスにネットワークエージェントを SSH でインストールすると、エラーになることがあります。その場合、ネットワークエージェントをインストールするには、/etc/sudoers で Defaults requiretty オプションをコメントアウト（つまりコメント構文で囲むように）します。SSH での接続中に、Defaults requiretty オプションが問題になる条件の詳細は、Bugzilla バグトラッキング Web サイトを参照してください。

モバイルデバイス管理

Kaspersky Security Center Cloud コンソールからのモバイルデバイス保護の管理は、モバイルデバイス管理機能を使用して行われます。自社の従業員が使用しているモバイルデバイスを管理する場合は、モバイルデバイス管理を有効にして設定してください。

モバイルデバイス管理を使用して、従業員の Android デバイスを管理できます。デバイスにインストールされた Kaspersky Security for Mobile を使用して保護します。このモバイルアプリケーションにより、モバイルデバイスを Web の脅威、ウイルス、その他の脅威をもたらすプログラムから保護します。

モバイルデバイスへの保護の導入および管理の詳細については、Kaspersky Security for Mobile のヘルプを参照してください。

Detection and Response の機能

このセクションには、Kaspersky Security Center Cloud コンソールと連携して、コンソールに検知とレスポンスの機能を追加できるカスペルスキー製品に関する情報が含まれています。

検知とレスポンスの機能について

Kaspersky Security Center Cloud コンソールのインターフェイスでは、他のカスペルスキー製品の機能を統合できます。たとえば、Kaspersky Security Center Cloud コンソールの機能に検知とレスポンスの機能を追加できます：

検知とレスポンスのソリューションは、組織の IT インフラストラクチャを複雑なサイバー脅威から保護するように設計されています。脅威の自動検知と、検知された脅威への対応を組み合わせたこのソリューションの機能により、新しい脆弱性攻撃、ランサムウェア、ファイルレス攻撃、正規のシステムツールを使用する手法などの複雑な攻撃に対抗することができます。

次のソリューションと連携できます。

- Kaspersky Endpoint Detection and Response Optimum

  Kaspersky Endpoint Protection Platform（EPP とも表記）が脅威を検出すると、Kaspersky Security Center Cloud コンソールはアラートリストに新しいアラートを追加します。アラートには、検知した脅威に関する詳細情報が含まれており、脅威を分析および調査できます。また、脅威の活動連鎖の図表の作成により脅威を可視化できます。グラフでは、検知された脅威の導入の段階について、時系列で説明します。

  応答として、事前定義されたレスポンス処理の 1 つを選択できます。たとえば、信頼されていないオブジェクトの隔離、侵害されたデバイスのネットワークからの隔離、信頼されていないオブジェクトに対する実行ブロックルールの作成などです。

  製品のアクティベーションに関する情報については、Kaspersky Endpoint Detection and Response Optimum のヘルプを参照してください。

- Kaspersky Managed Detection and Response

  Kaspersky EPP 製品が脅威を検出すると、Kaspersky Security Center Cloud コンソールは新しいインシデントをインシデントリストに追加します。インシデントには、検知した脅威に関する詳細情報が含まれています。MDR Security Operation Center（SOC）アナリスト、またはサードパーティ企業がインシデントを調査し、インシデントを解決するためのレスポンスを提案します。ユーザーは提案されたレスポンスを手動で許可または拒否できます。すべてのレスポンスを自動許可するオプションをオンにすることもできます。

  製品のアクティベーションに関する情報については、Kaspersky Managed Detection and Response のヘルプを参照してください。

- Kaspersky Endpoint Detection and Response Expert

  このソリューションは、SOC アナリストのチームがある組織向けです。検知した脅威は、調査のために SOC アナリストに割り当て可能なアラートまたはインシデントとして登録されます。Kaspersky Endpoint Detection and Response Expert を使用すると、各アラートや各インシデントに関する詳細な情報の参照や、アラート、インシデントの管理ツール、脅威のルール、カスタムルールの作成が可能となります。SOC アナリストまたはセキュリティ担当者は、レスポンスの動作を手動で選択できます。また、事前定義された自動的なレスポンス方法を採用することも可能です。

  製品のアクティベーションに関する情報は、Kaspersky Endpoint Detection and Response Expert のヘルプを参照してください。

検知とレスポンスの機能の連携後のインターフェイスの変更

次のカスペルスキー製品は、Kaspersky Security Center Cloud コンソールのインターフェイスと連携できる検知とレスポンスの機能を提供します。

- Kaspersky Endpoint Detection and Response (EDR) Optimum
- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response (EDR) Expert

次の表では、連携後に製品が Kaspersky Security Center Cloud コンソールのインターフェイスに加える変更を示します。

連携しているカスペルスキー製品によって行われたインターフェイスの変更

解決	Kaspersky Security Center Cloud コンソールでの変更
Kaspersky EDR Optimum	次の項目を追加します： • ［**アラート**］セクション（［**監視とレポート**］→［**アラート**］）この製品によって検出されたアラートは、［**最適**］タブに一覧表示されます • ［**ダッシュボード**］のウィジェット（［**監視とレポート**］→［**ダッシュボード**］）
Kaspersky MDR	次の項目を追加します： • ［**MDR**］セクション（［**監視とレポート**］→［**MDR**］） • ［**MDR 機能を表示**］オプション（［**設定**］→［**インターフェイスのオプション**］→［**MDR 機能を表示**］） • ［**ダッシュボード**］のウィジェット（［**監視とレポート**］→［**ダッシュボード**］）
Kaspersky EDR Expert	次の項目を追加します： • ［**アラート**］セクション（［**監視とレポート**］→［**アラート**］）この製品によって検出されたアラートは、［**Expert**］タブに一覧表示されます • ［**インシデント**］セクション（［**監視とレポート**］→［**インシデント**］） • ［**脅威のルール**］セクション（［**監視とレポート**］→［**脅威のルール**］） • ［**カスタムルール**］セクション（［**監視とレポート**］→［**カスタムルール**］） • Kaspersky EDR Expert の全般設定（［**設定**］→［**連携**］→［**Kaspersky EDR Expert**］） • ［**ダッシュボード**］のウィジェット（［**監視とレポート**］→［**ダッシュボード**］）

ネットワーク接続されたデバイスの検出と管理グループの作成

このセクションでは、ネットワーク接続されたデバイスの検索と検出、これらのデバイスの管理グループの作成について説明します。

Kaspersky Security Center Cloud コンソールでは、条件を指定してデバイスを検索できます。検索結果をテキストファイルに保存できます。

検索と検出の検出機能により、次のデバイスを見つけることができます：

- Kaspersky Security Center Cloud コンソール管理サーバーとそのセカンダリ管理サーバーの管理グループに属する管理対象デバイス
- Kaspersky Security Center Cloud コンソール管理サーバーとそのセカンダリ管理サーバーで管理される未割り当てデバイス

ネットワーク接続されたデバイスの検出シナリオ

セキュリティ製品の初期導入の前に、デバイスの検索を実行する必要があります。ネットワーク接続されたデバイスがすべて検出されると、これらのデバイスに関する情報を取得し、ポリシーを通してデバイスを管理できます。ネットワーク内に新しいデバイスが存在するか、また過去に検出されたデバイスが現在もネットワーク内に存在するかを確認するには、定期的なネットワークポーリングが必要です。

シナリオを完了すると、デバイスの検索が設定され、指定したスケジュールに従って実行されます。

必須条件

Kaspersky Security Center Cloud コンソールでは、ディストリビューションポイントを使用してデバイスの検索が実行されます。開始する前に、次を実行します：

- ディストリビューションポイントとして動作するデバイスを決定します。
- 選択したデバイスにネットワークエージェントをインストールします。
- ディストリビューションポイントとして動作するデバイスを手動で割り当てます。

実行するステップ

このシナリオは段階的に進行します：

1. **検出の種別の選択**

   どの種別の検出を定期的に使用するかを決定します。

2. **ポーリングの設定**

   各ディストリビューションポイントのプロパティで、選択したネットワークポーリングを有効にして種別（Windows ネットワークのポーリング、ドメインコントローラーのポーリング、または IP アドレス範囲のポーリング）を設定します。ポーリングのスケジュールが組織のニーズに合致していることを確認します。

   ネットワークに接続されたデバイスがドメインに含まれている場合は、ドメインコントローラーのポーリングを使用することを推奨します。

3. **検出されたデバイスを管理グループに追加するルールの設定（任意）**

   ネットワーク内に新しいデバイスが追加された場合、これらのデバイスは定期的なポーリング中に検出され、［**未割り当てデバイス**］グループに自動的に含まれます。必要に応じて、［**管理対象デバイス**］グループに自動的にこれらのデバイスを移動するルールを設定できます。また、保持ルールを確立することもできます。

   このルール設定のステップを省略した場合、新しく検出されたデバイスはすべて［**未割り当てデバイス**］グループに割り当てられ、そこから移動されません。必要に応じて、これらのデバイスを［**管理対象デバイス**］グループに手動で移動できます。デバイスを［**管理対象デバイス**］グループに手動で移動する場合、各デバイスの情報を分析し、管理グループに移動するかどうかや、どの管理グループに移動するかを決定できます。

ネットワークポーリング操作が完了したら、新しく検出されたデバイスが、設定したルールに従って配置されていることを確認します。ルールを設定していない場合、デバイスは［**未割り当てデバイス**］グループに配置されたままになります。

ネットワークポーリング

Kaspersky Security Center Cloud コンソールは、Windows ネットワークの定期的なポーリング、IP アドレス範囲、Microsoft Active Directory ドメインコントローラーと Samba ドメインコントローラーによって、ネットワークの構造や、このネットワーク上のデバイスに関する情報を取得します。Samba ドメインコントローラーの場合、Samba 4 が Active Directory ドメインコントローラーとして使用されます。ネットワークポーリングは、スケジュールに応じて手動または自動で開始できます。

このポーリングの結果に基づき、Kaspersky Security Center Cloud コンソールは未割り当てデバイスのリストをアップデートします。新しく検出されたデバイスを自動的に管理グループに移動するためのルールを設定することもできます。

Kaspersky Security Center Cloud コンソールでは、次のネットワークポーリングの方法を使用します：

- *IP アドレス範囲のポーリング*。Kaspersky Security Center Cloud コンソールは、ICMP（Internet Control Message Protocol）パケットを使用して、指定された IP アドレス範囲をポーリングし、その IP アドレス範囲内にあるデバイスの完全なデータを作成します。

- *Windows ネットワークのポーリング*。2 つの Windows ネットワークのポーリング（簡易または完全）のいずれかを実行できます。簡易ポーリングでは Kaspersky Security Center Cloud コンソールが、すべてのネットワークドメインとワークグループ内のデバイスの NetBIOS 名リストの情報のみ取得します。完全ポーリングでは、各デバイスに対して、オペレーティングシステム（OS）の名前、IP アドレス、DNS 名、NetBIOS 名の情報が要求されます。

- *ドメインコントローラーのポーリング*。Active Directory の単位構造と Active Directory グループ内のデバイスの DNS 名に関する情報が、Kaspersky Security Center Cloud コンソールのデータベースに記録されます。

ポーリングの結果は、*Windows ネットワークのポーリング*と*ドメインコントローラーのポーリング*の方法別に、［**検出と製品の導入**］→［**検出**］セクションに表示されます。

*IP アドレス範囲のポーリング*方法のポーリング結果は、［**検出と製品の導入**］→［**未割り当てデバイス**］セクションに表示されます。

1 台のデバイスが複数の検出領域に表示される場合があります。あるデバイスが HQ ドメインで検出され、アドレスが 192.168.0.1 の場合、そのデバイスは［**Windows ドメイン**］セクションと［**未割り当てデバイス**］セクションの両方に表示されます。各ポーリング方法のネットワークポーリングの設定は変更できます。たとえば、ポーリングのスケジュールや、ポーリングの対象を Active Directory フォレストとするか特定のドメインのみにするかなどの設定が可能です。

Windows ネットワークのポーリング

Windows ネットワークのポーリングの概要

簡易ポーリングでは管理サーバーが、すべてのネットワークドメインとワークグループ内のデバイスの NetBIOS 名リストの情報のみ取得します。完全ポーリングでは、各クライアントデバイスに対して次の情報が要求されます：

- オペレーティングシステムの名前
- IP アドレス
- DNS 名
- NetBIOS 名

簡易ポーリングと完全ポーリングの両方で次の要件を満たす必要があります：

- UDP 137/138、TCP 139 ポートをネットワークで利用できる必要があります。
- Microsoft のコンピューターブラウザーサービスを必ず使用し、ディストリビューションポイント上でプライマリブラウザーコンピューターが有効である必要があります。
- Microsoft のコンピューターブラウザーサービスを必ず使用し、クライアントデバイス上でプライマリブラウザーコンピューターが有効であり、かつ次の条件を満たす必要があります：
  - ネットワークデバイスが 32 台以内の場合、1 台以上のデバイスで実行する
  - ネットワークデバイス 32 台につき、1 台以上のデバイスで

完全ポーリングは簡易ポーリングを 1 回以上実行している場合にのみ実行できます。

Windows ネットワークのポーリング設定の表示と変更

Windows ネットワークのポーリングのプロパティを変更するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
3. ネットワークポーリングに使用するディストリビューションポイントの名前をクリックします。
   ディストリビューションポイントのプロパティウィンドウが開きます。
4. ［**Windows ドメインのポーリング**］セクションを選択します。
5. ［**ネットワークポーリングを有効にする**］を使用して、Windows ネットワークのポーリングをオンまたはオフにします。
6. 簡易ポーリングと完全ポーリングのスケジュールを設定します。

7. ［OK］をクリックします。

プロパティが保存され、検出されたすべての Windows ドメインおよびワークグループに適用されます。

ドメインコントローラーのポーリング

Kaspersky Security Center Cloud コンソールは、Microsoft Active Directory ドメインコントローラーと Samba ドメインコントローラーのポーリングをサポートしています。Samba ドメインコントローラーの場合、Samba 4 が Active Directory ドメインコントローラーとして使用されます。ドメインコントローラーまたはディストリビューションポイントをポーリングすると、ドメイン構造、ユーザーアカウント、セキュリティグループ、およびドメインに含まれるデバイスの DNS 名に関する情報を取得します。ドメインコントローラーのポーリングは、設定したスケジュールに従って実行されます。

必須条件

ドメインコントローラーをポーリングする前に、次のプロトコルが有効になっていることを確認してください：

- 簡易認証およびセキュリティ層（SASL）
- ライトウェイトディレクトリアクセスプロトコル（LDAP）

ドメインコントローラーデバイスで次のポートが使用可能であることを確認してください：

- SASL の場合は 389
- TLS の場合は 636

ディストリビューションポイントを使用したドメインコントローラーのポーリング

ディストリビューションポイントを使用してドメインコントローラーをポーリングすることもできます。Windows または Linux ベースの管理対象デバイスは、ディストリビューションポイントとして機能できます。

Linux ディストリビューションポイントの場合、Microsoft Active Directory ドメインコントローラーと Samba ドメインコントローラーのポーリングがサポートされています。
Windows ディストリビューションポイントの場合、Microsoft Active Directory ドメインコントローラーのポーリングのみがサポートされます。
Mac ディストリビューションポイントを使用したポーリングはサポートされていません。

ディストリビューションポイントを使用してドメインコントローラーのポーリングを設定するには：

1. ディストリビューションポイントのプロパティを開きます。
2. ［**ドメインコントローラーのポーリング**］セクションを選択します。
3. ［**ドメインコントローラーのポーリングを有効にする**］をオンにします。
4. ポーリングするドメインコントローラーを選択します。

Linux ディストリビューションポイントを使用する場合は、［**指定したドメインのポーリング**］セクションで、［**追加**］をクリックし、ドメインコントローラーのアドレスとユーザー資格情報を指定します。

Windows ディストリビューションポイントを使用する場合は、次のオプションのいずれかをオンにできます：

- **現在のドメインのポーリング**
- **ドメインフォレスト全体のポーリング**
- **指定したドメインのポーリング**

5. 必要に応じて、［**ポーリングのスケジュールを設定する**］をクリックして、ポーリングスケジュールオプションを指定します。

   ポーリングは、指定されたスケジュールに従ってのみ開始されます。ポーリングを手動で開始することはできません。

ポーリングが完了すると、ドメイン構造が［**ドメインコントローラー**］セクションに表示されます。

デバイス移動ルールを設定し有効にしている場合、新たに検出されたデバイスは自動的に［**管理対象デバイス**］グループに含まれます。移動ルールがオンでない場合、新たに検出されたデバイスは自動的に**未割り当てデバイス**グループに含まれます。

検出されたユーザーアカウントは、Kaspersky Security Center Cloud コンソールでのドメイン認証に使用できます。

ドメインコントローラーのポーリング結果の表示

ドメインコントローラーのポーリング結果を表示するには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**ドメインコントローラー**］の順に選択します。

   検出された組織単位のリストが表示されます。

2. 組織単位を選択し、［**デバイス**］をクリックします。

   組織単位に含まれるデバイスのリストが表示されます。

リスト内を検索したり、結果をフィルターすることができます。

IP アドレス範囲のポーリング

Kaspersky Security Center Cloud コンソールは、通常の DNS 要求を使用して、指定された範囲のすべての IP アドレスに対して、IP アドレスを DNS 名へ解決する逆引きの名前解決を試行します。この処理が成功すると、取得した名前に対してサーバーは「`ICMP ECHO REQUEST`（Ping コマンドと同一）」を送信します。これに対してデバイスが応答した場合、デバイスの情報が Kaspersky Security Center Cloud コンソールのデータベースに追加されます。逆引きの名前解決は、IP アドレスを付与されているがコンピューターではないネットワークデバイス（ネットワークプリンターやルーターなど）を除外するために必要です。

このポーリング方法は、ローカル DNS サービスが適切に構成されているかどうかに依存します。ローカル DNS サービスで、逆引きの検索ゾーンが設定されている必要があります。逆引きの検索ゾーンが設定されていない場合、IP アドレス範囲のポーリングを実行しても、ポーリング結果は得られません。Active Directory を使用しているネットワークでは、こうした検索ゾーンが自動的に維持されます。ただし、これらのネットワークでは、IP アドレス範囲のポーリングを使用しても Active Directory のポーリングで得られる以上の情報は取得できません。また、ネットワーク規模が小さい場合、その他のネットワークサービスでは逆引きの検索ゾーンが必要ないことが多いため、管理者が逆引きの検索ゾーンを設定していない場合も多いです。こうした理由から、IP アドレス範囲のポーリングは既定ではオフになっています。

最初に、Kaspersky Security Center Cloud コンソールは、ネットワークポーリングに使用するディストリビューションポイントデバイスのネットワーク設定からポーリング用の IP アドレス範囲を取得します。デバイスアドレスが 192.168.0.1 でサブネットマスクが 255.255.255.0 の場合、Kaspersky Security Center Cloud コンソールは 192.168.0.0/24 ネットワークをポーリング対象のアドレスのリストに自動的に含めます。Kaspersky Security Center Cloud コンソールは 192.168.0.1 から 192.168.0.254 までのすべてのアドレスのポーリングを実行します。

Windows ネットワークのポーリングや Active Directory のポーリングを使用する場合は、IP アドレス範囲のポーリングの使用は推奨されません。

IP アドレス範囲のポーリング設定の表示と変更

IP アドレス範囲のポーリング設定の表示と変更を行うには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
3. ネットワークポーリングに使用するディストリビューションポイントの名前をクリックします。
   ディストリビューションポイントのプロパティウィンドウが開きます。
4. ［**IP アドレス範囲のポーリング**］セクションを選択します。
5. ［**IP アドレス範囲のポーリングを有効にする**］を使用して、IP ポーリングをオンまたはオフにします。
6. ポーリングスケジュールを設定します。既定では、IP ポーリングは 420 分（7 時間）ごとに実行されます。
7. 必要に応じて、ポーリングする IP アドレス範囲を追加または変更します。
   ポーリング間隔の指定時には、指定する値が［IP アドレスの有効期間］の値を超えないように注意してください。IP アドレスの有効期間の間にポーリングによって IP アドレスが確認されなかった場合、この IP アドレスはポーリングの結果から自動的に削除されます。既定では、（DHCP プロトコルを使用して割り当てられる）動的 IP アドレスは 24 時間ごとに変更されるので、ポーリング結果の有効期間は 24 時間です。
8. ［**OK**］をクリックします。

プロパティが保存され、すべての IP アドレス範囲に適用されます。

Samba ドメインコントローラーの設定

Kaspersky Security Center Cloud コンソールは、Samba 4 上でのみ実行される Linux ドメインコントローラーをサポートします。

Samba ドメインコントローラーは、Microsoft Active Directory ドメインコントローラーと同じスキーマ拡張をサポートします。Samba 4 スキーマ拡張機能を使用すると、Samba ドメインコントローラーと Microsoft Active Directory ドメインコントローラーとの完全な互換性を有効にすることができます。これはオプションのアクションです。

Samba ドメインコントローラーと Microsoft Active Directory ドメインコントローラーの完全な互換性を有効にすることを推奨します。これにより、Kaspersky Security Center Cloud コンソールと Samba ドメインコントローラー間の適切な対話が保証されます。

Samba ドメインコントローラーと Microsoft Active Directory ドメインコントローラーの完全な互換性を有効にするには、次の手順を実行します：

1. RFC2307 スキーマ拡張を使用するには、次のコマンドを実行します：

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Samba ドメインコントローラーでスキーマのアップデートを有効にします。これを行うには、ファイル /etc/samba/smb.conf に以下の行を追加します：

   ```
   dsdb:schema update allowed = true
   ```

   スキーマのアップデートがエラーで完了した場合は、スキーママスターとして機能するドメインコントローラーの完全な復元を実行する必要があります。

Samba ドメイン コントローラーを正しくポーリングするには、/etc/samba/smb.conf ファイルで `netbios name` と `workgroup` パラメータを指定する必要があります。

IP アドレス範囲の追加と変更

最初に、Kaspersky Security Center Cloud コンソールは、ネットワークポーリングに使用するディストリビューションポイントデバイスのネットワーク設定からポーリング用の IP アドレス範囲を取得します。デバイスアドレスが 192.168.0.1 でサブネットマスクが 255.255.255.0 の場合、Kaspersky Security Center Cloud コンソールは 192.168.0.0/24 ネットワークをポーリング対象のアドレスのリストに自動的に含めます。Kaspersky Security Center Cloud コンソールは 192.168.0.1 から 192.168.0.254 までのすべてのアドレスのポーリングを実行します。自動的に定義された IP アドレス範囲を編集したり、カスタム IP アドレス範囲を追加できます。

新しい IP アドレス範囲を追加するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
3. ネットワークポーリングに使用するディストリビューションポイントの名前をクリックします。
   ディストリビューションポイントのプロパティウィンドウが開きます。
4. ［**IP アドレス範囲のポーリング**］セクションを選択します。
5. 新しい IP アドレス範囲を追加するには、［**追加**］をクリックします。
6. 表示されたウィンドウで、次の設定を行います：

- **名前**

  IP アドレス範囲の名前。「192.168.0.0/24」のように、指定した IP アドレス範囲自体を名前として使用することもできます。

- **IP 区間またはサブネットアドレスとマスク**

  開始 IP アドレスと終了 IP アドレスを指定するか、サブネットアドレスとサブネットマスクを指定して、IP アドレス範囲を設定します。サブネットは、個数の制限なく必要な数だけ追加できます。名前のある IP アドレス範囲同士での範囲の重複は許可されていませんが、1 つの IP アドレス範囲内の名前のないサブネット（IP 区間同士）にはそうした制限はありません。

- **IP アドレスの有効期間（時間）**

  このパラメータの指定時には、値がポーリングのスケジュールで指定したポーリング間隔を超えるように指定してください。IP アドレスの有効期間の間にポーリングによって IP アドレスが確認されなかった場合、この IP アドレスはポーリングの結果から自動的に削除されます。既定では、（DHCP プロトコルを使用して割り当てられる）動的 IP アドレスは 24 時間ごとに変更されるので、ポーリング結果の有効期間は 24 時間です。

7. ［**OK**］をクリックします。

IP アドレス範囲のリストに新しい IP アドレス範囲が追加されます。

ポーリングの完了後、［**デバイス**］を使用して、検出されたデバイスのリストを表示できます。既定では、ポーリング結果の有効期間は 24 時間で、これは IP アドレスの有効期間と同じ長さです。

ディストリビューションポイントと接続ゲートウェイの調整

Kaspersky Security Center Cloud コンソールの管理グループ構造では、次の機能が実行されます：

- ポリシー範囲の設定

  関連する設定をデバイスに適用する別の方法として、*ポリシープロファイル*を使用する方法があります。この場合、ポリシーの範囲は、タグ、Active Directory 組織単位内のデバイスの場所、Active Directory セキュリティグループの所属などによって設定されます。

- グループタスク範囲の設定

  管理グループの階層に基づいていない、グループタスク範囲の定義方法が存在します。これは、デバイス選択用のタスクと特定のデバイス用のタスクを使用することです。

- デバイスとセカンダリ管理サーバーへのアクセス権限の設定

- ディストリビューションポイントの割り当て

管理グループ構造を構築する際には、ディストリビューションポイントを最適に割り当てるために、組織ネットワークのトポロジーを考慮する必要があります。ディストリビューションポイントを最適に分散配置すると、組織ネットワークのトラフィック量を軽減できます。

組織の組織図とネットワークトポロジーに応じて、管理グループ構造に次の標準設定を適用できます：

- 単一のオフィス
- 複数の小規模なリモートオフィス

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

ディストリビューションポイントの数の計算と設定

ネットワークに存在するクライアントデバイスの数に応じて、必要となるディストリビューションポイントの数も多くなります。ネットワークに必要なディストリビューションポイントの数の計算には、次の表を使用します。

ディストリビューションポイントとして使用するデバイスは、十分な空きディスク容量があること、定期的にシャットダウンされないこと、スリープモードが無効になっていることを確認してください。

単一のセグメントで構成されるネットワーク上での、デバイス数に応じた用途専用のディストリビューションポイントの数

ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
300 台未満	0（ディストリビューションポイントを割り当てない）
300 以上	許容：N/10,000 + 1、推奨：N/5,000 + 2（N はネットワーク上のデバイスの数）

複数のセグメントで構成されるネットワーク上での、デバイス数に応じた用途専用のディストリビューションポイントの数

各ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
10 台未満	0（ディストリビューションポイントを割り当てない）
10... 100	1
100 以上	許容：N/10,000 + 1、推奨：N/5,000 + 2（N はネットワーク上のデバイスの数）

通常のクライアントデバイス（ワークステーション）のディストリビューションポイントとしての使用

通常のクライアントデバイス（ワークステーション）をディストリビューションポイントとして使用する場合、管理サーバーと通信チャネルの負荷低減のために、下表に従ってディストリビューションポイントを割り当ててください。

単一のセグメントで構成されるネットワーク上での、デバイス数に応じた、ディストリビューションポイントとして動作するワークステーションの数

ネットワークセグメントでのクライアントデバイスの数	ディストリビューションポイントの数
300 台未満	0（ディストリビューションポイントを割り当てない）
300 以上	N/300 + 1（N はネットワーク上のデバイスの数。ただし、ディストリビューションポイントは 3 台以上必要）

複数のセグメントで構成されるネットワーク上での、デバイス数に応じた、ディストリビューションポイントとして動作するワークステーションの数

各ネットワークセグメントでのク	ディストリビューションポイントの数

ライアントデバイスの数	
10 台未満	0（ディストリビューションポイントを割り当てない）
10... 30	1
31... 300	2
300 以上	N/300 + 1（N はネットワーク上のデバイスの数。ただし、ディストリビューションポイントは 3 台以上必要）

ディストリビューションポイントが使用できない場合は、定義データベース、ソフトウェアモジュール、カスペルスキー製品を手動でアップデートするか、カスペルスキーのアップデートサーバーから直接アップデートします。

ディストリビューションポイントの標準設定：単一のオフィス

標準の「単一のオフィス」設定では、すべてのデバイスが組織ネットワーク内に置かれているため、お互いを「見る」ことができます。組織ネットワークは、いくつかの部分に区切られ（ネットワークまたはネットワークセグメント）、狭い帯域幅によって連結されるかたちで構成されている場合があります。

管理グループの構造は、次の方法で構築することが可能です：

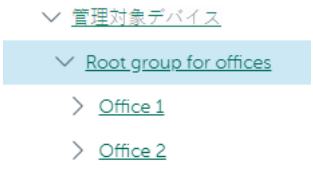
- ネットワークトポロジーを考慮に入れて管理グループの構造を構築します。管理グループの構造が、厳密にネットワークトポロジーを反映していなくても問題ありません。ネットワークが区切られた各部分と特定の管理グループの間に一致があれば十分です。

- ネットワークトポロジーを考慮に入れずに管理グループの構造を構築します。この場合は、ディストリビューションポイントとして動作する 1 台以上のデバイスをネットワークの区切られた各部分のルート管理グループ（たとえば、**管理対象デバイス**グループ）に対して割り当てる必要があります。ディストリビューションポイントは、すべて同じレベルに置かれ、組織ネットワーク内のすべてのデバイスを包含する同じ範囲を対象とします。この場合、各ネットワークエージェントは最短経路のディストリビューションポイントに接続します。ディストリビューションポイントへの経路は、tracert ユーティリティによって追跡できます。

ディストリビューションポイントの標準設定：複数の小規模なリモートオフィス

この標準設定は、インターネットを介して本社と通信する可能性のある多数の小規模なリモートオフィス向けの設定です。各リモートオフィスは NAT を介するようにその背後に配置されています。つまり、2 つのオフィスはお互いに分離されているため、お互いに接続することはできません。

管理グループ構造内で設定を反映させる必要があります。つまり、各リモートオフィスに対して、個別の管理グループを作成する必要があります（下の図のグループ［**Office 1**］と［**Office 2**］）。



管理グループ構造に含まれているリモートオフィス

1つのオフィスに対応する各管理グループに対して、1つまたは複数個のディストリビューションポイントを割り当てる必要があります。ディストリビューションポイントは、空きディスク容量が十分なリモートオフィスにあるデバイスである必要があります。たとえば、［**Office 1**］グループに導入されているデバイスは、［**Office 1**］管理グループに割り当てられているディストリビューションポイントにアクセスできます。

ノート PC を持ち運んでオフィス間を移動するユーザーが存在する場合は、各リモートオフィスで 2 台以上のデバイス（既存のディストリビューションポイントに加えて）を選択し、それらのデバイスをトップレベルの管理グループ（上の図の［**Root group for offices**］）用のディストリビューションポイントとして動作するように割り当てる必要があります。

例：［**Office 1**］管理グループ内にノート PC を導入しましたが、［**Office 2**］管理グループに対応するオフィスにマシンを持って移動するとします。ノート PC を移動させると、ネットワークエージェントは［**Office 1**］グループに割り当てられているネットワークエージェントへのアクセスを試行しますが、これらのディストリビューションポイントは使用不可の状態です。次に、ネットワークエージェントは、［**Root group for offices**］に割り当てられているディストリビューションポイントへのアクセスの試行を開始します。リモートオフィスはお互いに分離されているため、［**Root group for offices**］管理グループに割り当てられているディストリビューションポイントへのアクセスの試行は、ネットワークエージェントが［**Office 2**］グループ内にあるディストリビューションポイントへのアクセスを試行した際にのみ正常に実行されます。つまり、ノート PC は最初のオフィスに対応する管理グループ内に残りますが、ディストリビューションポイントについては移動後のオフィスに存在するディストリビューションポイントを使用します。

ディストリビューションポイントの手動での割り当て

Kaspersky Security Center Cloud コンソールで、ディストリビューションポイントとして動作するデバイスを手動で指定できます。ネットワークに必要なディストリビューションポイントの数と設定を計算することを推奨します。

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

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

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

ディストリビューションポイントとして動作するデバイスを手動で指定するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。
3. ［**割り当て**］をクリックします。
4. ディストリビューションポイントとして動作させるデバイスを選択します。
   デバイスを選択する際は、ディストリビューションポイントの動作とディストリビューションポイントとして動作するデバイスの要件を確認してください。
5. 選択したディストリビューションポイントの受け持ち範囲に含める管理グループを選択します。
6. ［**追加**］をクリックします。

追加されたディストリビューションポイントが、［**ディストリビューションポイント**］セクションのディストリビューションポイントのリストに表示されます。

7. 新しく追加したディストリビューションポイントをリストから選択し、プロパティウィンドウを開きます。

8. プロパティウィンドウでディストリビューションポイントを設定します。

- ［**全般**］セクションには、ディストリビューションポイントとクライアントデバイス間の対話の設定があります。

  - **SSL ポート**

    SSL を使用したクライアントデバイスとディストリビューションポイントの間の暗号化接続で使用する SSL ポートの番号。

    既定では、ポート 13000 が使用されます。

  - **マルチキャストを使用する**

    このオプションをオンにすると、グループ内にあるクライアントデバイスへのインストールパッケージの自動配布に IP マルチキャストが使用されます。

    IP マルチキャストを使用すると、インストールパッケージからクライアントデバイスのグループに製品をインストールするのに必要な時間が短縮されます。一方で、1 台のクライアントデバイスに製品をインストールする場合は、インストールの時間は長くなります。

  - **マルチキャスト IP アドレス**

    マルチキャストで使用される IP アドレス。224.0.0.0 ～ 239.255.255.255 の範囲で IP アドレスを定義できます。

    既定では、Kaspersky Security Center Cloud コンソールは定められた範囲内で一意の IP マルチキャストアドレスを自動的に割り当てます。

  - **IP マルチキャストポート番号**

    IP マルチキャストのポート番号。

    既定では、ポート番号は 15001 です。管理サーバーがインストールされたデバイスがディストリビューションポイントとして指定された場合、既定では SSL 接続でポート 13001 が使用されます。

  - **アップデートの配信**

アップデートは、次のアップデート元から管理対象デバイスに配布されます：

- このオプションがオンの場合は、このディストリビューションポイントです。
- このオプションがオフの場合は、管理サーバーやカスペルスキーのアップデートサーバーなどその他のディストリビューションポイントです。

アップデートの配信にディストリビューションポイントを使用している場合は、ダウンロード数を減らすため、トラフィックを節約できます。また、管理サーバーの負荷を軽減し、ディストリビューションポイント間の負荷を移動することもできます。ネットワークのディストリビューションポイントの数を計算して、トラフィックと負荷を最適化できます。

このオプションをオフにすると、アップデートのダウンロード数が増えて管理サーバーの負荷が増加する可能性があります。既定では、このオプションはオンです。

- **インストールパッケージの配布**

インストールパッケージは、次の配布元から管理対象デバイスに配布されます：

- このオプションがオンの場合は、このディストリビューションポイントです。
- このオプションがオフの場合は、管理サーバーやカスペルスキーのアップデートサーバーなどその他のディストリビューションポイントです。

インストールパッケージの配信にディストリビューションポイントを使用すると、ダウンロード数を減らすため、トラフィックを節約できます。また、管理サーバーの負荷を軽減し、ディストリビューションポイント間の負荷を移動することもできます。ネットワークのディストリビューションポイントの数を計算して、トラフィックと負荷を最適化できます。

このオプションをオフにすると、アップデートのダウンロード数が増えて管理サーバーの負荷が増加する可能性があります。既定では、このオプションはオンです。

- **プッシュサーバーを実行**

Kaspersky Security Center Cloud コンソールでは、ディストリビューションポイントは、ネットワークエージェントによって管理される Windows ベースおよび Linux ベースのデバイスのプッシュサーバーとして機能できます。プッシュサーバーの管理デバイスの範囲は、プッシュサーバーを有効にするディストリビューションポイントの範囲と同じです。同一の管理グループに複数のディストリビューションポイントを割り当てている場合は、各ディストリビューションポイントに対してプッシュサーバーを有効に設定できます。この場合、管理サーバーはディストリビューション間の負荷を分散します。

- **プッシュサーバーのポート**

プッシュサーバー用のポート番号です。使用されていないポートの番号を入力できます。

- ［**範囲**］セクションで、ディストリビューションポイントがアップデートを配信する範囲を指定します（管理グループまたはネットワークロケーション）。

Windows オペレーティングシステムが実行されているデバイスのみが、ネットワークロケーションを判別できます。他のオペレーティングシステムが実行されているデバイスのネットワークロケーションを判別することはできません。

- ［**KSN プロキシ**］セクションでは、ディストリビューションポイントを使用して管理対象デバイスからの KSN リクエストを転送するようにアプリケーションを設定できます：

  ディストリビューションポイントで KSN プロキシを有効にする

  ディストリビューションポイントとして使用しているデバイス上で KSN プロキシサービスが実行されます。この機能を使用することで、ネットワーク上でトラフィックを分配しなおし、最適化できます。

  この機能は、Linux または macOS を実行するディストリビューションポイントデバイスでサポートされていません。

  ディストリビューションポイントは、Kaspersky Security Network に関する声明に記載されている KSN の統計情報をカスペルスキーに送信します。既定では、KSN 声明は「%ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula」にあります。

  既定では、このオプションはオフです。管理サーバーのプロパティウィンドウで、［**Kaspersky Security Network への参加に同意する**］がオンになっている場合にのみ使用できます。

  アクティブ / パッシブモードのクラスターのノードをディストリビューションポイントに割り当て、ノード上で KSN プロキシサーバーを有効にできます。

- ディストリビューションポイントによる、Windows ドメイン、Active Directory、および IP アドレス範囲のポーリングを設定します：

  - **Windows ドメインのポーリング**

    Windows ドメインに対するデバイスの検索を有効にし、スケジュールを設定できます。

  - **Active Directory**

    Active Directory に対するネットワークのポーリングを有効にし、ポーリングのスケジュールを設定できます。

    Windows ディストリビューションポイントを使用する場合は、次のオプションのいずれかをオンにできます：

    - **現在の Active Directory ドメインのポーリング**
    - **Active Directory ドメインフォレストのポーリング**
    - **指定した Active Directory ドメインのみポーリング**：このオプションを選択した場合、1 つ以上の Active Directory ドメインをリストに追加してください

    ネットワークエージェント 15 がインストールされた Linux ディストリビューションポイントを使用する場合は、アドレスとユーザー資格情報を指定した Active Directory ドメインのみをポーリングできます。現在の Active Directory ドメインと Active Directory ドメインフォレストのポーリングは使用できません。

  - **IP アドレス範囲のポーリング**

デバイスの検索は IPv4 範囲および IPv6 ネットワークで有効にできます。

［**IP アドレス範囲のポーリングを有効にする**］をオンにすると、対象範囲を追加して実行スケジュールを設定できます。スキャン対象範囲のリストに IP アドレス範囲を追加できます。

［**Zeroconf を使用して IPv6 ネットワークのポーリングを実行する**］をオンにすると、ディストリビューションポイントは自動的にゼロコンフィギュレーションネットワーキング（「*Zeroconf*」とも表記）を使用して IPv6 ネットワークのポーリングを行います。この場合、ディストリビューションポイントはネットワーク全体を検索するため、指定した IP 範囲は無視されます。ディストリビューションポイントが Linux を実行している場合は、［**Zeroconf を使用して IPv6 ネットワークのポーリングを実行する**］を使用できます。Zerocong IPv6 ポーリングを使用するには、ディストリビューションポイントで avahi-browse ユーティリティをインストールする必要があります。

- ［**詳細**］セクションで、配信されたデータの格納用にディストリビューションポイントが使用するフォルダーを指定します：
  - **既定のフォルダーを使用する**

    このオプションをオンにすると、ディストリビューションポイント上でネットワークエージェントがインストールされているフォルダーが使用されます。

  - **指定したフォルダーを使用する**

    このオプションをオンにすると、この下のフィールドで、フォルダーのパスを指定できます。ディストリビューションポイントのローカルフォルダーまたは組織ネットワーク内の任意のデバイス上にあるフォルダーを指定できます。

    ネットワークエージェントの実行時にディストリビューションポイントで使用されるユーザーアカウントには、指定したフォルダーへの読み取りおよび書き込みアクセス権限が必要です。

9. ［**OK**］をクリックします。

選択されたデバイスがディストリビューションポイントとして使用されます。

管理グループに割り当てられたディストリビューションポイントのリストの編集

特定の管理グループに割り当てられたディストリビューションポイントのリストを表示し、ディストリビューションポイントを追加または削除してこのリストを編集できます。

管理グループに割り当てられたディストリビューションポイントのリストの表示と編集を行うには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ**］の順に選択します。
2. 管理グループのリストで、割り当てられたディストリビューションポイントを表示する管理グループを選択します。
3. ［**ディストリビューションポイント**］タブをクリックします。

4. ［**割り当て**］を使用して新しいディストリビューションポイントを管理グループに追加したり、割り当てられているディストリビューションポイントを［**割り当て解除**］を使用して削除することができます。

変更内容に応じて、新しいディストリビューションポイントがリストに追加されるか、既存のディストリビューションポイントがリストから削除されます。

ディストリビューションポイントのプッシュサーバーとしての使用

Kaspersky Security Center Cloud コンソールでは、ディストリビューションポイントは、ネットワークエージェントによって管理される Windows ベースおよび Linux ベースのデバイスのプッシュサーバーとして機能できます。プッシュサーバーの管理デバイスの範囲は、プッシュサーバーを有効にするディストリビューションポイントの範囲と同じです。同一の管理グループに複数のディストリビューションポイントを割り当てている場合は、各ディストリビューションポイントに対してプッシュサーバーを有効に設定できます。この場合、管理サーバーはディストリビューション間の負荷を分散します。

ディストリビューションポイントをプッシュサーバーとして使用して、管理対象デバイスと管理サーバー間の継続的な接続を確認できます。ローカルタスクの実行と停止、管理対象アプリケーションの統計の受信、トンネルの作成など、一部の操作には継続的な接続が必要です。ディストリビューションポイントをプッシュサーバーとして使用する場合は、ネットワークエージェントの UDP ポートにパケットを送信する必要はありません。

ディストリビューションポイントをプッシュサーバーとして使用するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。

3. プッシュサーバーとして使用するディストリビューションポイントをクリックします。

4. 選択したディストリビューションポイントのプロパティリストで、［**全般**］セクションに移動し、［**プッシュサーバーを実行**］をオンにします。
   ［**プッシュサーバーのポート**］入力フィールドが使用可能になります。

5. ［**プッシュサーバーのポート**］入力フィールドで、クライアントデバイスの接続に使用されるディストリビューションポイントのポートを指定します。既定では、ポート 13295 が使用されます。

   プッシュサーバーとして機能するディストリビューションポイントと管理対象デバイスとの間の接続を確立するには、指定したプッシュサーバーのポートを Microsoft Windows ファイアウォールの除外リストに手動で追加する必要があります。

6. ［OK］をクリックしてディストリビューションポイントのプロパティウィンドウを終了し、［**保存**］をクリックして変更を適用します。
   ［**プッシュサーバーを実行**］をオンにすると、プッシュサーバーとして機能するディストリビューションポイントで［**管理サーバーから切断しない**］が自動的にオンになります。このオプションは、ネットワークエージェントと管理サーバー間の早期接続を提供します。

7. ［ネットワークエージェントのポリシーの設定］ウィンドウを開きます。

8. ［**接続**］→［**ネットワーク**］の順に移動し、［**ディストリビューションポイントを使用して管理サーバーへ強制的に接続する**］をオンにします。このオプションのロックをオフにします。

9. また、［**ネットワーク**］サブセクションで、［**UDP ポートを使用する**］をオフにすることもできます。設定されたプッシュサーバーは、UDP ポート経由でパケットを送信する代わりに、管理対象デバイスと管理サーバー間の継続的な接続を提供します。

10. ［**OK**］をクリックして、ウィンドウを閉じます。

ディストリビューションポイントがプッシュサーバーとしての動作を開始します。クライアントデバイスへのプッシュ通知が送信可能になります。

［管理サーバーから切断しない］オプションを使用して、管理対象デバイスと管理サーバー間の継続的な接続を提供する

プッシュサーバーを使用しない場合、Kaspersky Security Center Cloud コンソールは、管理対象デバイスと管理サーバー間の継続的な接続を提供しません。管理対象デバイスのネットワークエージェントが、定期的に接続を確立し、管理サーバーと同期させます。同期セッションの間隔は、ネットワークエージェントのポリシーで定義されます。早期の同期実行が必要な場合、管理サーバー（または、使用されているディストリビューションポイント）は署名されたネットワークパケットを、IPv4 または IPv6 ネットワーク経由でネットワークエージェントの UDP ポートへ送信します。既定では、ポート番号は 15000 です。管理サーバーと管理対象デバイスとの間で UDP を使用した接続が確立できない場合、同期間隔の間の次の定期接続時に、ネットワークエージェントと管理サーバー間で同期が実行されます。

一部の動作は、ネットワークエージェントと管理サーバーが事前に接続されていないと実行できません。例：ローカルタスクの実行と停止、管理対象アプリケーションの統計情報の受信、トンネリング接続の作成など。この問題を解決するには、プッシュサーバーを使用していない場合は、［**管理サーバーから切断しない**］を使用し、管理対象デバイスと管理サーバーの間に継続的な接続があることを確認します。

クライアントデバイスと管理サーバー間の継続的な接続を確認するには：

1. 次のいずれかの手順を実行します：

   - 管理対象デバイスが管理サーバーに直接アクセスする場合（ディストリビューションポイントを経由しない場合）：

     a. メインメニューで、［**デバイス**］→［**管理対象デバイス**］の順に選択します。

     b. 継続的な接続を提供するデバイスの名前をクリックします。

     管理対象デバイスのプロパティウィンドウが表示されます。

   - 管理対象デバイスが、直接ではなく、ゲートウェイモードで実行されているディストリビューションポイントを介して管理サーバーにアクセスする場合：

     a. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

     管理サーバーのプロパティウィンドウが開きます。

     b. ［**全般**］タブで、［**ディストリビューションポイント**］セクションを選択します。

     c. ディストリビューションポイントのリストで、必要なディストリビューションポイントの名前をクリックします。

     選択したディストリビューションポイントのプロパティウィンドウが表示されます。

2. 表示されたプロパティウィンドウの［**全般**］セクションで、［**管理サーバーから切断しない**］をオンにします。

継続的な接続が、管理デバイスと管理サーバー間で確立されます。

［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

管理グループの作成

最初は、管理グループの階層には［**管理対象デバイス**］という名前の管理グループのみ含まれています。管理グループの階層の作成時に、デバイスと仮想マシンを［**管理対象デバイス**］グループに追加したり、サブグループを追加したりできます。各管理グループのプロパティウィンドウには、グループに関連するポリシー、タスク、デバイスに関する情報が含まれています。

管理グループを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. 新しいサブグループを作成する管理グループの横にあるチェックボックスをオンにします。
3. ［**追加**］をクリックします。
4. 新しい管理グループの名前を入力します。
5. ［**追加**］をクリックします。

   指定した名前の新しい管理グループが管理グループの階層に表示されます。

Active Directory またはドメインネットワークの構造に基づいて、管理グループの階層を作成することが可能です。テキストファイルからグループの構成を作成することも可能です。

管理グループの構造を作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. ［**インポート**］をクリックします。

   新規管理グループ構造作成ウィザードが開始します。ウィザードの指示に従ってください。

デバイス移動ルールの作成

デバイスを自動的に管理グループに割り当てるデバイス移動ルールを設定できます。

移動ルールを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**移動ルール**］の順に移動します。
2. ［**追加**］をクリックします。
3. 表示されたウィンドウの［**全般**］タブで、次の情報を指定します：

- **ルール名**

  新しいルールの名前を入力します。

  ルールのコピー時には、新しいルールでは、元のルールと同じ名前に「(1)」のようなインデックス「(数字)」が追加されます。

- **管理グループ**

  デバイスを自動的に移動する移動先の管理グループを選択します。

- **アクティブなルール**

  このオプションをオンにすると、ルールの保存後にルールが有効になり適用されます。

  このオプションをオフにすると、ルールは作成されますがオフの状態です。このオプションをオンにするまで、ルールは適用されません。

- **どの管理グループにも属していないデバイスのみ移動する**

  このオプションをオンにすると、未割り当てデバイスのみが選択したグループに移動します。

  このオプションをオフにすると、既に管理グループに割り当てられているデバイスと未割り当てデバイスの両方が選択したグループに移動します。

- **ルールの適用**

  次の中からいずれかを選択できます：

  - **各デバイスにつき1回**

    指定した条件に合致するデバイスで各デバイスにつき1回だけルールが適用されます。

  - **各デバイスで1度実行、以降はネットワークエージェントの再インストールごとに実行**

    指定した条件に合致するデバイスで各デバイスにつき1回ルールが適用され、その後はデバイスにネットワークエージェントが再インストールされた場合にのみ適用されます。

  - **ルールを永続的に適用**

    管理サーバーで自動的に設定されるスケジュールに従ってルールが適用されます（通常は数時間ごと）。

4. ［**ルールの条件**］タブで、デバイスを管理グループに移動する基準を少なくとも1つ指定します。

5. ［**保存**］をクリックします。

移動ルールが作成されます。新しいルールが移動ルールのリストに表示されます。

リストでの順位が高いほど、ルールの優先度が高くなります。移動ルールの優先度を上げたり下げたりするには、マウスを使用してルールをリスト内でそれぞれ上下に移動します。

デバイス属性が複数のルールの条件を満たしている場合、そのデバイスは優先度が最も高いルールの対象グループに移動されます（つまり、ルールのリスト内で最高ランク）。

デバイス移動ルールのコピー

異なる管理グループで同一のルールを使用する場合などに、移動ルールをコピーできます。

既存の移動ルールをコピーするには：

1. 次のいずれかの手順を実行します：

   - メインメニューで、［**アセット（デバイス）**］→［**移動ルール**］の順に移動します。
   - メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**移動ルール**］の順に移動します。

   移動ルールのリストが表示されます。

2. コピーするルールに隣接するチェックボックスをオンにします。
3. ［**コピー**］をクリックします。
4. 表示されるウィンドウで、必要に応じて［**全般**］タブで次の情報を変更します。ただし、設定を変更せずにルールのコピーのみを行う場合は、設定を変更する必要はありません：

   - **ルール名**

     新しいルールの名前を入力します。

     ルールのコピー時には、新しいルールでは、元のルールと同じ名前に「(1)」のようなインデックス「(数字)」が追加されます。

   - **管理グループ**

     デバイスを自動的に移動する移動先の管理グループを選択します。

   - **アクティブなルール**

     このオプションをオンにすると、ルールの保存後にルールが有効になり適用されます。

     このオプションをオフにすると、ルールは作成されますがオフの状態です。このオプションをオンにするまで、ルールは適用されません。

   - **どの管理グループにも属していないデバイスのみ移動する**

     このオプションをオンにすると、未割り当てデバイスのみが選択したグループに移動します。

     このオプションをオフにすると、既に管理グループに割り当てられているデバイスと未割り当てデバイスの両方が選択したグループに移動します。

   - **ルールの適用**

次の中からいずれかを選択できます：

- **各デバイスにつき1回**
  指定した条件に合致するデバイスで各デバイスにつき1回だけルールが適用されます。
- **各デバイスで1度実行、以降はネットワークエージェントの再インストールごとに実行**
  指定した条件に合致するデバイスで各デバイスにつき1回ルールが適用され、その後はデバイスにネットワークエージェントが再インストールされた場合にのみ適用されます。
- **ルールを永続的に適用**
  管理サーバーで自動的に設定されるスケジュールに従ってルールが適用されます（通常は数時間ごと）。

5. ［**ルールの条件**］タブで、自動的に移動するデバイスの基準を少なくとも1つ指定します。
6. ［**保存**］をクリックします。

新しい移動ルールが作成されます。新しいルールが移動ルールのリストに表示されます。

デバイスを管理グループへ手動で追加

デバイス移動ルールを作成してデバイスを管理グループに自動的に移動したり、選択した管理グループにデバイスを追加することで、デバイスを管理グループ間で手動で移動したりすることができます。このセクションでは、デバイスを管理グループに手動で追加する手順を説明します。

特定の管理グループに1台以上のデバイスを手動で追加するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. リストの上にある［**現在のパス：**<現在のパス>］をクリックします。
3. 表示されるウィンドウで、デバイスを追加する管理グループを選択します。
4. ［**デバイスの追加**］をクリックします。
   デバイス移動ウィザードが起動します。
5. 管理グループに追加するデバイスのリストを作成します。

デバイスへの接続時に、またはデバイスの検出後に、管理サーバーのデータベースに既に情報が追加されているデバイスのみを追加できます。

デバイスをリストに追加する方法を選択します：

- ［**デバイスの追加**］をクリックして、次のいずれかの方法でデバイスを指定します：
  - 管理サーバーによって検出されたデバイスのリストからデバイスを選択します。
  - デバイスのIPアドレスまたはIPアドレス範囲を指定します。

- デバイスの NetBIOS 名または DNS 名を指定します。

  デバイス名のフィールドには、空白文字、バックスペース、および禁止されている文字（, \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %）を含めることはできません。

- ［**デバイスをファイルからインポート**］をクリックして、テキストファイルからデバイスのリストをインポートします。各デバイスのアドレスまたは名前をそれぞれの行に指定する必要があります。

  ファイルには、空白文字、バックスペース、および禁止されている文字（, \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %）を含めることはできません。

6. 管理グループに追加するデバイスのリストを表示します。デバイスを追加または削除することでリストを編集できます。

7. リストが正しいことを確認したら、［**次へ**］をクリックします。

ウィザードによってデバイスリストが処理され、結果が表示されます。正常に処理されたデバイスが管理グループに追加され、管理サーバーによって作成された名前でデバイスのリストに表示されます。

デバイスまたはクラスターを手動で管理グループに移動する

管理グループ間で、または未割り当てデバイスのグループから管理グループにデバイスを移動できます。

管理グループからクラスターまたはサーバーアレイを別の管理グループに移動することもできます。クラスターまたはサーバーアレイを別のグループに移動すると、そのすべてのノードも一緒に移動します。これは、クラスターとそのノードのいずれかが常に同じ管理グループに属しているためです。［**デバイス**］タブで単一のクラスターノードを選択すると、［**グループへ移動**］が使用できなくなります。

特定の管理グループに 1 台以上のデバイスまたはクラスターを移動するには：

1. デバイスの移動元の管理グループを開きます。開くには、次のいずれかの操作を行います：

   - 管理グループを開くには、メインメニューで、［**アセット（デバイス）**］→［**グループ**］→［**<グループ名>**］→［**管理対象デバイス**］の順に移動します。

   - ［**未割り当てデバイス**］のグループを開くには、メインメニューで、［**検出と製品の導入**］→［**未割り当てデバイス**］の順に移動します。

2. 管理グループにクラスターまたはサーバーアレイが含まれている場合、［**管理対象デバイス**］セクションは、［**デバイス**］タブと［**クラスターとサーバーアレイ**］タブの 2 つのタブに分割されます。移動するオブジェクトのタブを開きます。

3. 別のグループに移動するデバイスまたはクラスターに隣接するチェックボックスをオンにします。

4. ［**グループへ移動**］をクリックします。

5. 管理グループの階層で、選択したデバイスまたはクラスターの移動先の管理グループに隣接するチェックボックスをオンにします。

6. ［**移動**］をクリックします。

選択したデバイスまたはクラスターが、選択した管理グループに移動します。

未割り当てデバイスの保持ルールの設定

Windows のネットワークポーリングの完了後、検出されたデバイスは［未割り当てデバイス］管理グループのサブグループに配置されます。［**検出と製品の導入**］ - ［**検出**］ - ［**Windows ドメイン**］の順に移動すると、この管理グループが見つかります。［**Windows ドメイン**］フォルダーが親グループです。この親グループ内に、ポーリングで検出された対応ドメインとワークグループに基づいて命名された子グループが含まれています。親グループにはモバイルデバイスの管理グループが含まれる場合もあります。親グループとそれぞれの子グループで、未割り当てデバイスの保持ルールを設定できます。保持ルールはデバイスの検出の設定には依存せず、デバイスの検出が無効な場合でも機能します。

デバイスの保持ルールは、ディスク全体の暗号化で暗号化された1つ以上のドライブを備えたデバイスには影響しません。このようなデバイスは自動的に削除されず、手動でのみ削除できます。暗号化されたドライブを含むデバイスを削除する必要がある場合は、まずドライブを復号化してから、デバイスを削除してください。

未割り当てデバイスの保持ルールを設定するには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**Windows ドメイン**］の順に選択します。
2. 次のいずれかの手順を実行します：
   - 親グループの設定を編集するには、［**プロパティ**］をクリックします。
     Windows ドメインのプロパティウィンドウが開きます。
   - 子グループの設定を編集するには、目的の子グループの名前をクリックします。
     子グループのプロパティウィンドウが開きます。
3. 次の設定を定義します：
   - **次の期間デバイスが不可視の場合グループから削除（日）**

     このオプションをオンにすると、デバイスをグループから自動的に削除するまでの期間を指定できます。既定では、この設定が子グループにも反映されます。既定の期間は 7 日です。
     既定では、このオプションはオンです。
   - **親グループから継承する**

     このオプションをオンにすると、デバイスの保持期間が設定が親グループから現在のグループに継承され、変更することはできません。
     このオプションは子グループでのみ利用できます。
     既定では、このオプションはオンです。
   - **子グループへ強制的に継承する**

     設定値が子グループに配信され、子グループのプロパティではそれらの設定がロックされます。
     既定では、このオプションはオフです。

4. ［**同意**］をクリックします。

変更内容が保存され、適用されます。

ネットワーク保護の設定

このセクションには、ポリシーとタスクの手動設定、ユーザーロール、管理グループの構造とタスクの階層構造の構築に関する情報を記載しています。

シナリオ：ネットワーク保護の設定

クイックスタートウィザードにより、既定の設定でポリシーとタスクが作成されます。これらの設定は、組織のルールなどに照らして最適でない、または許容できない内容を含む可能性があります。したがって、ネットワークの必要性に応じて、これらのポリシーとタスクを調整し、他のポリシーとタスクを作成してください。

必須条件

開始する前に、クイックスタートウィザードを含む Kaspersky Security Center Cloud コンソールの初期設定シナリオを完了したことを確認してください。

クイックスタートウィザードの実行中に、［**管理対象デバイス**］管理グループに次のポリシーとタスクが作成されます：

- Kaspersky Endpoint Security のポリシー
- Kaspersky Endpoint Security をアップデートするグループタスク
- ネットワークエージェントのポリシー
- 脆弱性とアプリケーションのアップデートの検索（ネットワークエージェントのタスク）

実行するステップ

ネットワーク保護の設定は、次の手順で進みます：

1. **カスペルスキー製品のポリシーとポリシーのプロファイルの設定と各デバイスへの反映**

   管理対象デバイスにインストールされているカスペルスキー製品のポリシーとポリシーのプロファイルを設定しデバイスに反映するには、デバイスベースとユーザーベースの 2 種類のセキュリティ管理方法を使用できます。2 種類の方法を組み合わせることもできます。

2. **カスペルスキー製品のリモート管理用のタスクの設定**

   必要に応じて、クイックスタートウィザードを使用して作成したタスクを確認、調整します。

   実行手順の説明：

   - Kaspersky Endpoint Security をアップデートするグループタスクの設定
   - *脆弱性とアプリケーションのアップデートの検索タスクの作成*

   必要に応じて、クライアントデバイスにインストールされているカスペルスキー製品を管理するためのタスクを追加で作成します。

3. **データベースでのイベント情報による負荷の評価と制限**

管理対象アプリケーションの動作中のイベントに関する情報は、クライアントデバイスから送信され、管理サーバーデータベースに記録されます。管理サーバーの負荷を軽減するには、データベースに保管される可能性のあるイベント数の最大値を評価し、上限を設定します。

実行手順の説明：イベントの最大数の設定

結果

この手順を完了すると、カスペルスキー製品、タスク、管理サーバーで取得されるイベントの設定によってネットワークの保護が機能するようになります。

- ポリシーとポリシーのプロファイルに従ってカスペルスキー製品が設定されます。
- 製品が一連のタスクによって管理されるようになります。
- データベースに保存されるイベント数の上限が設定されます。

ネットワーク保護の設定が完了すると、定義データベースとカスペルスキー製品の定期アップデートの設定ステップに進むことができます。

デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理の概要

セキュリティ設定を、デバイスの仕様の観点やユーザーロールの観点から管理できます。1つ目のアプローチは*デバイスベースのセキュリティ管理*、2つ目のアプローチは*ユーザーベースのセキュリティ管理*と呼ばれます。異なるデバイスに異なる設定を適用するには、いずれかの管理方法あるいは両者を組み合わせた管理方法を使用できます。

デバイスベースのセキュリティ管理では、デバイスごとの状況などに合わせて、セキュリティ製品について複数の異なる設定を管理対象デバイスに適用できます。たとえば、異なる管理グループに属するデバイスに、異なる設定を適用できます。あるいは、Active Directory でデバイスに割り当てられている用途や、ハードウェアの仕様などに応じて、デバイスを区分することもできます。

ユーザーベースのセキュリティ管理を使用すると、ユーザーロールに応じて、異なるセキュリティ設定を適用できます。複数のユーザーロールを作成し、ユーザーごとに適切なユーザーロールを割り当てた上で、デバイスの所有者のユーザーロールに応じて、異なるセキュリティ設定をデバイスに適用できます。たとえば、経理部門の従業員と人事部門の従業員それぞれのデバイスに異なるアプリケーション設定を適用する場合などがありえます。これにより、ユーザーベースのセキュリティ管理を実施すると、経理部門の従業員と人事部門の従業員のカスペルスキー製品に対して、それぞれ独自の設定が適用されます。詳細設定により、製品設定のどの部分をユーザー側で設定でき、どの部分は管理者による設定が強制的に適用されるかを指定できます。

ユーザーベースのセキュリティ管理を使用すると、特定の1人のユーザーに特定の製品設定を適用できます。該当する従業員が社内で固有のロールを担っていたり、特定のユーザーのデバイスに関連したセキュリティ問題を監視したい場合などに、こうした処理が必要になることがあります。社内でのこの従業員のロールに基づいて、ユーザーが製品設定を変更できる権限を拡張したり制限できます。たとえば、ローカルオフィスのクライアントデバイスを管理しているシステム管理者の権限を拡張する場合などです。

デバイスベースのセキュリティ管理とユーザーベースのセキュリティ管理を組み合わせることもできます。たとえば、管理グループごとに製品ポリシーを設定した上で、企業内の1つ以上のユーザーロールを対象としたポリシープロファイルを作成するなどの方法を使用できます。この場合、ポリシーとポリシープロファイルは次の順序で適用されます。

1. デバイスベースのセキュリティ管理用に作成されたポリシーが適用されます。

2. ポリシーは、ポリシープロファイルの優先度に応じてポリシープロファイルで変更されます。

3. ポリシーは、ユーザーロールと関連付けられたポリシープロファイルで変更されます。

ポリシーの設定と継承先への反映：デバイスベースの管理

このセクションでは、管理対象デバイスにインストールされているカスペルスキー製品の設定をデバイスベースで一元的に行う手順について説明します。この手順を完了すると、すべての管理対象デバイスにインストールされている製品が、定義した製品ポリシーとポリシープロファイルに従って設定されます。

また、デバイスベースの管理方法の代替案もしくは追加で組み合わせて使用する管理方法としてユーザーベースのセキュリティ管理も検討すると有益な場合があります。

プロセス

カスペルスキー製品のデバイスベースの管理シナリオは、次の 2 つの手順からなります。

1. **製品ポリシーの設定**

   管理対象デバイスにインストールされているカスペルスキー製品ごとにポリシーを作成して、製品の設定を指定します。これらのポリシーはクライアントデバイスに反映されます。

   クイックスタートウィザードを使用してネットワークの保護を設定する場合、Kaspersky Security Center Cloud コンソールは Kaspersky Endpoint Security for Windows の既定のポリシーを作成します。このウィザードを使用して設定プロセスを完了した場合、この製品の新しいポリシーを作成する必要はありません。Kaspersky Endpoint Security ポリシーの手動セットアップに進みます。

   複数の管理グループからなる階層構造が存在する場合、既定では、子管理グループがプライマリ管理サーバーのポリシーを継承します。子グループでの継承を強制的に適用して、上位のポリシーで指定された設定の変更を禁止できます。一部の設定のみを強制的に継承させたい場合は、上位のポリシーで該当する設定項目をロックできます。残りのロックされていない設定は下位のポリシーで変更できます。ポリシーの階層を作成することで、管理グループ内の管理対象デバイスを効果的に管理できます。

   実行手順の説明：ポリシーの作成

2. **ポリシーのプロファイルの作成（任意）**

   同じ管理グループ内にあるデバイスを異なるポリシー設定に従って動作させる場合には、ポリシーのプロファイルを作成します。ポリシーのプロファイルには、ポリシー設定のサブセットが指定されています。このサブセットはポリシーとともに対象デバイスに配信され、*プロファイルの有効化条件*と呼ばれる特定の条件下でポリシーを補完する機能を果たします。プロファイルに含まれるのは、管理対象デバイスでアクティブな「基本」ポリシーとは異なる設定（差分）のみです。

   プロファイルの有効化条件を使用することで、たとえば、Active Directory の特定の組織単位やセキュリティグループに属するデバイス、特定のハードウェア設定のデバイス、特定のタグが付与されているデバイスなどの条件に応じて異なるポリシープロファイルを適用できます。タグを使用すると特定の基準を満たすデバイスをフィルタリングできます。たとえば、「*Windows*」というタグを作成し、Windows オペレーティングシステムを実行しているデバイスすべてにこのタグを付与し、ポリシープロファイルの有効化条件としてこのタグを指定します。これにより、Windows を実行しているすべてのデバイスにインストールされているカスペルスキー製品は該当するポリシープロファイルで管理されます。

   実行手順の説明：

   - ポリシーのプロファイルの作成
   - ポリシーのプロファイルの有効化ルールの作成

3. **ポリシーとポリシープロファイルの管理対象デバイスへの反映**

管理サーバーと管理対象デバイスは、Kaspersky Security Center Cloud コンソールを数時間ごとに自動的に同期します。同期中に、新しいまたは変更されたポリシーとポリシープロファイルが管理対象デバイスに反映されます。自動同期を回避して、［強制同期］コマンドを使用して手動で同期を実行できます。同期が完了すると、ポリシーとポリシープロファイルが配信され、インストールされているカスペルスキー製品に適用されます。

ポリシーとポリシーのプロファイルがデバイスに配信されたかを確認できます。Kaspersky Security Center Cloud コンソールでは、デバイスのプロパティで該当する配信日時が表示されます。

実行手順の説明：強制同期

結果

デバイスベースの管理の導入手順が完了すると、ポリシーの階層を通して指定または反映された設定がカスペルスキー製品に適用されます。

管理グループに新しく追加されたデバイスには、設定された製品ポリシーとポリシープロファイルが自動的に適用されます。

ポリシーの設定と継承先への反映：ユーザーベースの管理

このセクションでは、管理対象デバイスにインストールされているカスペルスキー製品の設定をユーザーベースで一元的に行う手順について説明します。この手順を完了すると、すべての管理対象デバイスにインストールされている製品が、定義した製品ポリシーとポリシープロファイルに従って設定されます。

また、ユーザーベースの管理方法の代替案もしくは追加で組み合わせて使用する管理方法として デバイスベースのセキュリティ管理も検討すると有益な場合があります。2 種類の管理方法について詳しくは、以下を参照してください。

プロセス

カスペルスキー製品のユーザーベースの管理シナリオは、次の 2 つの手順からなります。

1. **製品ポリシーの設定**

   管理対象デバイスにインストールされているカスペルスキー製品ごとにポリシーを作成して、製品の設定を指定します。これらのポリシーはクライアントデバイスに反映されます。

   クイックスタートウィザードを使用してネットワークの保護を設定する場合、Kaspersky Security Center Cloud コンソールは Kaspersky Endpoint Security の既定のポリシーを作成します。このウィザードを使用して設定プロセスを完了した場合、この製品の新しいポリシーを作成する必要はありません。Kaspersky Endpoint Security ポリシーの手動セットアップに進みます。

   複数の管理グループからなる階層構造が存在する場合、既定では、子管理グループがプライマリ管理サーバーのポリシーを継承します。子グループでの継承を強制的に適用して、上位のポリシーで指定された設定の変更を禁止できます。一部の設定のみを強制的に継承させたい場合は、上位のポリシーで該当する設定項目をロックできます。残りのロックされていない設定は下位のポリシーで変更できます。ポリシーの階層を作成することで、管理グループ内の管理対象デバイスを効果的に管理できます。

   実行手順の説明：ポリシーの作成

2. **デバイスの所有者の指定**

   管理対象デバイスを対応するユーザーに割り当てます。

   実行手順の説明：デバイスの所有者ユーザーの指定

3. **組織内の主なユーザーロールの定義**

   組織内の従業員が行う様々な業務の主要なものを検討します。すべての従業員がロールに従って振り分けられるようにする必要があります。たとえば、所属部門、職務内容、役職などで振り分けを行うことができます。この検討が完了したら、各グループに対応するユーザーロールを作成する必要があります。各ユーザーロールには、そのロールに固有の製品設定を含む独自のポリシープロファイルが割り当てられることを念頭において作業してください。

4. **ユーザーロールの作成**

   前の手順で定義した従業員のグループごとにユーザーロールの作成と設定を行うか、定義済みのユーザーロールを使用します。ユーザーロールには製品の各機能に対するアクセス権限が組み合わされたかたちで付与されます。

   実行手順の説明：ユーザーロールの作成

5. **各ユーザーロールの対象範囲の指定**

   作成したユーザーロールごとに、ロールを割り当てるユーザーやセキュリティグループ、管理グループを指定します。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

   実行手順の説明：各ユーザーロールの対象範囲の編集

6. **ポリシーのプロファイルの作成**

   組織内のユーザーロールごとに、ポリシープロファイルを作成します。ポリシープロファイルによって、ユーザーのデバイスにインストールされている製品にユーザーロールに応じてどの設定が適用されるかが定義されます。

   実行手順の説明：ポリシープロファイルの作成

7. **ポリシープロファイルとユーザーロールの関連付け**

   作成したポリシープロファイルをユーザーロールに関連付けます。完了すると、指定されたロールを割り当てられたユーザーに対してポリシープロファイルが有効になります。ユーザーのデバイスにインストールされているカスペルスキー製品に、ポリシープロファイルで指定した設定が適用されます。

   実行手順の説明：ポリシーのプロファイルとロールの関連付け

8. **ポリシーとポリシープロファイルの管理対象デバイスへの反映**

   管理サーバーと管理対象デバイスは、Kaspersky Security Center Cloud コンソールを数時間ごとに自動的に同期します。同期中に、新しいまたは変更されたポリシーとポリシープロファイルが管理対象デバイスに反映されます。自動同期を回避して、［強制同期］コマンドを使用して手動で同期を実行できます。同期が完了すると、ポリシーとポリシープロファイルが配信され、インストールされているカスペルスキー製品に適用されます。

   ポリシーとポリシーのプロファイルがデバイスに配信されたかを確認できます。Kaspersky Security Center Cloud コンソールでは、デバイスのプロパティで該当する配信日時が表示されます。

   実行手順の説明：強制同期

結果

ユーザーベースの管理の導入手順が完了すると、ポリシーの階層を通して指定または反映された設定がカスペルスキー製品に適用されます。

新規ユーザーに対しては、新しいアカウントを作成して作成済みのユーザーロールのいずれかを割り当て、デバイスをユーザーに割り当てる必要があります。このユーザーのデバイスには、設定された製品ポリシーとポリシープロファイルが自動的に適用されます。

Kaspersky Endpoint Security ポリシーの手動セットアップ

このセクションでは、 Kaspersky Endpoint Security ポリシーの設定方法に関する推奨事項について説明します。ポリシーのプロパティウィンドウで設定を実行できます。設定を編集する際には、関連する設定グループの右側にあるロックアイコンをクリックして、指定した値をワークステーションに適用します。

Kaspersky Security Network の設定

Kaspersky Security Network（KSN）は、ファイル、Web リソース、およびソフトウェアのレピュテーションに関する情報を持つクラウド サービスのインフラストラクチャです。Kaspersky Security Network を使用することで、 Kaspersky Endpoint Security for Windows はより迅速に様々な種類の脅威に対応し、保護コンポーネントのパフォーマンスを向上させ、誤検知の可能性を減らすことができます。Kaspersky Security Network の詳細は、 Kaspersky Endpoint Security for Windows のヘルプを参照してください。

Kaspersky Endpoint Security for Windows のポリシーのプロパティウィンドウの［**アプリケーション設定**］→［**Advanced Threat Protection**］セクションで、 Kaspersky Security Network の動作を設定できます。

KSN について推奨される設定を指定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。
   選択したポリシーのプロパティウィンドウが表示されます。
3. ポリシーのプロパティで、［**アプリケーション設定**］→［**先進の脅威対策**］→［**Kaspersky Security Network**］の順に選択します。
4. ［**管理サーバーを KSN プロキシサーバーとして使用する**］がオンになっていることを確認します。このオプションを使用することで、ネットワーク上でトラフィックを再分配し、最適化できます。

   > Managed Detection and Response を使用する場合、ディストリビューションポイントの［**KSN プロキシ**］をオンにし、拡張 KSN モードを有効にする必要があります。

5. （任意）［KSN プロキシサービスを使用できない場合は、KSN サーバーを使用する］を有効にします。これを行うには、［**KSN プロキシサーバーが使用できない場合は Kaspersky Security Network サーバーを使用する**］をオンにします。
   KSN サーバーは、カスペルスキー側に配置されている場合（KSN の使用時）とサードパーティ側に配置されている場合（KPSN の使用時）があります。
6. ［**OK**］をクリックします。

KSN について推奨される設定が指定されます。

ファイアウォールで保護されているネットワークのリストの確認

Kaspersky Endpoint Security for Windows ファイアウォールがすべてのネットワークを保護していることを確認してください。既定では、ファイアウォールは次の種別の接続でネットワークを保護します：

- **パブリックネットワーク**：アンチウイルス製品、ファイアウォール、またはフィルターは、このようなネットワーク内のデバイスを保護しません。
- **ローカルネットワーク**：このネットワーク内のデバイスは、ファイルとプリンターへのアクセスが制限されます。
- **信頼できるネットワーク**：このようなネットワーク内のデバイスは、ファイルやデータへの攻撃や不正アクセスから保護されます。

カスタムネットワークを設定している場合は、ファイアウォールがネットワークを保護していることを確認してください。このために、 Kaspersky Endpoint Security for Windows ポリシーのプロパティでネットワークのリストを確認します。このリストには、すべてのネットワークが含まれているとは限りません。

ファイアウォールの詳細は、 Kaspersky Endpoint Security for Windows のヘルプを参照してください。

ネットワークのリストを確認するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。
   選択したポリシーのプロパティウィンドウが表示されます。
3. ポリシーのプロパティで、［**アプリケーション設定**］→［**脅威対策**］→［**ファイアウォール**］の順に選択します。
4. ［**使用可能なネットワーク**］で、［**ネットワーク設定**］をクリックします。
   ［**ネットワーク接続**］ウィンドウが表示されます。このウィンドウにはネットワークのリストが表示されます。
5. リストに欠落しているネットワークがある場合は、追加します。

管理サーバーのメモリからのソフトウェアの詳細情報の除外

ネットワークデバイスで起動されたソフトウェアモジュールに関する情報を管理サーバーに保存しないことを推奨します。その結果、管理サーバーのメモリがオーバーランすることはありません。

Kaspersky Endpoint Security for Windows ポリシーのプロパティで、この情報の保存を無効にすることができます。

インストール済みのソフトウェアモジュールに関する情報の保存を無効にするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。
   選択したポリシーのプロパティウィンドウが表示されます。
3. ポリシーのプロパティで、［**アプリケーション設定**］→［**全般設定**］→［**レポートと保管領域**］の順に選択します。

4. ［**管理サーバーへのデータ転送**］セクションで、［**起動されたアプリケーションの情報**］が上位のポリシーでオンになっている場合、これをオフにします。

   このチェックボックスをオンにすると、管理サーバーデータベースに、ネットワーク接続されたデバイス上にあるすべてのバージョンのソフトウェアモジュールに関する情報が保存されます。この情報は、Kaspersky Security Center Cloud コンソールのデータベース内に大量のディスク容量を必要とする場合があります（数十ギガバイト）。

インストール済みのソフトウェアモジュールに関する情報が保存されなくなります。

重要なポリシーイベントを管理サーバーデータベースに保存する

管理サーバーデータベースのオーバーフローを回避するために、データベースには重要なイベントのみを保存することを推奨します。

管理サーバーのデータベースへの重要なイベントの記録を設定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Endpoint Security for Windows のポリシーをクリックします。

   選択したポリシーのプロパティウィンドウが表示されます。
3. ポリシーのプロパティで、［**イベントの設定**］タブを開きます。
4. ［**緊急**］セクションで、［**イベントの追加**］をクリックし、次のイベントのチェックボックスのみをオンにします：

   - *使用許諾契約書の条項に違反しています*
   - *コンピューター起動時の自動起動が無効です*
   - *アクティベーションエラー*
   - *アクティブな脅威が検知されました。高度な駆除を開始する必要があります*
   - *駆除不可*
   - *以前開いた危険なリンクを検知しました*
   - *プロセスが終了しました*
   - *ネットワーク動作がブロックされました*
   - *ネットワーク攻撃が検知されました*
   - *アプリケーションの起動が禁止されました*
   - *アクセスが拒否されました（ローカルデータベース）*
   - *アクセスが拒否されました（KSN）*
   - *ローカルのアップデートエラー*

- *2 つのタスクを同時に開始できません*
- *Kaspersky Security Center との対話中にエラーが発生しました*
- *アップデートされていないコンポーネントがあります*
- *ファイル暗号化 / 復号化ルールの適用中にエラーが発生しました*
- *ポータブルモードの有効化中にエラーが発生しました*
- *ポータブルモードの無効化中にエラーが発生しました*
- *暗号化モジュールを読み込めません*
- *ポリシーを適用できません*
- *アプリケーション機能の変更中にエラーが発生しました*

5. ［**OK**］をクリックします。
6. ［**機能エラー**］セクションで、［**イベントの追加**］をクリックし、イベント「*無効なタスク設定です。設定は適用されません。*
7. ［**OK**］をクリックします。
8. ［**警告**］セクションで、［**イベントの追加**］をクリックし、次のイベントのチェックボックスのみをオンにします：
   - *セルフディフェンスが無効です*
   - *保護コンポーネントが無効です*
   - *予備のライセンスが正しくありません*
   - *侵入者がコンピューターまたは個人データに損害を与える可能性がある正規のソフトウェアが検知されました（ローカルデータベース）*
   - *侵入者がコンピューターまたは個人データに損害を与える可能性がある正規のソフトウェアが検知されました（KSN）*
   - *オブジェクトが削除されました*
   - *オブジェクトが駆除されました*
   - *ユーザーが暗号化ポリシーを拒否しました*
   - *ファイルは管理者によって Kaspersky Anti Targeted Attack Platform サーバー上の隔離から復元されました*
   - *ファイルは管理者によって Kaspersky Anti Targeted Attack Platform サーバー上で隔離されました*
   - *アプリケーション起動禁止に関する管理者へのメッセージ*
   - *デバイスのアクセス禁止に関する管理者へのメッセージ*
   - *Web ページのアクセス禁止に関する管理者へのメッセージ*

9. ［**OK**］をクリックします。

10. ［**情報**］セクションで、［**イベントの追加**］をクリックし、次のイベントのチェックボックスのみをオンにします：

    - *オブジェクトのバックアップコピーが作成されました*
    - *アプリケーションの起動がテストモードでブロックされています*

11. ［**OK**］をクリックします。

管理サーバーデータベースへの重要なイベントの記録が設定されます。

Kaspersky Endpoint Security のグループアップデートタスクの手動セットアップ

［**タスクの開始を自動的かつランダムに遅延させる**］がオンの場合、Kaspersky Endpoint Security での最適かつ推奨されるスケジュールオプションは［**新しいアップデートがリポジトリにダウンロードされ次第**］です。

タスク

このセクションでは、Kaspersky Security Center Cloud コンソールで使用するタスクについて説明します。

タスクの概要

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

次の種別のタスクはデバイスで実行されます：

- *ローカルタスク*- 特定の 1 台のデバイスで実行されるタスク

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

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

  タスクのプロパティで特別な設定を行わない限り、グループタスクは選択したグループのすべてのサブグループに影響します。

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

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

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

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

タスクの実行結果は各デバイスの OS イベントログと管理サーバーデータベースに保存されます。

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

タスクの対象範囲

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

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

*グローバルタスク*の作成時に、次の方法を使用して対象範囲を指定できます：

- 特定のデバイスを手動で指定する

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

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

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

- デバイスの抽出を指定する。

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

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

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

タスクの作成

タスクリストでタスクを作成できます。または、［**管理対象デバイス**］リストでデバイスを選択し、選択したデバイスに割り当てられる新しいタスクを作成します。

タスクリストにタスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。表示される指示に従ってください。
3. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
4. ［**終了**］をクリックします。

   タスクが作成され、タスクリストに表示されます。

選択したデバイスに割り当てる新しいタスクを作成するには：

メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

管理対象デバイスのリストが表示されます。

1. 管理対象デバイスのリストで、デバイスの横にあるチェックボックスを選択して、そのデバイスに対してタスクを実行します。対象のデバイスを見つけるには、検索機能とフィルター機能を使用できます。
2. ［**タスクの実行**］ボタンをクリックし、［**新しいタスクを作成する**］を選択します。

   新規タスクウィザードが起動します。

   ウィザードの最初の手順で、タスク範囲に含めるように選択したデバイスを削除できます。ウィザードの指示に従ってください。
3. ［**終了**］をクリックします。

   選択したデバイスに対してタスクが作成されます。

タスクリストの表示

Kaspersky Security Center Cloud コンソールで作成されたタスクのリストを表示できます。

タスクのリストを表示するには：

メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。

タスクのリストが表示されます。タスクは、関連するアプリケーションの名前でグループ化されます。たとえば、［アプリケーションのリモートアンインストール］タスクは管理サーバーに関連しており、［脆弱性とアプリケーションのアップデートの検索］タスクはネットワークエージェントを参照します。

タスクのプロパティを表示するには：

タスクの名前をクリックします。

タスクのプロパティウィンドウにいくつかの名前付きタブが表示されます。たとえば、［**タスク種別**］は［**全般**］タブに、タスクスケジュールは［**スケジュール**］タブに表示されます。

タスクの手動での開始

タスクは、各タスクのプロパティで指定されたスケジュール設定に従って、開始されます。タスクは、タスクリストからいつでも手動で開始できます。または、［**管理対象デバイス**］リストでデバイスを選択して、既存のタスクを開始できます。

タスクを手動で開始するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. リスト内で、削除するタスクに隣接するチェックボックスをオンにします。
3. ［**開始**］をクリックします。

タスクが開始します。タスクのステータスは、［**ステータス**］列で、または［**結果**］をクリックして確認できます。

選択したデバイスでのタスクの開始

デバイスのリストで1つ以上のクライアントデバイスを選択して、それらに対して以前に作成したタスクを開始できます。これにより、特定のデバイスのセットに対して以前に作成したタスクを実行できるようになりました。

タスクが割り当てられたデバイスは、タスクの実行時に選択したデバイスのリストに変更されます。

選択したデバイスに対するタスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。管理対象デバイスのリストが表示されます。

管理対象デバイスのリストで、チェックボックスを使用して、タスクを実行するデバイスを選択します。対象のデバイスを見つけるには、検索機能とフィルター機能を使用できます。

1. ［**タスクの実行**］ボタンをクリックし、［**既存のタスクを適用する**］を選択します。

   既存のタスクのリストが表示されます。

2. 選択したデバイスがタスクリストの上に表示されます。必要に応じて、このリストからデバイスを削除できます。1つを除いてすべてのデバイスを削除できます。

3. リストから目的のタスクを選択します。リストの上にある検索ボックスを使用して、目的のタスクを名前で検索できます。選択できるタスクは1つだけです。

4. ［**保存してタスクを開始**］をクリックします。

選択したタスクは、選択したデバイスに対してすぐに開始されます。タスクのスケジュール開始設定は変更されません。

タスクの全般的な設定とプロパティ

このセクションでは、ほとんどのタスクで表示および構成できる設定について説明します。使用可能な設定のリストは、構成しているタスクによって異なります。

タスク作成時に指定する設定

タスク作成時に次の設定を指定できます。これらの設定の一部は、作成したタスクのプロパティから変更することもできます。

- タスクを割り当てるデバイス：

  - **管理グループにタスクを割り当てる**

    任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

    たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

  - **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

    タスクを特定のデバイスに割り当てます。次のいずれかの方法で、デバイスを指定します：

    - デバイスの IP アドレス、NetBIOS 名、または DNS 名を指定します。
    - IP アドレス範囲を指定します。

      特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。
    - 管理サーバーで検出された、未割り当てデバイスを含むデバイスを選択します。

      たとえば、未割り当てデバイスでネットワークエージェントのインストールタスクを実行する時に、このオプションを使用すると便利です。

  - **デバイスの抽出にタスクを割り当てる**

    デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

    たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

- アカウントの設定：
  - **既定のアカウント**

    タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。

    既定では、このオプションがオンです。

  - **アカウントの指定**

    ［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

- OS の再起動設定：
  - **再起動しない**

    操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

  - **デバイスを再起動する**

    インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

  - **ユーザーに処理を確認する**

    手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

    既定では、このオプションがオンです。

  - **通知の繰り返し間隔（分）**

    このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

    既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

    このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

  - **再起動するまでの時間（分）**

ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

既定では、このオプションはオンです。既定の間隔は 30 分です。1分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

タスク作成後に指定する設定

次の設定は、タスク作成後にのみ指定できます。

- グループタスクの設定：

  - **サブグループへ導入**

    このオプションはグループタスクの設定内でのみ使用可能です。

    このオプションをオンにすると、タスク範囲には次のものが含まれます：

    - タスクの作成中に選択した管理グループ。
    - 選択された管理グループに属する管理グループのすべてのレベルはグループ階層の下にあります。

    このオプションをオフにすると、タスク範囲にはタスクの作成中に選択された管理グループのみが含まれます。

    既定では、このオプションはオンです。

  - **セカンダリまたは仮想管理サーバーに配信**

    このオプションをオンにすると、プライマリ管理サーバーに対して有効なタスクがセカンダリ管理サーバーに対しても適用されます（仮想管理サーバーも含まれます）。同じ種別のタスクがセカンダリ管理サーバーに既に存在する場合は、既存のタスクとプライマリ管理サーバーから継承した両方のタスクがセカンダリ管理サーバーに適用されます。

    このオプションは［**サブグループへ導入**］がオンになっている場合にのみ使用可能です。

    既定では、このオプションはオフです。

- タスクスケジュールの設定：

- **実行予定設定：**
  - **手動**

    タスクは、自動的には実行されません。手動でのみ開始できます。

    既定では、このオプションはオンです。

  - **N 分ごと**

    タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。

    既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

  - **N 時間ごと**

    指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。

    既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

  - **N 日ごと**

    日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

    既定では、現在のシステム日時から、1 日ごとにタスクが実行されます。

  - **N 週間ごと**

    指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

    既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

  - **毎日（サマータイムはサポートしていません）**

    日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を 1 時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

    このスケジュールの使用は推奨されません。Kaspersky Security Center Cloud コンソールの古いバージョンとの後方互換性を維持するために用意されているオプションとなります。

    既定では、毎日、現在のシステム時刻にタスクが実行されます。

  - **毎週**

    毎週、指定した曜日の指定した時刻にタスクを実行します。

  - **曜日ごと**

指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。
既定では、毎週金曜日の午後 6 時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。
  指定した日付が存在しない月には、月の最終日にタスクを実行します。
  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。
  既定では、月内のいかなる日付も選択されておらず、開始時刻は午後 6 時です。

- **新しいアップデートがリポジトリにダウンロードされ次第**

  新しいアップデートがディストリビューションポイントのリポジトリにダウンロードされると、Kaspersky Security Center Cloud コンソールがこのスケジュールのタスクをすべて実行します。ネットワークエージェントは、管理対象デバイスと管理サーバー間の定期的な同期時に、アップデートを使用できるかどうかを確認します（ハートビート）。

  たとえば、Kaspersky Endpoint Security などのセキュリティ製品に関連するアップデートタスクで、このスケジュールを使用できます。

  管理対象デバイスのネットワークエージェントで新しいアップデートを 25 時間以上検出できなかった場合、Kaspersky Security Center Cloud コンソールは、このデバイスでこのスケジュールのタスクをすべて実行します。これらのタスクは、新しいアップデートが検出されるまで毎時実行されます。管理対象デバイスと、リポジトリにアップデートをダウンロードするディストリビューションポイントが接続されていない場合も、Kaspersky Security Center Cloud コンソールはこれらのタスクを毎時実行します。

- **ウイルスアウトブレイク検知次第**

  ［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

  - ワークステーションとファイルサーバー向けアンチウイルス製品
  - 境界防御向けアンチウイルス製品
  - メールサーバー向けアンチウイルス製品

  既定では、すべてのアプリケーション種別がオンです。

  ウイルスアウトブレイクを検知したアンチウイルス製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。現在のタスクを実行する条件として、先に実行されるタスクの実行結果（「正常終了」または「エラー終了」）を選択できます。これにより、たとえば［**デバイスの電源をオンにする**］を選択して［*デバイスの管理*］タスクを実行し、その完了後に［*ウイルススキャン*］タスクを実行できます。このパラメータは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。

- **未実行のタスクを実行する**

  このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

  このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

  このオプションをオフにすると、スケジュール設定されたタスクだけがクライアントデバイス上で開始され、［**手動**］、［**1回**］、および［**即時**］に設定したタスクはネットワーク上で可視になっているクライアントデバイスでのみ開始されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

  既定では、このオプションはオンです。

- **タスクの開始を自動的かつランダムに遅延させる**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる（分）**

  このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

  このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

  既定では、このオプションはオフです。既定の時間は1分です。

- **Wake on LAN の機能を使用してタスク開始前にデバイスを起動する（分）**

タスク開始よりも指定した時間だけ前に、デバイス上のオペレーティングシステムが起動します。既定では、時間は 5 分です。

タスクの開始予定時刻が近づいても電源がオフだったデバイスも含めて、タスク範囲に含まれるすべてのクライアントデバイスでタスクを実行するには、このオプションをオンにします。

タスクの完了後にデバイスの電源を自動的にオフにする場合は、［**タスク完了後にデバイスをシャットダウンする**］を有効にします。このオプションは同じウィンドウ内にあります。

既定では、このオプションはオフです。

- **タスク完了後にデバイスをシャットダウンする**

  たとえば、毎週金曜日の業務時間終了後にクライアントデバイスへのアップデートのインストールを行い、その後デバイスの電源を切りたい時に、アップデートインストールタスクでこのオプションを使用できます。

  既定では、このオプションはオフです。

- **次の時間を超える場合はタスクを停止する（分）**

  指定した時間が経過すると、タスクが完了したかどうかに関係なくタスクが自動的に停止します。
  実行に時間がかかり過ぎているタスクを中断したい時に、このオプションを使用します。
  既定では、このオプションはオフです。既定のタスク実行時間は 120 分です。

- 通知：
  - ［**タスク履歴の保存**］セクション：
    - **すべてのイベントを保存**
    - **タスクの進捗に関連したイベントを保存**
    - **タスク実行結果のみ保存**
    - **管理サーバーのデータベースに保存（日）**

      タスク範囲に含まれるすべてのクライアントデバイスでのタスク実行に関するアプリケーションイベントが、指定した日数の間、管理サーバーに保存されます。この期間が過ぎると、情報が管理サーバーから削除されます。

      既定では、このオプションはオンです。

    - **デバイスの OS イベントログに保存**

      タスク実行に関するアプリケーションイベントが、各クライアントデバイスの Windows イベントログにローカルで保存されます。

      既定では、このオプションはオフです。

  - **エラーのみ通知**

- **メールで通知**

- タスク範囲の設定

- **範囲からの除外**

  タスクを適用しないデバイスのグループを指定できます。タスク範囲から除外できるのは、タスクが適用されない管理グループのサブグループのみです。

- **変更履歴**

タスクのエクスポート

Kaspersky Security Center Cloud コンソールを使用すると、タスクとその設定を KLT ファイルに保存できます。この KLT ファイルを使用して、Kaspersky Security Center Windows と Kaspersky Security Center Linux の両方に保存したタスクをインポートできます。

タスクをエクスポートするには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. エクスポートするタスクの横のチェックボックスをオンにします。

   複数のタスクを同時にエクスポートすることはできません。複数のタスクを選択すると、［**エクスポート**］が無効になります。管理サーバーのタスクもエクスポートできません。
3. ［**エクスポート**］をクリックします。
4. 表示される［**名前を付けて保存**］ウィンドウで、タスクファイルの名前とパスを指定します。［**保存**］をクリックします。

   ［**名前を付けて保存**］ウィンドウは、Google Chrome、Microsoft Edge、または Opera を使用している場合にのみ表示されます。別のブラウザーを使用する場合、タスクファイルは自動的に［**Downloads**］フォルダーに保存されます。

タスクのインポート

Kaspersky Security Center Cloud コンソールを使用すると、KLT ファイルからタスクをインポートできます。KLT ファイルには、エクスポートされたタスクとその設定が含まれています。

タスクをインポートするには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**インポート**］をクリックします。
3. ［**参照**］をクリックして、インポートするタスクファイルを選択します。
4. 開いたウィンドウで、KLT タスクファイルへのパスを指定して、［**開く**］をクリックします。選択できるタスクファイルは 1 つだけです。

   タスクの処理が始まります。

5. タスクが正常に処理されたら、タスクを割り当てるデバイスを選択します。これには、次のいずれかのオプションを選択します：

- **管理グループにタスクを割り当てる**

  任意の管理グループに属するデバイスにタスクを割り当てます。既存のグループを指定するか、新規グループを作成できます。

  たとえば、特定の管理グループに含まれるデバイスのみが対象のメッセージをユーザーに送信する時に、このオプションを使用すると便利です。

- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**

  タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

  特定のサブネットワークでタスクを実行する時に、このオプションを使用すると便利です。たとえば、経理担当者のデバイスにのみ特定のアプリケーションをインストールしたり、感染した可能性のあるサブネットワークでデバイスをスキャンする場合などです。

- **デバイスの抽出にタスクを割り当てる**

  デバイスの抽出に属するデバイスにタスクを割り当てます。既存の抽出のいずれかを選択できます。

  たとえば、特定のバージョンのオペレーティングシステムを使用しているデバイスを対象にタスクを実行する時に、このオプションを使用すると便利です。

6. タスク範囲を指定します。

7. ［**完了**］をクリックしてタスクのインポートを完了します。

インポート結果の通知が表示されます。タスクが正常にインポートされた場合は、［**詳細**］をクリックして、タスクのプロパティを表示できます。

インポートが成功すると、タスクがタスクリストに表示されます。タスクの設定とスケジュールもインポートされます。タスクはスケジュールに従って開始されます。

新しくインポートされたタスクと同じ名前のタスクが既に存在している場合、インポートされたタスクの名前に、たとえば **(1)**、**(2)** のようなインデックス「**(<次の連番>)**」が付きます。

クライアントデバイスの管理

このセクションでは、管理グループ内のデバイスを管理する方法について説明します。

管理対象デバイスの設定

管理対象デバイスの設定を表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

管理対象デバイスのリストが表示されます。

2. 管理対象デバイスのリストで、目的のデバイス名のリンクをクリックします。

選択したデバイスのプロパティウィンドウが表示されます。

次のタブは、設定の主なグループを表すプロパティ ウィンドウの上部に表示されます。

- **全般**

このタブは次のセクションで構成されています。

- ［**全般**］セクションには、クライアントデバイスに関する全般的な情報が表示されます。情報は、クライアントデバイスと管理サーバーとの前回の同期中に受信されたデータに基づいて提供されます：

  - **名前**

    このフィールドでは、管理グループ内のクライアントデバイスの名前を表示したり変更したりできます。

  - **説明**

    このフィールドでは、クライアントデバイスの補足的な説明を入力できます。

  - **デバイスのステータス**

    管理者によって定義された基準に基づいて、デバイス上のアンチウイルスによる保護のステータスとデバイスのネットワーク動作に対して割り当てられたクライアントデバイスのステータス。

  - **デバイスの所有者**

    デバイス所有者の名前。［**デバイスの所有者の管理**］をクリックすることにより、ユーザーをデバイスの所有者として割り当てたり削除したりすることができます。

  - **グループの完全名**

    クライアントデバイスが属する管理グループ。

  - **前回の定義データベースのアップデート**

    定義データベースまたはアプリケーションをデバイス上で前回アップデートした日付。

  - **管理サーバーへの接続**

    クライアントデバイスにインストールされたネットワークエージェントが管理サーバーに最後に接続した日時。

  - **前回の可視**

    デバイスが前回ネットワークで検出された日時。

  - **ネットワークエージェントのバージョン**

    インストールされているネットワークエージェントのバージョン。

- **作成**

  Kaspersky Security Center Cloud コンソール内でデバイスが作成された日付。

- **管理サーバーから切断しない**

  このオプションをオンにすると、管理対象デバイスと管理サーバー間の継続的な接続が維持されます。このオプションは、継続的な接続を提供するプッシュサーバーを使用していない場合に使用することがあります。

  このオプションがオフで、プッシュサーバーが使用されていない場合、管理対象デバイスは、データの同期または情報の送信のためにのみ管理サーバーに接続します。

  ［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

  このオプションは、管理対象デバイスでは既定でオフになっています。このオプションは、管理サーバーがインストールされているデバイスでは既定でオンになっており、オフにしようとしてもオンのままになります。

- ［**ネットワーク**］セクションには、クライアントデバイスのネットワークプロパティに関する次の情報が表示されます：

  - **IP アドレス**

    デバイスの IP アドレス。

  - **Windows ドメイン**

    このデバイスを含む Windows ドメインまたはワークグループ。

  - **DNS 名**

    クライアントデバイスの DNS ドメイン名。

  - **NetBIOS 名**

    クライアントデバイスの Windows ネットワークでの名前。

  - **IPv6 アドレス**

- ［**システム**］セクションには、クライアントデバイスにインストールされているオペレーティングシステムに関する情報が表示されます。

  - **オペレーティングシステム**
  - **CPU アーキテクチャ**
  - **OS 製造元**
  - **OS フォルダー**
  - **デバイス名**

- **仮想マシンの種別**

  仮想マシンの製造元。

- **動的仮想マシン (VDI の一部)**

  この行には、クライアントデバイスが VDI の一部である動的仮想マシンかどうかが表示されます。

- **OS のビルド**

- ［**プロテクション**］セクションには、次のようなクライアントデバイスにおけるアンチウイルスによる保護に関する現在のステータスが表示されます：

  - **可視**

    クライアントデバイスの可視性のステータス。

  - **デバイスのステータス**

    管理者によって定義された基準に基づいて、デバイス上のアンチウイルスによる保護のステータスとデバイスのネットワーク動作に対して割り当てられたクライアントデバイスのステータス。

  - **ステータスの説明**

    クライアントデバイスの保護と管理サーバーへの接続のステータス。

  - **保護ステータス**

    クライアントデバイスのリアルタイム保護に関する現在のステータスが表示されます。

    デバイスのステータスに変更があると、新しいステータスは、クライアントデバイスと管理サーバーが同期された後にのみデバイスのプロパティウィンドウに表示されます。

  - **前回の完全スキャン**

    クライアントデバイスで前回のマルウェアスキャンが実行された日時。

  - **ウイルスが検知されました**

    アンチウイルス製品のインストール後（最初のスキャンの場合）またはウイルスカウンターを前回リセットした後に、クライアントデバイスで検知された脅威の合計数。

  - **駆除できていないオブジェクト**

    クライアントデバイスにおける未処理ファイルの数。

    このフィールドは、モバイルデバイス上の未処理ファイルの数をスキップします。

- **ディスク暗号化ステータス**

  デバイスのローカルドライブでのファイル暗号化の現在のステータス。ステータスの説明は、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

- ［**製品が定義したデバイスのステータス**］セクションには、デバイスにインストールされている管理対象アプリケーションによって定義されたデバイスのステータスに関する情報が表示されます。このデバイスのステータスは、Kaspersky Security Center Cloud コンソールによって定義されたものとは異なる場合があります。

- **アプリケーション**

  このタブには、クライアントデバイスにインストールされているすべてのカスペルスキー製品のリストが表示されます。アプリケーション名をクリックすると、アプリケーションに関する一般情報、デバイスで発生したイベントのリスト、およびアプリケーション設定が表示されます。

- **アクティブなポリシーとポリシーのプロファイル**

  このタブには、管理対象デバイスで現在アクティブなポリシーとポリシープロファイルが一覧表示されます。

- **タスク**

  ［**タスク**］タブでは、既存タスクのリストの表示、新規タスクの作成、タスクの削除、タスクの開始と停止、タスク設定の変更、実行結果の表示など、クライアントデバイスのタスクを管理できます。タスクのリストは、管理サーバーとの前回のクライアント同期セッション中に受信されたデータに基づいて提供されます。管理サーバーは、タスクステータスに関する情報をクライアントデバイスに要求します。接続に失敗すると、ステータスは表示されません。

- **イベント**

  ［**イベント**］タブでは、選択したクライアントデバイスについて管理サーバーに記録されたイベントが表示されます。

- **セキュリティ問題**

  ［**セキュリティ問題**］タブでは、クライアントデバイスでのセキュリティ問題を表示、編集、作成できます。セキュリティ問題は、クライアントデバイスにインストールしたカスペルスキー製品によって自動で作成されるか、管理者が手動で作成します。たとえば、定期的にマルウェアを自分のリムーバブルドライブからデバイスに移しているユーザーがいた場合、管理者はこの件のセキュリティ問題を作成できます。管理者はセキュリティ問題のテキストに、概要説明と推奨される処分（ユーザーに下す懲戒処分など）を記載したり、ユーザーへのリンクを追加することもできます。

  必要な処分がすべて行われたセキュリティ問題は、*処理済み*と呼ばれます。未処理のセキュリティ問題がある場合、デバイスのステータスを*緊急*または*警告*に変更する条件として選択できます。

  このセクションには、デバイス用に作成したセキュリティ問題のリストがあります。セキュリティ問題は、重要度と種別で分類されます。セキュリティ問題のタイプは、セキュリティ問題を作成するカスペルスキー製品によって定義されます。［**処理済み**］列のチェックボックスをオンにすると、リストにある処理済みのセキュリティ問題を強調表示できます。

- **タグ**

［**タグ**］タブでは、クライアントデバイスの検索に使用されるキーワードのリストを管理できます。また、既存のタグのリストの表示、リストからのタグの割り当て、自動タグ付けルールの設定、新規タグの追加、既存のタグの名称変更、タグの削除なども可能です。

- **詳細**

このタブは次のセクションで構成されています。

- **アプリケーションレジストリ**。このセクションでは、クライアントデバイス上にインストールされたアプリケーションのレジストリとそのアップデートを表示し、アプリケーションレジストリの表示を設定することができます。

  インストール済みアプリケーションの情報は、クライアントデバイスにインストールされているネットワークエージェントから必要な情報が管理サーバーに送信されている場合に供給されます。管理サーバーへの情報の送信は、ネットワークエージェントまたはそのポリシーのプロパティウィンドウにある［**リポジトリ**］セクションで設定できます。

  アプリケーション名をクリックすると、アプリケーションの詳細とアプリケーションにインストールされているアップデートパッケージのリストを表示するウィンドウが開きます。

- **実行ファイル**。このセクションには、クライアントデバイスにある実行ファイルが表示されます。

- **ディストリビューションポイント**。このセクションでは、デバイスがインタラクトするディストリビューションポイントのリストについて説明します。

  - **ファイルへのエクスポート**

    ［**ファイルへのエクスポート**］をクリックすると、デバイスがインタラクトするディストリビューションポイントのリストがファイルに保存されます。既定では、デバイスのリストは CSV ファイルにエクスポートされます。

  - **プロパティ**

    ［**プロパティ**］をクリックすると、デバイスがインタラクトするディストリビューションポイントが表示および設定されます。

- **ハードウェアレジストリ**。このセクションでは、クライアントデバイスにインストールされているハードウェアに関する情報を表示できます。

- **適用可能なアップデート**。このセクションには、デバイスで検出されたがインストールされていないソフトウェアアップデートのリストが表示されます。

- **ソフトウェアの脆弱性**。このセクションには、クライアントデバイスにインストールされているサードパーティのソフトウェアの脆弱性に関する情報が表示されます。

  脆弱性をファイルに保存するには、保存する脆弱性に隣接するチェックボックスをオンにして、［**CSV へエクスポート**］または［**TXT へエクスポート**］をクリックします。

  このセクションには、次の設定項目があります：

  - **修正可能な脆弱性のみ表示**

    このオプションを有効にすると、パッチを使用して修正できる脆弱性が表示されます。

    このオプションをオフにすると、パッチを使用して修正できる脆弱性と、パッチがリリースされていない脆弱性の両方が表示されます。

    既定では、このオプションはオンです。

  - **脆弱性のプロパティ**

リストにあるソフトウェアの脆弱性の名前をクリックすると、選択したソフトウェアの脆弱性のプロパティが別のウィンドウに表示されます。ウィンドウで次の操作を実行できます：

- 対象の管理対象デバイスではこのソフトウェア脆弱性を無視するようにする（管理コンソールまたは Kaspersky Security Center Cloud コンソールで操作）。
- 脆弱性に対して推奨される修正のリストを表示する。
- 脆弱性を修正するソフトウェアアップデートを手動で指定する（管理コンソールまたは Kaspersky Security Center Cloud コンソール）。
- 脆弱性の該当数を表示する。
- 脆弱性を修正するための既存のタスクのリストを表示したり、脆弱性を修正するためのタスクを新規作成する。

- **リモート診断**。このセクションでは、クライアントデバイスのリモート診断を実行できます。

デバイスの抽出

*デバイスの抽出*は、特定の条件を指定してデバイスをフィルタリングできる機能です。デバイスの抽出を使用して、複数のデバイスを管理できます。たとえば、デバイスの抽出に含まれるデバイスのみを対象とするレポートを表示したり、デバイスの抽出に含まれるデバイスすべてを別のグループに移動したりできます。

Kaspersky Security Center Cloud コンソールでは、様々な*定義済みの抽出*（例：［**「緊急」ステータスのデバイス**］、［**プロテクションが無効です**］、［**アクティブな脅威を検知しました**］）を使用できます。定義済みの抽出は削除できません。*ユーザー定義の抽出*を追加で作成し設定できます。

ユーザー定義の抽出では、抽出範囲を「すべてのデバイス」「管理対象デバイス」「未割り当てデバイス」から選択できます。抽出条件のパラメータを指定できます。デバイスの抽出では、異なるパラメータを指定した複数の抽出条件を作成できます。たとえば、2 つの条件を作成し、それぞれに異なる IP アドレス範囲を指定できます。複数の条件を指定した場合、デバイスの抽出はいずれかの条件に 1 つでも一致するデバイスを表示します。これに対して、1 つの条件内で複数のパラメータが指定されている場合、すべてのパラメータを満たすことが求められます。たとえば、1 つの条件内で IP アドレス範囲とインストールされている製品名の両方が指定されている場合、該当する製品がインストールされていてなおかつ IP アドレスが指定した範囲内のデバイスのみが表示されます。

デバイスの抽出からデバイスリストを表示

Kaspersky Security Center Cloud コンソール、デバイスの抽出からデバイスのリストを表示できます。

デバイスの抽出からデバイスリストを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**デバイスの抽出**］、または［**検出と製品の導入**］→［**デバイスの抽出**］セクションの順に選択します。
2. 抽出リストで、デバイスの抽出の名前をクリックします。
   このページには、デバイスの抽出に含まれるデバイス関連情報のテーブルが表示されます。

3. デバイステーブルのデータは、次のようにしてグループ化およびフィルタリングできます：

   - 設定アイコン（ ）をクリックし、テーブルに表示する列を選択します。
   - フィルターアイコン（ ）をクリックしてから、呼び出したメニューでフィルター条件を指定して適用します。
     デバイスをフィルタリングしたテーブルが表示されます。

デバイスの抽出で1つまたは複数のデバイスを選択し、［**新規タスク**］をクリックして、これらのデバイスに適用されるタスクを作成できます。

デバイスの抽出で選択したデバイスを別の管理グループに移動するには、［**グループへ移動**］をクリックし、ターゲットの管理グループを選択します。

デバイスの抽出の作成

デバイスの抽出を作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**デバイスの抽出**］の順に移動します。
   デバイスの抽出のリストが表示されます。
2. ［**追加**］をクリックします。
   ［**デバイスの抽出の設定**］ウィンドウが表示されます。
3. 新しい抽出の名前を入力します。
4. デバイスの抽出に含めるデバイスを含むグループを指定します：

   - ［**デバイスの検索**］- 選択基準を満たし、［**管理対象デバイス**］または［**未割り当てデバイス**］グループに含まれるデバイスを検索します。
   - ［**管理対象デバイスの検索**］- 選択基準を満たし、［**管理対象デバイス**］グループに含まれるデバイスを検索します。
   - ［**未割り当てデバイスの検索**］- 選択基準を満たし、［**未割り当てデバイス**］グループに含まれるデバイスを検索します。

   ［**セカンダリ管理サーバーのデータを含める**］を有効にして、選択基準を満たし、セカンダリ管理サーバーによって管理されているデバイスを検索できるようにします。
5. ［**追加**］をクリックします。
6. 表示されたウィンドウで、この抽出に含めるデバイスが満たす必要のある条件を指定し、［**OK**］をクリックします。
7. ［**保存**］をクリックします。

デバイスの抽出が作成され、リストに追加されます。

デバイスの抽出の設定

デバイスの抽出を設定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**デバイスの抽出**］の順に移動します。
   デバイスの抽出のリストが表示されます。
2. 関連するユーザー定義のデバイス抽出を選択し、［**プロパティ**］をクリックします。
   ［**デバイスの抽出の設定**］ウィンドウが表示されます。
3. ［**全般**］タブで、［**新規の条件**］をクリックします。
4. この抽出に含めるデバイスが満たす必要のある条件を指定します。
5. ［**保存**］をクリックします。

   設定が適用され保存されます。

以下に、デバイスを抽出に割り当てる条件について説明します。条件は論理演算子「OR」を使用して結合されます。抽出には、少なくとも1つの条件を満たすデバイスが含まれます。

全般

［**全般**］セクションでは、抽出条件の名前を変更したり、条件を反転させたりすることができます：

抽出の条件を反転させる

このオプションをオンにすると、指定した抽出条件の選択状態が反転します。指定した条件に合致しないすべてのデバイスが、抽出に含まれるようになります。

既定では、このオプションはオフです。

ネットワークインフラストラクチャ

［**ネットワーク**］サブセクションでは、ネットワークデータを基にデバイスを抽出に含める場合に使用する基準を指定できます：

- **デバイス名**

  デバイスの Windows ネットワーク名（NetBIOS 名）、あるいは IPv4 アドレスまたは IPv6 アドレス。

- **ドメイン**

  指定した Windows ドメインに含まれるデバイスをすべて表示します。

- **管理グループ**

  指定した管理グループに含まれるデバイスを表示します。

- **説明**

デバイスのプロパティウィンドウ（［**全般**］セクションの［**説明**］）のテキスト。
［**説明**］で検索に使用する表現として、次の文字を使用できます：

- 1つの単語：
  - ***** -文字数不定の任意の文字列を表します。

    例：

    Server または **Server's** などの単語を記述するには、**Server*** と入力します。
  - **?** -任意の1文字を表します。

    例：

    Window または **Windows** などの単語を記述するには、**Windo?** と入力します。
    アスタリスク（*****）または疑問符（**?**）は、クエリの先頭文字としては使用できません。
- 複数の単語による検索：
  - スペース -指定した単語のいずれかがコメントに含まれているデバイスがすべて表示されます。

    例：

    Secondary または **Virtual** という単語が含まれている語句を検索する場合は、クエリに **Secondary Virtual** と入力します。
  - **+** -単語の前にプラス記号を付けると、すべての検索結果にその単語が含まれます。

    例：

    Secondary と **Virtual** の両方が含まれた語句を検索するには、クエリに **+Secondary+Virtual** と入力します。
  - **-** -単語の前にマイナス記号を付けると、すべての検索結果にその単語が含まれません。

    例：

    Secondary が含まれ、**Virtual** が含まれない語句を検索するには、クエリに **+Secondary-Virtual** と入力します。
  - **"<任意のテキスト>"** -引用符で囲まれたテキストを含むテキストが検索されます。

    例：

    Secondary Server という語句を検索する場合は、クエリに **"Secondary Server"** と入力します。

- **IP アドレス範囲**

  このオプションをオンにすると、検索されるデバイスが属する IP アドレス範囲の最初と最後の IP アドレスを入力できます。
  既定では、このオプションはオフです。

- **別の管理サーバーの管理対象**

次のいずれかの値を選択します：

- **はい**：デバイス移動ルールは、他の管理サーバーによって管理されているクライアントデバイスにのみ適用されます。これらのサーバーは、デバイス移動ルールを設定するサーバーとは異なります。
- ［**いいえ**］。デバイス移動ルールは、現在の管理サーバーによって管理されているクライアントデバイスにのみ適用されます。
- **値を選択しない**：条件は当てはまりません。

［**Active Directory**］サブセクションでは、Active Directory データを基にデバイスを抽出に含めるための基準を設定できます：

- **デバイスが配置されている Active Directory 組織単位**

  このオプションをオンにすると、抽出には、入力フィールドで指定した Active Directory 組織単位のデバイスが含まれます。

  既定では、このオプションはオフです。

- **子組織単位を含める**

  このオプションをオンにすると、抽出には、指定した Active Directory 組織単位のすべての子組織単位（OU)のデバイスが含まれます。

  既定では、このオプションはオフです。

- **デバイスが属している Active Directory グループ**

  このオプションを有効にすると、抽出には、入力フィールドで指定した Active Directory グループのデバイスが含まれます。

  既定では、このオプションはオフです。

［**ネットワーク活動**］サブセクションでは、ネットワークアクティビティを基にデバイスを抽出に含める場合に使用する基準を指定できます：

- **ディストリビューションポイントとして動作**

  検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：

  - **はい**：ディストリビューションポイントとして動作するデバイスが抽出に含まれます。
  - ［**いいえ**］。ディストリビューションポイントとして機能するデバイスが抽出に含まれません。
  - **値を選択しない**：基準は適用されません。

- **管理サーバーから切断しない**

検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：

- **有効**：［**管理サーバーから切断しない**］をオンにしたデバイスが抽出に含まれます。
- **無効**：［**管理サーバーから切断しない**］をオフにしたデバイスが抽出に含まれます。
- **値を選択しない**：基準は適用されません。

- **接続プロファイルが切り替えられました**

検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：

- **はい**：接続プロファイルを切り替えた結果として管理サーバーに接続されたデバイスが抽出に含まれます。
- ［**いいえ**］。接続プロファイルを切り替えた結果として管理サーバーに接続されたデバイスが抽出に含まれません。
- **値を選択しない**：基準は適用されません。

- **前回の管理サーバーへの接続**

このチェックボックスを使用して、管理サーバーに前回接続した日時によるデバイスの検索の基準を設定できます。

このチェックボックスをオンにすると、入力フィールドで、クライアントデバイスにインストールされたネットワークエージェントと管理サーバーとの間に前回接続が確立された日時の範囲を指定できます。指定された間隔内のデバイスが抽出に含まれます。

このチェックボックスをオフにすると、この基準は適用されません。

既定では、このチェックボックスはオフです。

- **ネットワークポーリングで検出された新規デバイス**

過去数日間のネットワークポーリングで検出された新規デバイスを検索します。

このオプションをオンにすると、［**検出期間（日）**］フィールドで指定した期間中のデバイスの検索で検出された新規デバイスのみが、抽出に含まれます。

このオプションをオフにすると、デバイスの検索で検出された新規デバイスがすべて抽出に含まれます。

既定では、このオプションはオフです。

- **デバイスが可視**

検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます：

- **はい**：ネットワークで現在可視のデバイスを抽出に含めます。
- ［**いいえ**］。ネットワークで現在不可視のデバイスを抽出に含めます。
- **値を選択しない**：基準は適用されません。

［**クラウドセグメント**］サブセクションでは、それぞれのクラウドセグメントを基にデバイスを抽出に含めるための基準を設定できます：

- **デバイスがクラウドセグメント内にある**

  このオプションをオンにすると、AWS、Azure、Google クラウドセグメントからデバイスを選択できます。

  ［**子オブジェクトも含む**］オプションも有効にする場合は、選択したセグメントのすべての子オブジェクトに対して検索が実行されます。

  検索結果には、指定したセグメントのデバイスしか含まれません。

- **API を使用して検出されたデバイス**

  ドロップダウンリストで、API ツールによりデバイスが検出されるかどうかを選択できます：

  - **はい**：デバイスは、AWS、Azure、または Google API を使用して検出されます。
  - ［**いいえ**］。AWS、Azure、または Google API を使用してデバイスを検出できません。つまり、クラウド環境の外にあるか、クラウド環境内にあるデバイスは API で検出できません。
  - 値なし：この条件は当てはまりません。

デバイスのステータス

［**管理対象デバイスのステータス**］サブセクションでは、管理対象アプリケーションからのデバイスのステータスの説明を基にデバイスを抽出に含めるための基準を設定できます：

- **デバイスのステータス**

  ドロップダウンリストからデバイスのステータス（「*OK*」「*緊急*」「警告」）を選択します。

- **リアルタイム保護のステータス**

  リアルタイム保護のステータスを選択できるドロップダウンリスト。指定されたリアルタイム保護ステータスのデバイスが抽出に含まれます。

- **デバイスステータスの説明**

  このフィールドで、「*OK*」「*緊急*」「*警告*」のいずれかのステータスをデバイスに割り当てる条件に対応するチェックボックスをオンにできます。

［**管理対象アプリケーションのコンポーネントのステータス**］サブセクションでは、管理対象アプリケーションのコンポーネントのステータスを基にデバイスを抽出に含めるための基準を設定できます：

- **データ漏洩対策のステータス**

  データ漏洩対策のステータス（*デバイスからのデータなし*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **コラボレーションサーバーの保護ステータス**

サーバーコラボレーションの保護ステータス（*デバイスからのデータなし*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **メールサーバーの保護ステータス**

  メールサーバーの保護のステータス（*デバイスからのデータなし*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

- **Endpoint Sensor ステータス**

  Endpoint Sensor のステータス（*デバイスからのデータなし*、*停止*、*開始中*、*一時停止*、*実行中*、*失敗*）を基にデバイスを検索します。

［**管理対象アプリケーションのステータスに影響がある問題**］サブセクションでは、管理対象アプリケーションで検知される可能性のある問題のリストを基にデバイスを抽出に含めるために使用する基準を設定できます：選択した問題のうち1つ以上の問題が存在するデバイスが抽出に含まれます複数のアプリケーションを対象とする問題については、同じ問題をすべてのアプリケーションのリストで自動的に選択するオプションがあります。

管理対象アプリケーションからのステータスの説明に対応するチェックボックスをオンにできます。これらのステータスが受信されると、デバイスが抽出に含まれます。複数のアプリケーションを対象とするステータスについては、同じステータスをすべてのアプリケーションのリストで自動的に選択するオプションがあります。

システムの詳細

［**オペレーティングシステム**］セクションでは、オペレーティングシステム種別を基にデバイスを抽出に含める場合に使用する基準を指定できます。

- **プラットフォームの種別**

  このチェックボックスをオンにすると、オペレーティングシステムをリストから選択できます。指定したオペレーティングシステムがインストールされたデバイスが検索結果に含まれます。

- **OS サービスパックのバージョン**

  このフィールドでは、オペレーティングシステムのパッケージバージョンを「*X.Y*」形式で指定できます。これによって、デバイスに対する移動ルールの適用方法が決定されます。既定では、バージョンの値は指定されていません。

- **OS のビット数**

  ドロップダウンリストで、オペレーティングシステムのアーキテクチャを選択できます。これによって、デバイスに対する移動ルールの適用方法が決定されます（［**不明**］、［**x86**］、［**AMD64**］、［**IA64**］）。既定では、リストでオプションが選択されていないため、オペレーティングシステムのアーキテクチャは定義されていません。

- **OS のビルド**

この設定は Windows オペレーティングシステムにのみ適用できます。

オペレーティングシステムのビルド番号です。選択したオペレーティングシステムのビルド番号が、入力したビルド番号と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したビルド番号を除くすべてのビルド番号を検索するようにも設定できます。

- **OS のリリース番号**

この設定は Windows オペレーティングシステムにのみ適用できます。

オペレーティングシステムのリリース ID です。選択したオペレーティングシステムのリリース ID が、入力したリリース ID と「等しい」「それより古い」「それより新しい」かを指定して検索できます。また、指定したリリース ID を除くすべてのリリース ID を検索するようにも設定できます。

［**仮想マシン**］セクションでは、仮想マシンであるか仮想デスクトップインフラストラクチャ（VDI）の一部であるかによってデバイスを抽出に含めるための基準を設定できます：

- **仮想マシン**

このドロップダウンリストで、次のオプションを選択できます：

- **未定義**。
- ［**いいえ**］。仮想マシンでないデバイスを検索します。
- **はい**：仮想マシンであるデバイスを検索します。

- **仮想マシンの種別**

このドロップダウンリストで、仮想マシンの製造元を選択できます。

このドロップダウンリストは、［**仮想マシン**］の値が［**はい**］または［**判断しない**］である場合に使用できます。

- **仮想デスクトップインフラストラクチャの一部**

このドロップダウンリストで、次のオプションを選択できます：

- **未定義**。
- ［**いいえ**］。仮想デスクトップインフラストラクチャの一部でないデバイスを検索します。
- **はい**：仮想デスクトップインフラストラクチャ（VDI）の一部であるデバイスを検索します。

［**ハードウェアレジストリ**］サブセクションでは、取り付けたハードウェアを基にデバイスを抽出に含めるための基準を設定できます：

ハードウェアの詳細を取得する Linux デバイスに lshw ユーティリティがインストールされていることを確認してください。使用されているハイパーバイザーによっては、仮想マシンから取得されたハードウェアの詳細が不完全である場合があります。

- **デバイス**

  このドロップダウンリストでは、装置の種別を選択できます。その装置を備えたすべてのデバイスが検索結果に含まれます。

  このフィールドでは全文検索が可能です。

- **製造元**

  このドロップダウンリストで、装置の製造元の名前を選択できます。その装置を備えたすべてのデバイスが検索結果に含まれます。

  このフィールドでは全文検索が可能です。

- **デバイス名**

  デバイスの Windows ネットワークでの名前。指定された名前のデバイスが抽出に含まれます。

- **説明**

  デバイスまたはハードウェア装置の説明。このフィールドで指定された説明が付けられたデバイスが抽出に含まれます。

  デバイスの説明は、そのデバイスのプロパティウィンドウにあらゆる形式で入力できます。このフィールドでは全文検索が可能です。

- **デバイスの製造元**

  デバイスの製造元の名前。このフィールドで指定された製造元のデバイスが抽出に含まれます。

  コンピューターの製造元名は、デバイスのプロパティウィンドウで入力できます。

- **シリアル番号**

  このフィールドで指定されたシリアル番号が付けられたすべてのハードウェアユニットが抽出に含まれます。

- **インベントリ番号**

  このフィールドで指定されたインベントリ番号が付けられた機器が抽出に含まれます。

- **ユーザー**

  このフィールドで指定されたユーザーのすべてのハードウェアユニットが抽出に含まれます。

- **場所**

デバイスまたはハードウェアユニットの場所（本社、支社など）。このフィールドで指定された場所に導入されるコンピューターまたはその他のデバイスが抽出に含まれます。

デバイスの場所は、そのデバイスのプロパティウィンドウにおいて、あらゆる形式で記載できます。

- **CPU クロック周波数（MHz）（最小）**

  CPU の最小クロック周波数。入力フィールドで指定されたクロック周波数範囲と一致する CPU を搭載したデバイスが抽出に含まれます。

- **CPU クロック周波数（MHz）（最大）**

  CPU の最大クロック周波数。入力フィールドで指定されたクロック周波数範囲と一致する CPU を搭載したデバイスが抽出に含まれます。

- **仮想 CPU コア数（最小）**

  仮想 CPU コアの最小数。入力フィールドで指定された仮想コア数の範囲に一致する CPU を搭載したデバイスが抽出に含まれます。

- **仮想 CPU コア数（最大）**

  仮想 CPU コアの最大数。入力フィールドで指定された仮想コア数の範囲に一致する CPU を搭載したデバイスが抽出に含まれます。

- **ハードディスク容量（GB）（最小）**

  デバイス上のハードディスクの最小容量。入力フィールドで指定されたハードディスクの容量の範囲に適合するデバイスが抽出に含まれます。

- **ハードディスク容量（GB）（最大）**

  デバイス上のハードディスクの最大容量。入力フィールドで指定されたハードディスクの容量の範囲に適合するデバイスが抽出に含まれます。

- **RAM サイズ（MB）（最小）**

  デバイスの RAM の最小サイズ。入力フィールドで指定されたサイズ範囲に一致する RAM を搭載したデバイスが抽出に含まれます。

- **RAM サイズ（MB）（最大）**

  デバイスの RAM の最大サイズ。入力フィールドで指定されたサイズ範囲に一致する RAM を搭載したデバイスが抽出に含まれます。

サードパーティ製ソフトウェアの詳細

［**アプリケーションレジストリ**］サブセクションでは、インストール済みのアプリケーションを基にデバイスを検索するための基準を設定できます：

- **アプリケーション名**

  アプリケーションを選択できるドロップダウンリスト。指定したアプリケーションがインストールされているデバイスが抽出に含まれます。

- **アプリケーションのバージョン**

  選択したアプリケーションのバージョンを指定できる入力フィールド。

- **製造元**

  デバイスにインストールされているアプリケーションの製造元を選択できるドロップダウンリスト。

- **アプリケーションのステータス**

  アプリケーションのステータス（*インストール済み*、*未インストール*）を選択できるドロップダウンリスト。指定のアプリケーションがインストール済みまたは未インストールのデバイスが、選択したステータスに応じて抽出に含まれます。

- **アップデートによって検索**

  このオプションをオンにすると、該当するデバイスにインストールされているアプリケーションのアップデートに関する情報を使用して検索が実行されます。このチェックボックスをオンにすると、［**アプリケーション名**］、［**アプリケーションのバージョン**］、［**アプリケーションのステータス**］というフィールドがそれぞれ、［**アップデート名**］、［**アップデートのバージョン**］、［**ステータス**］に変わります。

  既定では、このオプションはオフです。

- **互換性がないセキュリティ製品**

  サードパーティのセキュリティ製品を選択できるドロップダウンリスト。指定したアプリケーションがインストールされているデバイスが、検索時に抽出に含まれます。

- **アプリケーションタグ**

  このドロップダウンリストでは、アプリケーションタグを選択できます。選択したタグが説明にあるアプリケーションをインストール済みのすべてのデバイスが、デバイスの抽出に含まれます。

- **指定したタグのないデバイスに適用する**

  このオプションをオンにすると、選択したタグがいずれも説明に含まれないデバイスが抽出に含まれます。

  このオプションをオフにすると、基準が適用されません。

  既定では、このオプションはオフです。

［**脆弱性とアップデート**］サブセクションでは、Windows Update をどこから取得するかを基にデバイスを抽出に含める場合に使用する基準を指定できます：

WUA の管理サーバーへの切り替え

このドロップダウンリストから、次のいずれかを選択できます：

- **はい**：これを選択すると、Windows Update の更新プログラムを管理サーバーから受信するデバイスが検索結果に含まれます。
- ［**いいえ**］。これを選択すると、Windows Update の更新プログラムを他の提供元から受信するデバイスが検索結果に含まれます。

カスペルスキー製品の詳細

［**カスペルスキー製品**］サブセクションでは、選択した管理対象アプリケーションを基にデバイスを抽出に含めるための基準を設定できます：

- **アプリケーション名**

  カスペルスキー製品の名前で検索を実行する場合、抽出に含めるデバイスの基準を、ドロップダウンリストで設定できます。

  リストには、管理コンピューターに管理プラグインがインストールされているアプリケーションの名前のみが表示されます。

  アプリケーションが選択されていない場合、この基準は適用されません

- **アプリケーションのバージョン**

  カスペルスキー製品のバージョン番号で検索を実行する場合、抽出に含めるデバイスの基準を、入力フィールドで設定できます。

  バージョン番号が指定されていない場合、この基準は適用されません。

- **重要なアップデート名**

  アプリケーションのステータス（*インストール済み*、*未インストール*）を選択できるドロップダウンリスト。指定のアプリケーションがインストール済みまたは未インストールのデバイスが、選択したステータスに応じて抽出に含まれます。

  製品の名前またはアップデートパッケージ番号で検索する場合の、抽出に含めるデバイスの基準を、入力フィールドで設定できます。

  このフィールドが空白の場合、この基準は適用されません。

- **モジュールの最終アップデート期間を選択**

  このオプションを使用して、デバイスにインストールされているソフトウェアモジュールの前回のアップデート日時でデバイスを検索する基準を設定できます。

  このチェックボックスをオンにすると、入力フィールドで、デバイスにインストールされているアプリケーションモジュールの前回のアップデートが実行された日時の範囲を指定できます。

  このチェックボックスをオフにすると、この基準は適用されません。

  既定では、このチェックボックスはオフです。

- **デバイスを管理サーバーで管理する**

  ドロップダウンリストで、Kaspersky Security Center Cloud コンソールで管理されているデバイスを抽出に含めることができます：

  - **はい**：Kaspersky Security Center Cloud コンソールで管理されているデバイスが抽出に含まれます。
  - ［**いいえ**］。Kaspersky Security Center Cloud コンソールにより管理されていないデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

- **セキュリティ製品がインストールされています**

  ドロップダウンリストで、セキュリティ製品がインストールされているすべてのデバイスを抽出に含めることができます：

  - **はい**：セキュリティ製品がインストールされているすべてのデバイスが抽出に含まれます。
  - ［**いいえ**］。セキュリティ製品がインストールされていないすべてのデバイスが抽出に含まれます。
  - **値を選択しない**：基準は適用されません。

［**プロテクション**］サブセクションでは、保護ステータスを基にデバイスを抽出に含めるための基準を設定できます：

- **定義データベースの公開日時**

  このオプションをオンにすると、定義データベースの公開日時でクライアントデバイスを検索できます。入力フィールドで設定した期間に基づいて検索が実行されます。

  既定では、このオプションはオフです。

- **定義データベースのレコード数**

  このオプションを有効にすると、定義データベースのレコード数でクライアントデバイスを検索できます。入力フィールドで、定義データベースのレコード数の上下のしきい値を設定できます。

  既定では、このオプションはオフです。

- **前回のスキャン**

  このオプションをオンにすると、前回マルウェアスキャンを実行した日時でクライアントデバイスを検索できます。入力フィールドで、前回マルウェアスキャンを実行した期間を指定できます。

  既定では、このオプションはオフです。

- **検知された脅威**

  Advanced Encryption Standard（AES）対称ブロック暗号アルゴリズム。ドロップダウンリストから、暗号化キーのサイズ（56 ビット、128 ビット、192 ビット、または 256 ビット）を選択できます。

  指定可能な値：*AES56*、*AES128*、*AES192*、または *AES256*。

このオプションをオンにすると、検知されたウイルスの数でクライアントデバイスを検索できます。入力フィールドで、ウイルス検知数の上下のしきい値を設定できます。

既定では、このオプションはオフです。

［**製品コンポーネント**］サブセクションには、対応する管理プラグインが Kaspersky Security Center Cloud コンソールにインストールされているアプリケーションのコンポーネントのリストが含まれています。

［**製品コンポーネント**］サブセクションでは、選択したアプリケーションの管理下にあるコンポーネントのステータスとバージョン番号を基にデバイスを抽出に含めるための基準を設定できます：

- **ステータス**

  アプリケーションから管理サーバーに送信されたコンポーネントのステータスに基づいてデバイスを検索します。次のステータスのいずれかを選択できます：*N/A*、*停止*、*一時停止*、*開始中*、*実行中*、*失敗*、*インストールされていない*、*ライセンスでサポートされていない*。管理対象デバイスにインストールされたアプリケーションの選択したコンポーネントのステータスが指定したステータスと一致する場合、そのデバイスが抽出に含まれます。

  製品から送信されるステータス：

  - *停止* - コンポーネントが無効で、現在動作していません。
  - *一時停止* - コンポーネントの動作が中断中です（例：管理対象製品でユーザーが保護を一時停止した）。
  - *開始中* - コンポーネントが利用開始プロセスを実行中です。
  - *実行中* - コンポーネントが有効で正常に動作しています。
  - *エラー* - コンポーネントの動作中にエラーが発生しました。
  - *未インストール* - 製品のカスタムインストールの設定時に、ユーザーがコンポーネントをインストール対象として選択しませんでした。
  - *ライセンスでサポートされていない* - ライセンスは選択したコンポーネントをカバーしていません。

  他のステータスとは異なり、［*N/A*］ステータスはアプリケーションから送信されたものではありません。このステータスは、選択したコンポーネントのステータスについて、アプリケーションに情報がないことを示します。たとえば、デバイスにインストールされているアプリケーションのいずれにも選択したコンポーネントが属していない場合や、デバイスの電源がオフの場合などです。

- **バージョン**

  リストで選択したコンポーネントのバージョン番号に基づいてデバイスを検索します。`3.4.1.0` などのバージョン番号を入力し、選択したコンポーネントのバージョン番号がこれと「等しい」「それより古い」「それより新しい」かを指定できます。また、指定したバージョンを除くすべてのバージョンを検索するようにも設定できます。

タグ

［**タグ**］セクションでは、管理対象デバイスの説明に追加済みのキーワード（タグ）を基にデバイスを抽出に含めるための基準を設定できます：

少なくとも1個のタグが一致する場合に適用する

このオプションをオンにすると、選択されたタグを1つ以上説明に含むデバイスが検索結果に表示されます。

このオプションをオフにすると、選択されたすべてのタグを説明に含むデバイスのみが検索結果に表示されます。

既定では、このオプションはオフです。

基準にタグを追加するには、［**追加**］をクリックし、［**タグ**］入力フィールドをクリックしてタグを選択します。選択したタグを持つデバイスをデバイスの抽出に含めるか除外するかを指定します。

- **含む**

  このオプションをオンにすると、検索結果には、選択したタグが説明内に含まれるデバイスが表示されます。デバイスを検索するため、文字数不定の任意の文字列を表すアスタリスクを使用できます。

  既定では、このオプションがオンです。

- **含まない**

  このオプションをオンにすると、検索結果には、選択したタグが説明内に含まれないデバイスが表示されます。デバイスを検索するため、文字数不定の任意の文字列を表すアスタリスクを使用できます。

ユーザー

［**ユーザー**］セクションでは、オペレーティングシステムにログインしたユーザーのアカウントを基にデバイスを抽出に含めるための基準を設定できます。

- **前回システムにログインしたユーザー**

  このオプションをオンにすると、基準を設定するためのユーザーアカウントを選択できます。ユーザーリストはフィルタリングされており、内部ユーザーが表示されていることに注意してください。選択したユーザーがシステムの前回のログインを実行したデバイスが検索結果に含まれます。

- **少なくとも1回システムにログインしたユーザー**

  このオプションをオンにすると、基準を設定するためのユーザーアカウントを選択できます。ユーザーリストはフィルタリングされており、内部ユーザーが表示されていることに注意してください。指定したユーザーがシステムに少なくとも1回ログインしたデバイスが検索結果に含まれます。

デバイスの抽出からデバイスリストをエクスポート

Kaspersky Security Center Cloud コンソールには、デバイスの抽出からデバイスに関する情報を CSV または TXT ファイルに保存できます。

デバイスの抽出からデバイスリストをエクスポートするには：

1. デバイスの抽出からデバイスを含むテーブルを開きます。
2. 次のいずれかの方法を使用して、抽出するデバイスを選択します：
   - 特定のデバイスを選択するには、その横にあるチェックボックスをオンにしてください。
   - 現在のテーブルページからすべてのデバイスを抽出するには、デバイステーブルヘッダーのチェックボックスをオンにし、［**現在のページをすべて選択**］をオンにします。
   - テーブルからすべてのデバイスを抽出するには、デバイステーブルヘッダーのチェックボックスをオンにし、［**すべて選択**］をオンにします。

［**CSV へエクスポート**］または［**TXT へエクスポート**］をクリックします。テーブルに含まれる抽出したデバイスに関するすべての情報がエクスポートされます。

フィルター条件をデバイステーブルに適用した場合、エクスポートされるのは、表示された列からフィルター処理されたデータのみです。

抽出で管理グループからデバイスを削除

デバイスの抽出作業を行う場合は、デバイスを削除する必要がある管理グループに切り替えずに、この抽出に含まれる管理グループからデバイスを削除することができます。

管理グループからデバイスを削除するには：

1. メインメニューで、［**アセット（デバイス）**］→［**デバイスの抽出**］、または［**検出と製品の導入**］→［**デバイスの抽出**］セクションの順に選択します。
2. 抽出リストで、デバイスの抽出の名前をクリックします。
   このページには、デバイスの抽出に含まれるデバイス関連情報のテーブルが表示されます。
3. 削除するデバイスを選択し、［**削除**］をクリックします。
   選択したデバイスが対応する管理グループから削除されます。

デバイスが不可視の時の処理の表示と設定

グループ内のクライアントデバイスがアクティブでない場合、通知を受け取ることができます。こうしたデバイスを自動的に削除することもできます。

グループ内のデバイスがアクティブでない場合の処理を表示したり設定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. 目的の管理グループの名前をクリックします。
   管理グループのプロパティウィンドウが開きます。

3. プロパティウィンドウで［**設定**］タブに移動します。

4. ［**継承**］セクションで、次のオプションの有効と無効を切り替えます：

- **親グループから継承する**

  クライアントデバイスが属する親グループからこのセクションの設定が継承されます。このオプションをオンにすると、［**ネットワーク上のデバイスのアクティビティ**］の設定がロックされ変更できなくなります。

  このオプションは管理グループに親グループが存在する場合にのみ利用できます。

  既定では、このオプションはオンです。

- **設定を子グループへ強制的に継承させる**

  設定値が子グループに配信され、子グループのプロパティではそれらの設定がロックされます。

  既定では、このオプションはオフです。

5. ［**デバイスのアクティビティ**］セクションで、次のオプションの有効と無効を切り替えます：

- **次の期間デバイスが不可視の場合管理者に通知（日）**

  このオプションをオンにすると、管理者が非アクティブなデバイスについて通知を受け取ります。［**デバイスがネットワーク上で長期間アクティブになっていません**］イベントが作成されるまでの期間を指定できます。既定の期間は 7 日です。

  既定では、このオプションはオンです。

- **次の期間デバイスが不可視の場合グループから削除（日）**

  このオプションをオンにすると、デバイスをグループから自動的に削除するまでの期間を指定できます。既定の期間は 60 日です。

  既定では、このオプションはオンです。

6. ［**保存**］をクリックします。

変更内容が保存され、適用されます。

デバイスのステータスの概要

Kaspersky Security Center Cloud コンソールは、各管理対象デバイスにステータスを割り当てます。特定のステータスは、ユーザーが定義した条件を満たしているかどうかによって異なります。場合によっては、デバイスにステータスを割り当てる時に、Kaspersky Security Center Cloud コンソールはネットワーク内のデバイスの可視性フラグを考慮します（下の表を参照）。Kaspersky Security Center Cloud コンソールが 2 時間以内にネットワーク内のデバイスを見つけられない場合、デバイスの可視性フラグは「*不可視*」に設定されます。

ステータスは次の通りです：

- *緊急*または*緊急* / *可視*

- *警告*または*警告 / 可視*
- *OK*または*OK / 可視*

次の表では、「*緊急*」または「*警告*」ステータスをデバイスに割り当てるために満たすべき既定の条件を、可能なすべての値とともに一覧で表示します。

デバイスにステータスを割り当てる条件

条件	条件の説明	設定可能な値
セキュリティ製品がインストールされていません	デバイスにネットワークエージェントはインストールされていますが、セキュリティ製品はインストールされていません。	• 切り替えスイッチをオン • 切り替えスイッチをオフ
ウイルスが多数検知されました	ウイルススキャンタスクなどのウイルス検知タスクによりデバイスでウイルスが検知され、検知数が指定された値を超えました。	0 より大きい値
リアルタイム保護レベルが管理者の設定と異なります	デバイスはネットワーク上で可視ですが、リアルタイム保護レベルがデバイスのステータスの条件として管理者によって設定されたレベルと異なっています。	• 停止 • 一時停止 • 実行中
マルウェアスキャンが長期間実行されていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、*マルウェアのスキャン*タスクもローカルスキャンタスクも実行されていない状態が指定期間を越えて続いています。この条件は、7 日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。	1 日より大きい値
定義データベースがアップデートされていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、このデバイスで定義データベースがアップデートされていない状態が指定期間を越えて続いています。この条件は、1 日以上前に管理サーバーデータベースに追加されたデバイスにのみ適用されます。	1 日より大きい値
長期間接続されていません	デバイスにネットワークエージェントはインストールされていますが、デバイスがオフになっており、デバイスが管理サーバーに接続されていない状態が指定期間を越えて続いています。	1 日より大きい値
アクティブな脅威を検知しました	［**アクティブな脅威**］フォルダー内の未処理オブジェクトの数が指定の値を上回っています。	0 項目より大きい値
再起動が必要です	デバイスはネットワーク上で可視ですが、アプリケーションが選択した理由でデバイスの再起動を必要とする状態が指定期間を越えて続いています。	0 分より大きい値
競合アプリケーションがインストールされています	デバイスはネットワーク上で可視ですが、ネットワークエージェントから実行されたソフトウェアインベントリにより、競合するアプリケーションがデバイスにインストールされていることを検知しました。	• 切り替えスイッチをオフ • 切り替えスイッチをオ

		ン
ソフトウェアの脆弱性が検知されました	デバイスはネットワーク上で可視でネットワークエージェントもインストールされていますが、*脆弱性とアプリケーションのアップデートの検索*タスクが、デバイスにインストールされているアプリケーションで指定された重要度の脆弱性を検知しました。	• 緊急 • 高 • 中 • 脆弱性を修正できない場合は無視する • 修正プログラムがインストール用に割り当てられている場合は無視する
ライセンスの有効期間が終了しました	デバイスはネットワーク上で可視ですが、ライセンスの有効期間が終了しています。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
ライセンスの有効期間がまもなく終了します	デバイスはネットワーク上で可視ですが、ライセンスの有効期間の残り日数が指定した期間以下しかありません。	0 日より大きい値
Windows Update 更新プログラムのチェックが長期間実行されていません	デバイスはネットワーク上で可視ですが、Windows Update の同期の実行タスクが実行されていない状態が指定期間を越えて続いています。	1 日より大きい値
暗号化ステータスが無効です	デバイスにネットワークエージェントはインストールされていますが、デバイスの暗号化結果が割り当て条件として指定されているものと合致しました。	• ユーザーが拒否したため、ポリシーに準拠していない（外部デバイスのみ）。 • エラーにより、ポリシーに準拠していない。

		• ポリシーを適用したら再起動する必要がある。 • 暗号化ポリシーが指定されていない。 • サポートされていない。 • ポリシーを適用するとき。
モバイルデバイスの設定がポリシーに適合していません	コンプライアンスルールをチェックしたところ、モバイルデバイスの設定が Kaspersky Endpoint Security for Android ポリシーで指定された設定と異なります。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
未処理のセキュリティ問題が検出されました	未処理のセキュリティ問題がデバイス上でいくつか見つかりました。セキュリティ問題は、クライアントデバイスにインストールしたカスペルスキー製品によって自動で作成されるか、管理者が手動で作成します。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
製品が定義したデバイスのステータス	デバイスのステータスが管理対象アプリケーションによって定義されています。	• 切り替えスイッチをオフ • 切り替えスイッチをオン
デバイスに空き容量がありません	デバイスの空き容量が指定された値未満またはデバイスと管理サーバーを同期できませんでした。デバイスが管理サーバーと正常に同期されなおかつデバイスの空き容量が指定値以上になった場合、ステータスが［*緊急*］または［*警告*］から［*OK*］に変更されます。	0 MB より大きい値
デバイスが管理対象外になりました	デバイスの検索中、デバイスはネットワークで認識されましたが、管理サーバーとの同期に 3 回以上失敗しました。	• 切り替えスイッチをオフ • 切り替えスイッチをオ

		ン
プロテクションが無効です	デバイスはネットワーク上で可視ですが、デバイス上でセキュリティ製品が無効になっている状態が指定期間を越えて続いています。 この場合、セキュリティ製品の状態は*停止中*または*エラー*となり、*開始中*、*実行中*、*中断中*とは異なります。	0 分より大きい値
セキュリティ製品が実行されていません	デバイスはネットワーク上で可視でセキュリティ製品もインストールされていますが、セキュリティ製品が実行されていません。	• 切り替えスイッチをオフ • 切り替えスイッチをオン

Kaspersky Security Center Cloud コンソールでは、指定した条件が満たされると、管理グループのデバイスのステータスが自動的に切り替わるように設定できます。指定した条件が満たされると、クライアントデバイスには、「*緊急*」または「*警告*」のステータスのいずれかが割り当てられます。指定した条件を満たしていない場合、クライアントデバイスには「*OK*」ステータスが割り当てられます。

1つの条件の複数の値に対して異なるステータスを対応させることができます。たとえば、［**定義データベースがアップデートされていません**］条件の値が「**3 日より大きい値**」の場合はクライアントデバイスに「*警告*」ステータスが割り当てられ、条件値が「**7 日より大きい値**」の場合は「*緊急*」ステータスが割り当てられます。

Kaspersky Security Center Cloud コンソールによってデバイスにステータスが割り当てられると、一部の条件（条件説明の列を参照）で可視性フラグが考慮されます。たとえば、ある管理対象デバイスは［定義データベースがアップデートされていません］条件を満たしていたために「*緊急*」ステータスが割り当てられました。のちにデバイスには可視性フラグが設定され、その後、そのデバイスは「*OK*」ステータスが割り当てられます。

デバイスのステータスの切り替えの設定

デバイスに「*緊急*」または「*警告*」ステータスを割り当てる条件を変更できます。

デバイスのステータスの「緊急」への切り替えを有効にするには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. グループのリストが開いたら、デバイスのステータスの切り替えを設定するグループ名をクリックします。
3. プロパティウィンドウが開いたら、［**デバイスのステータス**］タブを選択します。
4. 左側のペインで、［**緊急**］を選択します。
5. 右側のペインの［**指定されている場合は「緊急」に設定**］セクションで、デバイスに［*緊急*］ステータスを割り当てる条件をオンにします。

親ポリシーでロック状態になっていない設定のみ変更できます。

6. リスト内の条件の横にあるラジオボタンをオンにします。
7. リストの左上にある［**編集**］をクリックします。
8. 選択した条件に対して適切な値を設定します。
   すべての条件に値を設定できるわけではありません。
9. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*緊急*」ステータスが割り当てられます。

デバイスのステータスの「警告」への切り替えを有効にするには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. グループのリストが開いたら、デバイスのステータスの切り替えを設定するグループ名をクリックします。
3. プロパティウィンドウが開いたら、［**デバイスのステータス**］タブを選択します。
4. 左側のペインで、［**警告**］を選択します。
5. 右側のペインの［**指定されている場合は「警告」に設定**］セクションで、デバイスに［*警告*］ステータスを割り当てる条件をオンにします。

   > 親ポリシーでロック状態になっていない設定のみ変更できます。

6. リスト内の条件の横にあるラジオボタンをオンにします。
7. リストの左上にある［**編集**］をクリックします。
8. 選択した条件に対して適切な値を設定します。
   すべての条件に値を設定できるわけではありません。
9. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*警告*」ステータスが割り当てられます。

クライアントデバイスの管理サーバーの変更

［**管理サーバーの変更**］タスクを使用して、クライアントデバイスを管理する管理サーバーを別のサーバーに変更できます。タスクの完了後、選択したクライアントデバイスは指定した管理サーバーの管理下に置かれます。次の管理サーバー間でデバイス管理を切り替えることができます：

- プライマリ管理サーバーとそのいずれかの仮想管理サーバー
- 同じプライマリ管理サーバーの 2 つの仮想管理サーバー

クライアントデバイスを管理する管理サーバーを別のサーバーに変更するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. Kaspersky Security Center Cloud コンソールアプリケーションで、［**管理サーバーの変更**］タスク種別を選択します。
4. 作成中のタスク名を入力します。
   タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクを割り当てるデバイスを選択します。
6. 選択したデバイスの管理に使用する管理サーバーを選択します。
7. 次のようにアカウントの設定を指定します。
   - **既定のアカウント**
     タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。
     既定では、このオプションがオンです。
   - **アカウントの指定**
     ［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。
   - **アカウント**
     タスクを実行するアカウント。
   - **パスワード**
     タスクが実行されるアカウントのパスワード。
8. ［**タスク作成の終了**］ページで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
9. ［**終了**］をクリックします。
   タスクが作成され、タスクリストに表示されます。
10. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。
11. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。
12. ［**保存**］をクリックします。
    タスクが指定した設定で作成されます。
13. 作成したタスクを実行します。

タスクが完了すると、タスクの対象となったクライアントデバイスは、タスク設定で指定した管理サーバーの管理下に置かれます。

クラスターとサーバーアレイについて

Kaspersky Security Center Cloud コンソールでは、クラスター技術がサポートされます。クライアントデバイスにインストールされたアプリケーションがサーバーアレイの一部であることを確認する情報が、ネットワークエージェントから管理サーバーに送信されると、このクライアントデバイスはクラスターノードになります。

管理グループにクラスターまたはサーバーアレイが含まれている場合、［**管理対象デバイス**］ページには 2 つのタブが表示されます。1つは個々のデバイス用で、もう1つはクラスターおよびサーバーアレイ用です。管理対象デバイスがクラスターノードとして検出されると、クラスターは個別のオブジェクトとして［**クラスターとサーバーアレイ**］タブに追加されます。

クラスターまたはサーバーアレイノードは、他の管理対象デバイスとともに［**デバイス**］タブに一覧表示されます。個別のデバイスとしてノードのプロパティを表示したり、他の操作を実行したりできますが、クラスターノードを削除したり、そのクラスターとは別に他の管理グループに移動したりすることはできません。クラスター全体の削除または移動のみが可能です。

クラスターまたはサーバーアレイで実行できる操作は次の通りです：

- プロパティを表示する
- クラスターまたはサーバーアレイを別の管理グループに移動する

  クラスターまたはサーバーアレイを別のグループに移動すると、そのすべてのノードも一緒に移動します。これは、クラスターとそのノードのいずれかが常に同じ管理グループに属しているためです。
- 削除

  クラスターまたはサーバーアレイの削除は、クラスターまたはサーバーアレイが組織のネットワークに存在しなくなった場合にのみ行うことを推奨します。クラスターがまだネットワーク上に表示され、ネットワークエージェントとカスペルスキーセキュリティ製品がまだクラスターノードにインストールされている場合、Kaspersky Security Center Cloud コンソールは、削除されたクラスターとそのノードを管理対象デバイスのリストに自動的に戻します。

クラスターまたはサーバーアレイのプロパティ

クラスターまたはサーバーアレイの設定を表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］→［**クラスターとサーバーアレイ**］の順に移動します。

   クラスターとサーバーアレイのリストが表示されます。

2. 必要なクラスターまたはサーバーアレイの名前をクリックします。

選択したクラスターまたはサーバーアレイのプロパティウィンドウが表示されます。

全般

［**全般**］セクションには、クラスターまたはサーバーアレイに関する一般情報が表示されます。情報は、管理サーバーでクラスターノードの前回の同期中に受信されたデータに基づいて提供されます。

- **名前**
- **説明**
- **Windows ドメイン**

  クラスターまたはサーバーアレイを含む Windows ドメインまたはワークグループ。

- **NetBIOS 名**

  クラスターまたはサーバーアレイの Windows ネットワーク名。

- **DNS 名**

  クラスターまたはサーバーアレイの DNS ドメインの名前。

タスク

［**タスク**］タブでは、既存タスクのリストの表示、新規タスクの作成、タスクの削除、開始、停止、タスク設定の変更、実行結果の表示など、クラスターまたはサーバーアレイに割り当てられたタスクを管理できます。リストされているタスクは、クラスターノードにインストールされているカスペルスキーセキュリティ製品に関連するものです。Kaspersky Security Center Cloud コンソールは、クラスターノードからタスクリストとタスクステータスの詳細を受け取ります。接続に失敗すると、ステータスは表示されません。

ノード

このタブには、クラスターまたはサーバーアレイに含まれるノードのリストが表示されます。ノード名をクリックすると、デバイスのプロパティウィンドウが表示されます。

カスペルスキー製品

プロパティウィンドウには、クラスターノードにインストールされているカスペルスキーセキュリティ製品に関連する情報と設定を含む追加のタブが含まれている場合もあります。

デバイスのタグ

このセクションでは、デバイスタグの概要と、デバイスタグの作成、編集、手動または自動でのデバイスのタグ付けを行う方法を説明しています。

デバイスタグの概要

Kaspersky Security Center Cloud コンソールでは、デバイスにタグを割り当てることができます。*タグ*は、デバイスのグループ化、説明、または検索に使用することができるデバイスのラベルです。デバイスに割り当てられたタグは、抽出の作成、デバイスの検索、および各管理グループへのデバイスの割り当てに使用できます。

デバイスには、手動または自動でタグ付けできます。個々のデバイスにタグ付けする必要がある場合は、手動のタグ付けを使用することができます。自動タグ付けは、指定したタグ付けルールに従い、Kaspersky Security Center Cloud コンソールによって実行されます。

デバイスには、指定されたルールが適合する場合に自動的にタグ付けされます。個々のルールは各タグに対応します。ルールは、デバイス、オペレーティングシステム、デバイスにインストールされたアプリケーションのネットワークプロパティ、およびその他のデバイスのプロパティに適用されます。たとえば、ネットワークに Windows、Linux、macOS を実行する複数のデバイスが含まれている場合、すべての Linux ベースのデバイスに `[Linux]` タグを割り当てるルールを設定できます。その後、デバイスの抽出を作成する場合にこのタグを使用できます。これにより、すべての Linux ベースのデバイスを抽出し、タスクを割り当てることができます。次の場合は、デバイスからタグが自動的に削除されます：

- タグの割り当てルールの条件をデバイスが満たさなくなった場合。
- タグを割り当てるルールがオフになったあるいは削除された場合。

管理サーバーごとのタグのリストとタグ付けルールのリストは、プライマリ管理サーバーとセカンダリ管理サーバーを含むその他のすべての管理サーバーとは影響関係を持ちません。タグ付けのルールは、ルールが作成された管理サーバーのデバイスに対してのみ適用されます。

デバイスタグの作成

デバイスのタグを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. ［**追加**］をクリックします。
   新規タグの入力ウィンドウが表示されます。
3. ［**タグ**］にタグ名を入力します。
4. ［**保存**］をクリックして変更内容を保存します。

   デバイスタグのリストに新しいタグが表示されます。

デバイスタグの名前変更

デバイスタグの名前を変更するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. 名前を変更するタグの名前をクリックします。
   タグのプロパティウィンドウが表示されます。
3. ［**タグ**］でタグ名を変更します。
4. ［**保存**］をクリックして変更内容を保存します。

デバイスタグのリストに更新したタグが表示されます。

デバイスタグの削除

デバイスタグを削除するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. リストから削除するデバイスタグを選択します。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**はい**］をクリックします。

デバイスタグが削除されます。削除されたタグが割り当てられていたすべてのデバイスから、このタグが自動的に削除されます。

削除したタグは、自動タグルールから自動的に削除されません。タグの削除後も、タグを割り当てるルールの条件に初めて合致した場合にのみ、新規デバイスに対してタグが割り当てられます。

このタグがアプリケーションまたはネットワークエージェントによってデバイスに割り当てられている場合、削除されたタグはデバイスから自動的に削除されません。デバイスからタグを削除するには、klscflag ユーティリティを使用します。

タグを割り当てられているデバイスの表示

タグを割り当てられているデバイスを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に選択します。
2. 割り当て先のデバイスを確認するタグの横の［**デバイスの表示**］をクリックします。

表示されるデバイスのリストには、タグが割り当てられているデバイスのみが表示されます。

デバイスタグのリストに戻るには、ブラウザーの「**戻る**」をクリックします。

デバイスに割り当てられているタグの表示

デバイスに割り当てられているタグを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
2. タグを表示するデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**タグ**］タブをクリックします。

選択したデバイスに割り当てられているタグのリストが表示されます。

デバイスに別のタグを割り当てたり、割り当て済みのタグを削除することができます。管理サーバーに存在するすべてのタグを表示することもできます。

手動でのデバイスのタグ付け

デバイスにタグを割り当てるには：

1. メニューを移動して、別のタグを追加するデバイスに割り当てられているタグを表示します。
2. ［**追加**］をクリックします。
3. 表示されたウィンドウで、次のいずれかを実行します：
   - 新しいタグを作成して割り当てるには、［**新しいタグを作成する**］を選択して新しいタグの名前を入力します。
   - 既存のタグを選択するには、［**既存のタグを割り当てる**］を選択し、ドロップダウンリストから目的のタグを選択します。
4. ［**OK**］をクリックして変更を適用します。
5. ［**保存**］をクリックして変更内容を保存します。

選択したタグがデバイスに割り当てられます。

複数デバイスにタグを割り当てるには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. タグを割り当てるデバイスを選択します。
3. ［**タグ**］をクリックし、ドロップダウンリストから［**割り当て**］を選択します。
4. ウィンドウが開いたら、ドロップダウンリストからタグを選択します。
   必要に応じて、複数のタグを選択できます。
   また、次の操作ができます：
   - タグの名前を編集するには、［**編集**］（）アイコンをクリックします。
     新しいタグ名を指定し、［**保存**］をクリックします。

     > デバイスのタグのリスト内にあるタグの名前も変更されます。

   - タグを削除するには、［**削除**］（）アイコンをクリックします。
     表示されたウィンドウで［**削除**］をクリックします。

     > タグは管理サーバーからも削除されます。

5. ［**保存**］をクリックします。

選択したデバイスにタグが割り当てられます。割り当てられたタグは削除できます。

デバイスに割り当てられたタグの削除

解除されたタグ自身は削除されません。必要に応じて、手動で削除できます。

アプリケーションまたはネットワークエージェントによってデバイスに割り当てられたタグを手動で削除することはできません。これらのタグを削除するには、klscflag ユーティリティを使用します。

デバイスからタグを削除するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. タグを表示するデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**タグ**］タブをクリックします。
4. 削除するタグに隣接するチェックボックスをオンにします。
5. リストの上部にある［**タグを解除する**］をクリックします。
6. 表示されたウィンドウで［**はい**］をクリックします。

タグがデバイスから削除されます。

複数のデバイスからタグを削除するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. タグを削除するデバイスを選択します。
3. ［**タグ**］をクリックし、ドロップダウンリストから［**削除**］を選択します。
4. ウィンドウが開いたら、削除するタグの横にあるチェックボックスをオンにします。

ウィンドウには、手順 2 で選択したすべてのデバイスに割り当てられたすべてのタグが表示されます。

5. ［**保存**］をクリックします。

タグがデバイスから削除されます。

デバイスの自動タグルールの表示

デバイスの自動タグルールを表示するには：

次のいずれかの手順を実行します：

- メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**自動タグルール**］の順に選択します。
- メインメニューで、［**アセット（デバイス）**］→［**タグ**］→［**デバイスのタグ**］の順に移動し、［**自動タグルールの設定**］をクリックします。
- デバイスに割り当てられているタグを確認し、［**設定**］をクリックします。

デバイスの自動タグルールのリストが表示されます。

デバイスの自動タグルールの編集

デバイスの自動タグルールを編集するには：

1. デバイスの自動タグルールを表示します。
2. 編集するルールの名前をクリックします。
   ルールの設定ウィンドウが表示されます。
3. ルールのプロパティ全般を編集します：
   a. ［**ルール名**］で、ルール名を変更します。
      名前は 256 文字以下でなければなりません。
   b. 次のいずれかの手順を実行します：
      - スイッチを［**ルールが有効**］に切り替えるとルールを有効にできます。
      - スイッチを［**ルールが無効**］に切り替えるとルールを無効にできます。
4. 次のいずれかの手順を実行します：
   - 新しい条件を追加する場合は、［**追加**］をクリックし、開いたウィンドウで新しい条件の設定を指定します。
   - 既存の条件を編集するには、編集する条件の名前をクリックし、条件設定を編集します。
   - 条件を削除するには、削除する条件の横のチェックボックスを選択し、［**削除**］をクリックします。
5. 設定ウィンドウで、［**OK**］をクリックします。
6. ［**保存**］をクリックして変更内容を保存します。

編集後のルールがリストに表示されます。

デバイスの自動タグルールの作成

デバイスの自動タグルールを作成するには：

1. デバイスの自動タグルールを表示します。

2. ［**追加**］をクリックします。
   新規ルールの設定ウィンドウが表示されます。

3. ルールのプロパティ全般を設定します：

   a. ［**ルール名**］で、ルール名を入力します。
      名前は 256 文字以下でなければなりません。

   b. 次のいずれかの手順を実行します：

      - スイッチを［**ルールが有効**］に切り替えるとルールを有効にできます。
      - スイッチを［**ルールが無効**］に切り替えるとルールを無効にできます。

   c. ［**タグ**］で、新しいデバイスタグの名前を入力するか、リストから既存のデバイスタグを選択します。
      名前は 256 文字以下でなければなりません。

4. 条件セクションで［**追加**］をクリックして新しい条件を追加します。
   新しい条件の設定ウィンドウが表示されます。

5. 条件の名前を入力します。
   名前は 256 文字以下でなければなりません。名前は、1 つのルール内で一意である必要があります。

6. 次の条件によりルールのトリガーを設定します：複数の条件を選択できます。

   - **ネットワーク** - デバイスのネットワークプロパティ（Windows ネットワーク上のデバイス名、デバイスがドメインまたは IP サブネットに含まれるかなど）。

     > Kaspersky Security Center Cloud コンソールで使用するデータベースに大文字と小文字を区別する照合が設定されている場合は、デバイスの DNS 名の指定時に大文字と小文字を区別してください。そうしないと、自動タグ付けルールが機能しません。

   - **アプリケーション** - デバイス上のネットワークエージェントの存在、オペレーティングシステムの種別、バージョン、アーキテクチャ。
   - **仮想マシン** - デバイスが仮想マシンの特定の種別に属しているかどうか。
   - **Active Directory** - Active Directory 組織単位内のデバイスの存在および Active Directory グループ内のデバイスの所属。
   - **アプリケーションレジストリ** - デバイス上の異なる製造元によるアプリケーションの存在。

7. ［**OK**］をクリックして変更内容を保存します。
   必要に応じて、1 つのルールに対して複数の条件を設定できます。この場合、タグは少なくとも 1 つの条件を満たすデバイスに割り当てられます。

8. ［**保存**］をクリックして変更内容を保存します。

新しく作成されたルールは、選択した管理サーバーによって管理されているデバイスに適用されます。デバイスの設定がルールの条件を満たす場合、そのデバイスにタグが割り当てられます。

設定後、ルールは次の状況で適用されます：

- サーバーの負荷に応じて、自動的かつ定期的に適用
- ルールの編集後に適用
- 手動でのルール実行時に適用
- ルールの条件に合致するデバイスの設定の変更やデバイスのグループの設定の変更を管理サーバーが検知した後に適用

複数のタグ付けルールを作成できます。複数のタグ付けルールを作成しており、それらのルールのそれぞれの条件が同時に満たされる場合は、1つのデバイスに複数のタグを割り当てることができます。すべての割り当てられたタグのリストは、デバイスのプロパティで確認できます。

デバイスの自動タグルールの実行

ルールを実行すると、ルールのプロパティで指定されたタグが、ルールのプロパティで指定された条件に合致するデバイスに割り当てられます。有効なルールのみを実行できます。

デバイスの自動タグルールを実行するには：

1. デバイスの自動タグルールを表示します。
2. 実行する有効なルールに隣接するチェックボックスをオンにします。
3. ［**ルールを実行**］をクリックします。

   選択したルールが実行されます。

デバイスの自動タグルールの削除

デバイスの自動タグルールを削除するには：

1. デバイスの自動タグルールを表示します。
2. 削除するルールに隣接するチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されるウィンドウで、もう一度［**削除**］をクリックします。

   選択したルールが削除されます。このルールのプロパティで指定されていたタグは、このタグが割り当てられていたすべてのデバイスから割り当て解除されます。

> 解除されたタグ自身は削除されません。必要に応じて、手動で削除できます。

隔離とバックアップ

デバイススキャン中、クライアントデバイスにインストール済みのカスペルスキー製品によって、ファイルが隔離やバックアップに移動されることがあります。

*隔離*とは、感染の可能性があるファイルおよび検知時点で駆除できないファイルを格納する特別なリポジトリです。

*バックアップ*は、駆除中に削除または変更されたファイルのバックアップコピーを保存することを目的としています。

Kaspersky Security Center Cloud コンソールは、デバイス上のカスペルスキー製品によって隔離またはバックアップに配置されたファイルをまとめたリストを作成します。クライアントデバイス上のネットワークエージェントによって、隔離とバックアップにあるファイルに関する情報が管理サーバーに転送されます。

Kaspersky Security Center Cloud コンソールでは、リポジトリのファイルは管理サーバーにコピーされません。すべてのファイルは、デバイス上のリポジトリに保存されます。

リポジトリからのファイルのダウンロード

Kaspersky Security Center Cloud コンソールでは、クライアントデバイス上でセキュリティ製品によって隔離またはバックアップに配置されたファイルのコピーをダウンロードできます。ファイルは指定した場所にコピーされます。

デバイスの設定で［**管理サーバーから切断しない**］がオンになっているか、プッシュサーバーまたは接続ゲートウェイが使用中であるかのいずれかに合致した場合のみ、ファイルをダウンロードできます。いずれの条件も満たさない場合は、ダウンロードできません。

［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

隔離またはバックアップにあるファイルのコピーをハードディスクに保存するには：

1. 次のいずれかの手順を実行します：

   - Quarantineからファイルのコピーを保存するには、メインメニューで、［**操作**］→［**リポジトリ**］→［**隔離**］の順に移動します。
   - バックアップからファイルのコピーを保存するには、メインメニューで、［**操作**］→［**リポジトリ**］→［**バックアップ**］の順に移動します。

2. 表示されるウィンドウで、ダウンロードするファイルを選択し、［**ダウンロード**］をクリックします。

   ダウンロードが開始されます。クライアントデバイスで隔離に配置されたファイルのコピーが、指定したフォルダーに保存されます。

リポジトリからのファイルの削除

隔離またはバックアップからファイルを削除するには：

1. 次のいずれかの手順を実行します：

   - Quarantineからファイルのコピーを保存するには、メインメニューで、［**操作**］→［**リポジトリ**］→［**隔離**］の順に移動します。

- バックアップからファイルのコピーを保存するには、メインメニューで、［**操作**］→［**リポジトリ**］→［**バックアップ**］の順に移動します。

2. 表示されるウィンドウで、削除するファイルを選択し、［**削除**］をクリックします。

3. 削除するファイルを確認します。

リポジトリ（隔離またはバックアップ）にファイルを配置したセキュリティ製品が、その配置したファイルをリポジトリから削除します。

クライアントデバイスのリモート診断

Windows ベースと Linux ベースのクライアントデバイス上での次の操作のリモート実行についてリモート診断を使用できます：

- トレースの有効化と無効化、トレースレベルの変更、トレースファイルのダウンロード
- システム情報とアプリケーション設定のダウンロード
- イベントログのダウンロード
- アプリケーションのダンプファイルの生成
- 診断の開始および診断レポートのダウンロード
- アプリケーションの起動、停止、再起動

クライアントデバイスからダウンロードしたイベントログと診断レポートを、管理者自身による問題のトラブルシューティングに活用できます。また、テクニカルサポートにお問い合わせいただいた場合、テクニカルサポートの担当者がより詳細な分析を行うために、トレースファイル、ダンプファイル、イベントログ、診断レポートをクライアントデバイスからダウンロードするように求められる場合もあります。

リモート診断ウィンドウを開く

Windows ベースと Linux ベースのクライアントデバイスのリモート診断を実行するには、リモート診断ウィンドウを開く必要があります。

リモート診断ウィンドウを開くには：

1. リモート診断ウィンドウを開くデバイスを選択するには、次のいずれかを実行します：
   - デバイスが管理グループに属している場合は、メインメニューで、［**アセット（デバイス）**］→［**グループ**］→［**<グループ名>**］→［**管理対象デバイス**］の順に移動します。
   - デバイスが未割り当てデバイスグループに属している場合は、メインメニューで、［**検出と製品の導入**］→［**未割り当てデバイス**］の順に移動します。
2. 目的のデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**詳細**］タブをクリックします。

4. 表示されたウィンドウで、［**リモート診断**］をクリックします。

   クライアントデバイスの［**リモート診断**］ウィンドウが開きます。管理サーバーとクライアントデバイス間の接続が確立されていない場合、エラーメッセージが表示されます。

あるいは、Linux ベースのクライアントデバイスに関するすべての診断情報を一度に取得する必要がある場合は、このデバイスで collect.sh スクリプトを実行できます。

アプリケーションのトレースの有効化と無効化

Xperf トレースを含む、アプリケーションのトレースを有効または無効にできます。

トレースの有効化および無効化

リモートデバイスでのトレースを有効または無効にするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。

   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。
3. アプリケーションリストで、トレースを有効または無効にするアプリケーションを選択します。

   リモート診断オプションのリストが表示されます。
4. トレースを有効にする場合：

   a. ［**トレース**］セクションで［**トレースを有効化**］をクリックします。

   b. ［**トレースレベルを変更**］ウィンドウで表示される設定の既定値は変更しないことを推奨します。設定値の編集が必要な場合は、テクニカルサポート担当者が必要な変更をご案内します。次の設定を使用できます：

   - **トレースレベル**

     トレースレベルでは、トレースファイルに含める情報の詳細度を指定できます。

   - **ローテーションありトレース**

     トレース情報を上書きし、トレースファイルのサイズが過剰に大きくなるの防止します。トレース情報を保存するために使用できるファイルの最大数と、各ファイルの最大サイズを指定します。トレースファイルの数が指定した最大数と同じになり、書き込み中のファイルのサイズが指定した最大サイズに達すると、新しいトレースファイルを作成できるように最も古いトレースファイルが削除されます。

     ローテーションありトレースは、Kaspersky Endpoint Security でのみ使用可能です。

   c. ［**保存**］をクリックします。

選択したアプリケーションのトレースが有効になります。場合によっては、トレースを有効にするには、セキュリティ製品とタスクを再起動しなければならないことがあります。

Linux ベースのクライアントデバイスでは、Kaspersky Security Agent コンポーネントのアップデーターのトレースは、ネットワークエージェント設定によって規制されます。したがって、Linux を実行しているクライアントデバイスでは、このコンポーネントに対して［**トレースを有効化**］および［**トレースレベルを変更**］がオフになっています。

5. 選択したアプリケーションのトレースを無効にする場合は、［**トレースを無効化**］をクリックします。

   選択したアプリケーションのトレースが無効になります。

Xperf トレースの有効化

Kaspersky Endpoint Security では、テクニカルサポート担当者がシステムのパフォーマンス情報の Xperf トレースを有効にするようにお願いする場合があります。

Xperf トレースを有効にして設定するか、無効にするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。

   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。
3. アプリケーションのリストから Kaspersky Endpoint Security for Windows を選択します。

   Kaspersky Endpoint Security for Windows のリモート診断オプションのリストが表示されます。
4. ［**Xperf トレース**］セクションで［**Xperf トレースを有効化**］をクリックします。

   Xperf トレースが既に有効になっている場合、［**Xperf トレースを無効化**］が代わりに表示されます。Kaspersky Endpoint Security for Windows の Xperf トレースを無効にする場合は、このボタンをクリックしてください。
5. ［**Xperf トレースのレベルを変更**］ウィンドウが開くので、テクニカルサポート担当者からの依頼内容に応じて、次の操作を実行してください：

   a. 次のいずれかのトレースレベルを選択します：

   - **低レベル**

     この種別のトレースファイルには、システムに関する最小限の量の情報が含まれています。

     既定では、このオプションがオンです。

   - **高レベル**

     この種別のトレースファイルには*低レベル*のトレースファイルより詳細な情報が含まれています。*低レベル*のトレースファイルではパフォーマンスを十分に評価できない場合などに、テクニカルサポートの担当者から提出を求められることがあります。*高レベル*のトレースファイルには、ハードウェア、オペレーティングシステム、プロセスとアプリケーションの開始と終了のリスト、パフォーマンスの評価に使用されたイベント、Windows システム評価ツールからのイベントなどに関する情報を含む技術情報が含まれます。

   b. 次のいずれかの Xperf トレース種別を選択します：

- **基本**

  Kaspersky Endpoint Security の動作中にトレース情報が取得されます。
  既定では、このオプションがオンです。

- **再起動時**

  管理対象デバイスでのオペレーティングシステムの起動時にトレース情報を受信します。このトレース種別は、デバイスが起動してから Kaspersky Endpoint Security が起動するまでの間にシステムパフォーマンスに影響を与える問題が発生している場合に使用すると効果的です。

［**ローテーションファイルのサイズ（MB）**］を有効にし、トレースファイルのサイズが過剰に大きくなるのを防止するように依頼される場合もあります。続いて、トレースファイルの最大サイズを設定します。ファイルが指定した最大サイズに達すると、最も古いトレース情報が削除され、新しい情報が上書きされます。

c. ローテーションするファイルサイズを定義します。

d. ［**保存**］をクリックします。

Xperf トレースが有効になり設定されます。

6. Kaspersky Endpoint Security for Windows の Xperf トレースを無効にする場合は、［**Xperf トレース**］セクションの［**Xperf トレースを無効化**］をクリックしてください。
   Xperf トレースが無効になります。

アプリケーションのトレースファイルのダウンロード

デバイスの設定で［**管理サーバーから切断しない**］がオンになっているか、プッシュサーバーまたは接続ゲートウェイが使用中であるかのいずれかに合致した場合のみ、クライアントデバイスからトレースファイルをダウンロードできます。いずれの条件も満たさない場合は、ダウンロードできません。

［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

アプリケーションのトレースファイルをダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。
   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。
3. アプリケーションのリストで、トレースファイルをダウンロードするアプリケーションを選択します。
4. ［**トレース**］セクションで、［**トレースファイル**］をクリックします。
   トレースファイルのリストが表示された［**デバイスのトレースログ**］ウィンドウが開きます。
5. ダウンロードするファイルをトレースファイルのリストから選択します。
6. 次のいずれかの手順を実行します：

- ［**ダウンロード**］をクリックして、選択したファイルをダウンロードします。ダウンロードするファイルを1つまたは複数選択できます。

- 選択したファイルの一部をダウンロード：

  a. ［**一部をダウンロード**］をクリックします。

  複数のファイルの一部を同時にダウンロードすることはできません。複数のトレースファイルを選択すると、［**一部をダウンロード**］がオフになります。

  b. ウィンドウが開いたら、名前を指定し、必要に応じてダウンロードするファイルの部分を指定します。

  Linux ベースのデバイスの場合、ファイル部分名の編集は使用できません。

  c. ［**ダウンロード**］**をクリックします。**

選択したファイル、またはその一部が指定の場所にダウンロードされます。

トレースファイルの削除

不要になったトレースファイルを削除することができます。

トレースファイルを削除するには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. 表示された［モート診断］ウィンドウで、［**イベントログ**］タブを選択します。
3. ［**トレースファイル**］セクションで、削除するトレースファイルに応じて［**Windows Update ログ**］または［**リモートインストールログ**］をクリックします。

   トレースファイルのリストが表示された［**デバイスのトレースログ**］ウィンドウが開きます。
4. 削除するファイルをトレースファイルのリストから1つまたは複数選択します。
5. ［**削除**］をクリックします。

選択したトレースファイルが削除されます。

アプリケーション設定のダウンロード

デバイスの設定で［**管理サーバーから切断しない**］がオンになっているか、プッシュサーバーまたは接続ゲートウェイが使用中であるかのいずれかに合致した場合のみ、クライアントデバイスからアプリケーション設定をダウンロードできます。いずれの条件も満たさない場合は、ダウンロードできません。

［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

クライアントデバイスからアプリケーション設定をダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［ **カスペルスキー製品**］タブを選択します。

3. ［**アプリケーション設定**］セクションで［**ダウンロード**］をクリックして、クライアントデバイスにインストールされたアプリケーションの設定に関する情報をダウンロードします。

情報を含む ZIP アーカイブが指定された場所にダウンロードされます。

クライアントデバイスからシステム情報のダウンロード

デバイスの設定で［**管理サーバーから切断しない**］がオンになっているか、プッシュサーバーまたは接続ゲートウェイが使用中であるかのいずれかに合致した場合のみ、クライアントデバイスから自分のデバイスにシステム情報をダウンロードできます。いずれの条件も満たさない場合は、ダウンロードできません。

［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

クライアントデバイスからアプリケーション設定をダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. ［リモート診断］ウィンドウで［**システム情報**］タブを選択します。
3. ［**ダウンロード**］をクリックして、クライアントデバイスに関するシステム情報をダウンロードします。

情報を含むファイルが指定された場所にダウンロードされます。

イベントログのダウンロード

デバイスの設定で［**管理サーバーから切断しない**］がオンになっているか、プッシュサーバーまたは接続ゲートウェイが使用中であるかのいずれかに合致した場合のみ、クライアントデバイスから自分のデバイスにイベントログをダウンロードできます。いずれの条件も満たさない場合は、ダウンロードできません。

［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

リモートデバイスからイベントログをダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. ［リモート診断］ウィンドウの［**イベントログ**］タブで、［**全デバイスのログ**］をクリックします。
3. ［**全デバイスのログ**］ウィンドウで、関連するログを 1 つまたは複数選択します。
4. 次のいずれかの手順を実行します：

   - ［**ファイル全体をダウンロード**］をクリックして、選択したログをダウンロードします。
   - 選択したログの一部をダウンロード：

     a. ［**一部をダウンロード**］をクリックします。

     複数のログの一部を同時にダウンロードすることはできません。複数のイベントログを選択すると、［**一部をダウンロード**］がオフになります。

     b. ウィンドウが開いたら、名前を指定し、必要に応じてダウンロードするログの部分を指定します。

     c. ［**ダウンロード**］をクリックします。

選択したイベントログ、またはその一部が指定の場所にダウンロードされます。

アプリケーションの起動、停止、再起動

クライアントデバイス上でアプリケーションを起動、停止、再起動することができます。

アプリケーションを起動、停止、再起動するには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。
   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。
3. アプリケーションのリストで、起動、停止、または再起動するアプリケーションを選択します。
4. 次のいずれかのボタンをクリックして処理を選択します：
   - **アプリケーションの停止**
     アプリケーションが現在実行されていないと、このボタンは使用できません。
   - **アプリケーションの再開**
     アプリケーションが現在実行されていないと、このボタンは使用できません。
   - **アプリケーションの開始**
     アプリケーションの実行が現在停止されていないと、このボタンは使用できません。

選択した処理に応じて、必要なアプリケーションがクライアントデバイス上で起動、停止、再起動します。

ネットワークエージェントを再起動すると、デバイスと管理サーバーとの現在の接続が失われることを伝えるメッセージが表示されます。

アプリケーションのリモート診断の実行と結果のダウンロード

リモートデバイスでアプリケーションの診断を開始して、結果をダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。
   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。
3. アプリケーションのリストで、リモート診断を実行するアプリケーションを選択します。
   リモート診断オプションのリストが表示されます。
4. ［**診断レポート**］セクションで［**診断を実行**］をクリックします。
   リモート診断が開始され、診断レポートが生成されます。診断が完了すると、［**診断レポートをダウンロード**］が使用可能になります。
5. ［**診断レポートをダウンロード**］をクリックしてレポートをダウンロードします。

レポートが指定した場所にダウンロードされます。

クライアントデバイスでのアプリケーションの実行

場合によっては、テクニカルサポートの担当者の指示に従って、クライアントデバイス上でアプリケーションを実行する必要があります。そのデバイスにアプリケーションをインストールする必要はありません。そのデバイスにアプリケーションをインストールする必要はありません。

クライアントデバイス上でアプリケーションを実行するには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. ［リモート診断］ウィンドウで［**リモートでアプリケーションを実行**］タブを選択します。
3. ［**アプリケーションファイル**］セクションで、［**参照**］をクリックして、クライアントデバイス上で実行するアプリケーションを含む ZIP アーカイブを選択します。

   ZIP アーカイブにはユーティリテフォルダーが含まれている必要があります。このフォルダーには、リモートデバイスで実行する実行ファイルが含まれています。

   必要に応じて、実行ファイル名とコマンドラインの引数を指定できます。これを行うには、**リモートデバイス上で実行されるアーカイブ内の実行ファイル**と［**コマンドラインの引数**］フィールドに入力します。
4. ［**アップロードして実行**］をクリックして、クライアントデバイス上で指定したアプリケーションを実行します。
5. カスペルスキーのサポート担当者の指示に従ってください。

アプリケーションのダンプファイルの生成

アプリケーションダンプファイルを使用すると、ある時点でクライアントデバイスで実行されているアプリケーションのパラメータを表示できます。このファイルには、アプリケーション用にロードされたモジュールに関する情報も含まれています。

ダンプファイルの生成は、Windows ベースのクライアントデバイスで実行されている 32 ビットプロセスでのみ使用可能です。Linux を実行しているクライアントデバイスおよび 64 ビットプロセスの場合、この機能はサポートされていません。

アプリケーションのダンプファイルを生成するには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. ［リモート診断］ウィンドウで［**リモートでアプリケーションを実行**］タブをクリックして選択します。
3. ［**ダンプファイルの生成**］セクションで、ダンプファイルを生成するアプリケーションの実行ファイルを指定します。
4. ［**ダウンロード**］をクリックして、指定したアプリケーションのダンプファイルを保存します。

指定したアプリケーションがクライアントデバイスで実行されていない場合、エラーメッセージが表示されます。

クライアントデバイスのデスクトップへのリモート接続

デバイスにインストールされているネットワークエージェントを使用して、クライアントデバイスのデスクトップへのリモートアクセスを取得できます。ネットワークエージェントを使用したデバイスへのリモート接続は、クライアントデバイスの TCP ポートと UDP ポートが閉じている場合でも可能です。

デバイスとの接続を確立すると、そのデバイスに保存されている情報へのフルアクセス権を取得できます。そのため、そのデバイスにインストールされているアプリケーションを管理することが可能です。

対象の管理対象デバイスのオペレーティングシステム設定でリモート接続を許可する必要があります。たとえば、Windows 10 の場合、このオプションの名前は［**このコンピューターへのリモートアシスタンスの接続を許可する**］です（このオプションを表示するには、［**コントロールパネル**］-［**システムとセキュリティ**］-［**システム**］-［**リモートの設定**］の順に選択します）。脆弱性とパッチ管理機能のライセンスがある場合は、管理対象デバイスへの接続を確立した時に、このオプションを強制的にオンにできます。ライセンスがない場合は、対象の管理対象デバイス上でローカルでオンにします。このオプションをオフにすると、リモート接続を実行できません。

デバイスへのリモート接続を確立するには、2 個のユーティリティが必要です：

- カスペルスキーのユーティリティ klsctunnel：このユーティリティはワークステーションに保管されている必要があります。このユーティリティは、クライアントデバイスと管理サーバー間の接続のトンネリングに使用します。

  Kaspersky Security Center Cloud コンソールでは、管理コンソールから管理サーバーを経由し、次にネットワークエージェントを経由して、管理対象デバイスの指定されたポートに到達する TCP 接続のトンネリングが可能です。トンネリングは、管理コンソールと管理対象デバイスを直接接続できない場合に、管理コンソールがインストールされたデバイスのクライアントアプリケーションを、管理対象デバイスの TCP ポートに接続するように設計されています。

  クライアントデバイスと管理サーバー間のトンネリング接続は、管理サーバーへの接続に使用するポートがデバイスで使用できない場合に必要です。デバイスのポートは、次の場合に利用できないことがあります：

  - リモートデバイスが NAT を使用するローカルネットワークに接続されている。
  - リモートデバイスが管理サーバーのローカルネットワークの一部であるが、ファイアウォールによりポートが閉じられている。

- リモートデスクトップ接続（Microsoft Windows 標準コンポーネント）。リモートデスクトップへの接続は、ユーティリティの設定に従い、Windows の標準のユーティリティ mstsc.exe を使用して確立されます。

  ユーザーの現在のリモートデスクトップのセッションへの接続は、ユーザーが認識することなく確立されます。セッションに接続すると、デバイスのユーザーは、事前の通知なくセッションから切断されます。

クライアントデバイスのデスクトップに接続するには、次の条件のうち 1 つを満たす必要があります。

- クライアントデバイスは、［**管理サーバーから切断しない**］がオンになっているディストリビューションポイントを持つ管理グループのメンバーです。
- クライアントデバイスの設定で、［**管理サーバーから切断しない**］がオンになっています。

  ［**管理サーバーから切断しない**］がオンになっているクライアントデバイスの合計数の上限は 300 です。

クライアントデバイスのデスクトップに接続するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. アクセスを取得するデバイスの名前の横にあるチェックボックスをオンにします。
3. ［**リモートデスクトップに接続**］をクリックします。
   ［リモートデスクトップ（Windows のみ）］ウィンドウが表示されます。
4. ［**ダウンロード**］をクリックして、klsctunnel ユーティリティをダウンロードします。
5. ［**クリップボードへコピー**］をクリックして、テキストフィールドからテキストをコピーします。このテキストは、管理サーバーと管理対象デバイス間の接続を確立するために必要な設定を含む、バイナリラージオブジェクト（BLOB）です。

   BLOB は 3 分間有効です。BLOB の有効期限が切れた場合は、［リモートデスクトップ（Windows のみ）］ウィンドウを再び開いて新しい BLOB を生成します。

6. klsctunnel ユーティリティを実行します。
   ユーティリティウィンドウが開きます。
7. コピーしたテキストをテキストフィールドに貼り付けます。
8. プロキシサーバーを使用する場合は、［**プロキシサーバーを使用する**］をオンにして、プロキシサーバーの接続設定を指定します。
9. ［**ポートを開く**］をクリックします。
   リモートデスクトップ接続のログインウィンドウが開きます。
10. Kaspersky Security Center Cloud コンソールに現在ログインしているアカウントの資格情報を指定します。
11. ［**接続**］をクリックします。

デバイスへの接続が確立されると、Microsoft Windows のリモートデスクトップ接続ウィンドウにデスクトップが表示されます。

Windows デスクトップ共有によるデバイスへの接続

デバイスにインストールされているネットワークエージェントを使用して、クライアントデバイスのデスクトップへのリモートアクセスを取得できます。ネットワークエージェントを使用したデバイスへのリモート接続は、クライアントデバイスの TCP ポートと UDP ポートが閉じている場合でも可能です。

このセッションのユーザーを切断することなく、クライアントデバイスでの既存のセッションに接続することができます。この場合、管理者とデバイスのセッションユーザーが、デスクトップのアクセスを共有します。

デバイスへのリモート接続を確立するには、2 個のユーティリティが必要です：

- カスペルスキーのユーティリティ klsctunnel：このユーティリティはワークステーションに保管されている必要があります。このユーティリティは、クライアントデバイスと管理サーバー間の接続のトンネリングに使用します。

Kaspersky Security Center Cloud コンソールでは、管理コンソールから管理サーバーを経由し、次にネットワークエージェントを経由して、管理対象デバイスの指定されたポートに到達する TCP 接続のトンネリングが可能です。トンネリングは、管理コンソールと管理対象デバイスを直接接続できない場合に、管理コンソールがインストールされたデバイスのクライアントアプリケーションを、管理対象デバイスの TCP ポートに接続するように設計されています。

クライアントデバイスと管理サーバー間のトンネリング接続は、管理サーバーへの接続に使用するポートがデバイスで使用できない場合に必要です。デバイスのポートは、次の場合に利用できないことがあります：

- リモートデバイスが NAT を使用するローカルネットワークに接続されている。
- リモートデバイスが管理サーバーのローカルネットワークの一部であるが、ファイアウォールによりポートが閉じられている。

- Windows デスクトップ共有：リモートデスクトップの既存のセッションに接続する場合、デバイスのセッションユーザーは管理者から接続要求を受信します。デバイスのリモートからの動作とその結果に関する情報は、Kaspersky Security Center Cloud コンソールにより作成されるレポートに保存されません。

  リモートクライアントデバイスでのユーザー操作の監査を設定できます。監査中に、管理者が開いている（または変更している）クライアントデバイスのファイルの情報が保存されます。

Windows デスクトップ共有を使用してクライアントデバイスのデスクトップに接続するには、次の条件を満たす必要があります：

- Microsoft Windows Vista 以降がワークステーションにインストールされている。

  使用する Windows のエディションに Windows デスクトップ共有機能が含まれているかどうかを確認するには、CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} が 32 ビットレジストリに含まれているかどうかを確認します。

- Microsoft Windows Vista 以降の Windows オペレーティングシステムがクライアントデバイスにインストールされている。

- Kaspersky Security Center Cloud コンソールが、脆弱性とパッチ管理ライセンスを使用しています。

- クライアントデバイスは、［**管理サーバーから切断しない**］がオンになっているディストリビューションポイントを持つ管理グループのメンバーであるか、クライアントデバイス設定でこのオプションがオンになっています。

  ［**管理サーバーから切断しない**］がオンになっているクライアントデバイスの合計数の上限は 300 です。

Windows デスクトップ共有を使用してクライアントデバイスのデスクトップに接続するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. アクセスを取得するデバイスの名前の横にあるチェックボックスをオンにします。
3. ［**Windows デスクトップ共有**］をクリックします。

   Windows デスクトップ共有ウィザードが表示されます。
4. ［**ダウンロード**］をクリックして klsctunnel ユーティティをダウンロードし、ダウンロードプロセスが完了するまで待ちます。

   klsctunnel ユーティリティがある場合は、このステップをスキップします。
5. ［**次へ**］をクリックします。
6. 接続するデバイス上のセッションを選択するには、［**次へ**］をクリックします。

7. 対象デバイスで表示されるダイアログで、デスクトップ共有セッションをデバイスのユーザーが許可する必要があります。許可されない場合は、セッションを使用できません。

   デバイスのユーザーがデスクトップ共有セッションを確認すると、ウィザードの次のページが開きます。

8. ［**クリップボードへコピー**］をクリックして、テキストフィールドからテキストをコピーします。このテキストは、管理サーバーと管理対象デバイス間の接続を確立するために必要な設定を含む、バイナリラージオブジェクト（BLOB）です。

   > BLOB は 3 分間有効です。有効期間が終了したら、新しい BLOB を生成してください。

9. klsctunnel ユーティリティを実行します。

   ユーティリティウィンドウが開きます。

10. コピーしたテキストをテキストフィールドに貼り付けます。

11. プロキシサーバーを使用する場合は、［**プロキシサーバーを使用する**］をオンにして、プロキシサーバーの接続設定を指定します。

12. ［**ポートを開く**］をクリックします。

    デスクトップ共有が新しいウィンドウで開始されます。デバイスと対話する場合は、メニューアイコン（  ）をウィンドウの左上でクリックし、［**対話モード**］を選択します。

スマートトレーニングモードでのルールの適用条件

このセクションでは、クライアントデバイス上の Kaspersky Endpoint Security for Windows によるアダプティブアノマリーコントロールルールを使用した検知結果について説明します。

ルールは、クライアントデバイス上の通常と異なるふるまいを検知し、ブロックできます。ルールをスマートトレーニングモードで動作させている場合は、ルールによって異常なふるまいが検知されると、すべての検知について Kaspersky Security Center Cloud コンソール管理サーバーにレポートが送信されます。これらの情報は［**リポジトリ**］フォルダーの［**スマートトレーニングでのルールの適用状況**］サブフォルダーのリストに保存されます。検知結果を適切だとして確認することも、同種のふるまいが異常なふるまいとみなされないように除外として追加することもできます。

検知結果に関する情報は、管理サーバーでイベントログ（他のイベントと同様）と［アダプティブアノマリーコントロール］レポートに保存されます。

アダプティブアノマリーコントロールルールおよびルールのモードとステータスの詳細については、Kaspersky Endpoint Security のヘルプを参照してください。

アダプティブアノマリーコントロールルールを使用した検知のリストの表示

アダプティブアノマリーコントロールルールを使用した検知のリストを表示するには：

1. メインメニューで、［**操作**］→［**リポジトリ**］の順に選択します。

2. ［**スマートトレーニングでのルールの適用状況**］をクリックします。

リストには、アダプティブアノマリーコントロールルールを使用した検知結果について次の情報が表示されます：

- **管理グループ**

  デバイスが属する管理グループの名前

- **デバイス名**

  ルールが適用されたクライアントデバイスの名前

- **名前**

  適用されたルールの名前

- **ステータス**

  除外済み、同期待ち - 管理者がこの項目を処理してルールの除外対象として追加した場合。このステータスは、クライアントデバイスと管理サーバーが次に同期するまで表示されます。同期が完了すると、項目はリストに表示されなくなります。

  確認済み、同期待ち - 管理者がこの項目を処理して確認した場合。このステータスは、クライアントデバイスと管理サーバーが次に同期するまで表示されます。同期が完了すると、項目はリストに表示されなくなります。

  （空白） - 管理者が項目を処理していない場合。

- **ユーザー名**

  検知が発生したプロセスを実行したクライアントデバイスユーザー名

- **処理済み**

  異常が検知された日付。

- **ソースプロセスのパス**

  処理を実行したプロセスであるソースプロセスのパス（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ソースプロセスのハッシュ**

  ソースプロセスファイルの SHA-256 ハッシュ（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ソースオブジェクトのパス**

プロセスを開始したオブジェクトのパス（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ソースオブジェクトのハッシュ**

  ソースファイルの SHA-256 ハッシュ（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ターゲットプロセスのパス**

  ターゲットプロセスのパス（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ターゲットプロセスのハッシュ**

  ターゲットファイルの SHA-256 ハッシュ（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ターゲットオブジェクトのパス**

  ターゲットオブジェクトのパス（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

- **ターゲットオブジェクトのハッシュ**

  ターゲットファイルの SHA-256 ハッシュ（詳しくは、Kaspersky Endpoint Security のヘルプを参照してください）。

各情報要素のプロパティを表示するには：

1. メインメニューで、［**操作**］→［**リポジトリ**］の順に選択します。
2. ［**スマートトレーニングでのルールの適用状況**］をクリックします。
3. 表示されたウィンドウで、目的のオブジェクトを選択します。
4. ［**プロパティ**］をクリックします。

   オブジェクトのプロパティウィンドウが開き、選択した要素に関する情報が表示されます。

アダプティブアノマリーコントロールルールによる検知結果のリストの任意の要素に対して確認または除外への追加を行えます。

対象の要素を確認するには：

検知結果のリストで任意の要素（または複数の要素）を選択して、［**確認**］をクリックします。

対象の要素のステータスが［**確認中**］に変更されます。

確認処理により、ルールで使用される統計が改善されます（詳しくは、Kaspersky Endpoint Security for Windows のヘルプを参照してください）。

要素を除外に追加するには：

検知結果のリストで任意の要素（または複数の要素）を選択して、［**除外**］をクリックします。

除外の追加ウィザードが起動します。ウィザードの指示に従ってください。

対象の要素を確認または拒否すると、クライアントデバイスと管理サーバーの次回の同期後にこの検知結果は検知結果リストから除外され、表示されなくなります。

アダプティブアノマリーコントロールルールから除外に追加

除外の追加ウィザードを使用して、Kaspersky Endpoint Security for Windows のアダプティブアノマリーコントロールルールに除外を追加できます。

アダプティブアノマリーコントロールノードから除外の追加ウィザードを開始するには：

1. メインメニューで、［**操作**］→［**リポジトリ**］→［**スマートトレーニングでのルールの適用状況**］の順に移動します。
2. 表示されるウィンドウで、検知結果のリストで任意の要素（または複数の要素）を選択して、［**除外**］をクリックします。

   1回につき最大1000個の除外を追加できます。上限を超える要素を選択して除外に追加しようとすると、エラーメッセージが表示されます。

除外の追加ウィザードが起動します。

ポリシーとポリシーのプロファイル

Kaspersky Security Center Cloud コンソールを使用して、カスペルスキー製品のポリシーを作成できます。このセクションでは、ポリシーおよびポリシーのプロファイルの概要、作成方法、編集方法を説明しています。

ポリシーについて

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

ポリシーのステータス

ステータス	説明
アク	現在デバイスに適用されているポリシー。各管理グループ内のカスペルスキー製品に対してア

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

ポリシーは、次のルールに従って機能します：

- 1つのアプリケーションに対して、異なる値を持つ複数のポリシーを定義することができます。
- 現在のアプリケーションに対してアクティブにできるポリシーは1つだけです。
- 特定のイベントが発生した時に、非アクティブポリシーを有効化できます。たとえば、ウイルスアウトブレイク中に、より厳格なアンチウイルスによる保護設定を適用することができます。
- ポリシーには子ポリシーを設定できます。

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

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

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

ポリシープロファイルは、次のルールに従って機能します：

- ポリシープロファイルは、特定の有効化条件下で有効になります。
- ポリシープロファイルには、ポリシー設定とは異なる設定値が含まれます。
- ポリシープロファイルを有効化すると、管理対象デバイスの有効な設定が変更されます。
- 1つのポリシーに最大100個のポリシープロファイルを含めることができます。

> 管理サーバーのポリシーは作成できません。

「ロック」属性とロックされた設定の概要

各ポリシー設定には、ロックのアイコン（🔒）があります。次の表は、ロックのステータスを示しています。

ロックのステータス

ステ	説明

ータス	
	設定の横に開いたロックが表示され、切り替えスイッチが無効になっている場合、その設定はポリシーで指定されていません。ユーザーは管理対象アプリケーションのインターフェイスを使用してこれらの設定を変更できます。このような設定を「*ロック解除*」と呼びます。
	設定の横に閉じたロックが表示され、切り替えスイッチが有効になっている場合、その設定はポリシーが適用されるデバイスに適用されます。ユーザーは、管理対象アプリケーションのインターフェイスでこれらの設定の値を変更することはできません。このような設定を「*ロック*」と呼びます。

管理対象デバイスに適用するポリシー設定のロックを閉じておくことを強く推奨します。ロックが解除されたポリシー設定は、管理対象デバイスのカスペルスキーのアプリケーション設定によって再度割り当てられます。

ロックを使用して、次の操作を実行します：

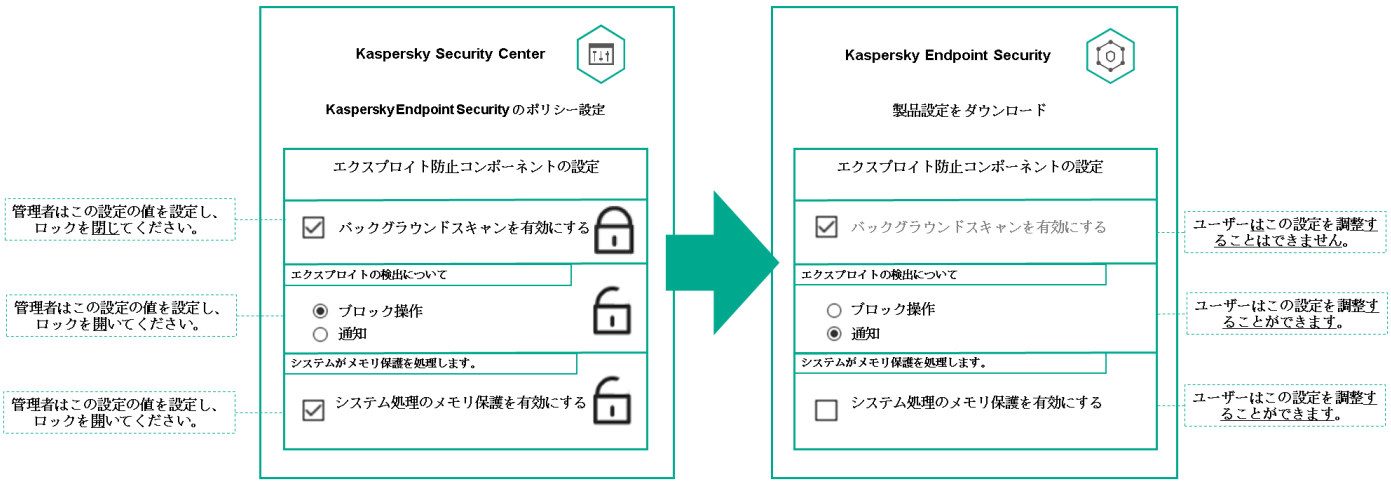
- 管理サブグループのポリシーの設定をロックする
- 管理対象デバイス上のカスペルスキー製品の設定をロックする

したがって、ロックされた設定は、有効な設定を管理対象デバイスに実装するために使用されます。

有効な設定の実装プロセスには、次の操作が含まれます：

- 管理対象デバイスが、カスペルスキー製品の設定値を適用する
- 管理対象デバイスが、ポリシーのロックされた設定の値を適用する

ポリシーおよび管理対象のカスペルスキー製品には、同じ設定内容が含まれています。ポリシー設定を構成すると、管理対象デバイスでカスペルスキー製品設定値が変更されます。管理対象デバイスのロックされた設定をユーザーが調整することはできません（下図を参照）：



ロックとカスペルスキー製品の設定

ポリシーとポリシーのプロファイルの継承

このセクションでは、ポリシーとポリシープロファイルの階層と継承について説明します。

ポリシーの階層

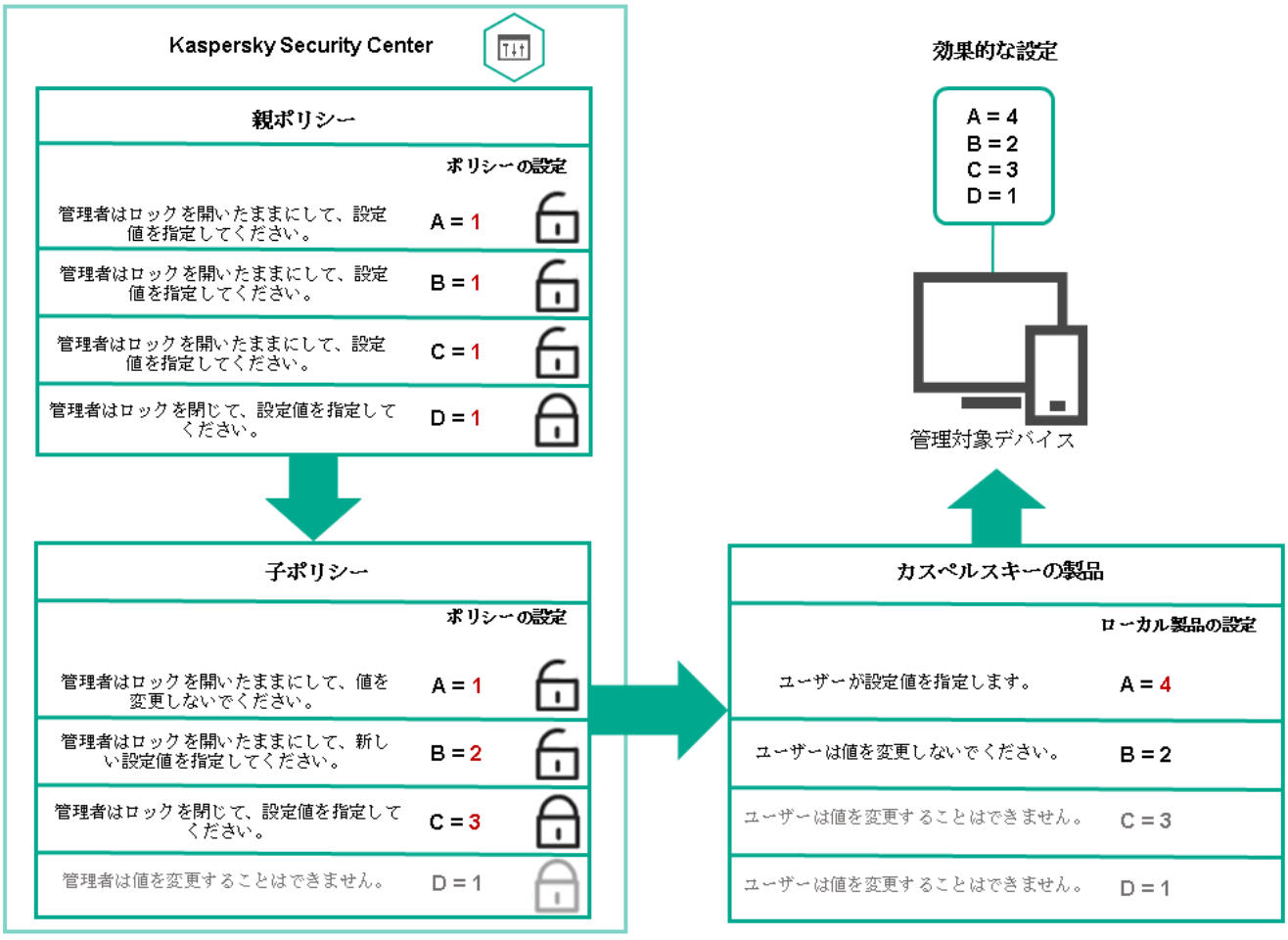
デバイスごとに異なる設定が必要な場合は、デバイスを管理グループに整理できます。

単一の管理グループにポリシーを1つ指定できます。ポリシー設定は*継承できます*。継承とは、上位（親）の管理グループのポリシーからサブグループ（子グループ）にポリシー設定値を受け取ることを意味します。

以降の説明では、親グループで設定されているポリシーを「*親ポリシー*」と表記する場合があります。サブグループ（子グループ）のポリシーを「*子ポリシー*」と表記する場合があります。

既定では、管理サーバーには少なくとも1つの管理対象デバイスグループが存在します。カスタムグループを作成する場合、それらは管理対象デバイスグループ内のサブグループ（子グループ）として作成されます。

同じアプリケーションのポリシーは、管理グループの階層に従って互いに影響を与えます。上位（親）管理グループのポリシーのロック済みの設定は、サブグループのポリシー設定値を再割り当てします（下の図を参照）。

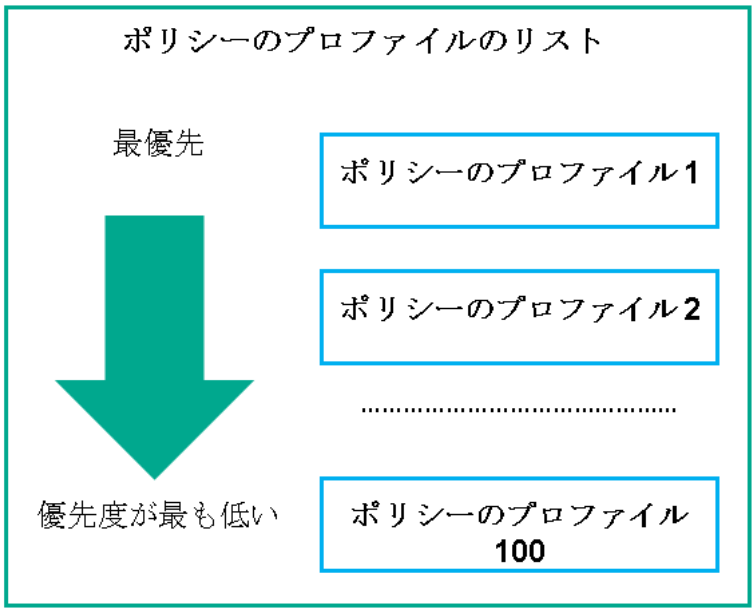


ポリシーの階層

ポリシーの階層内のポリシープロファイル

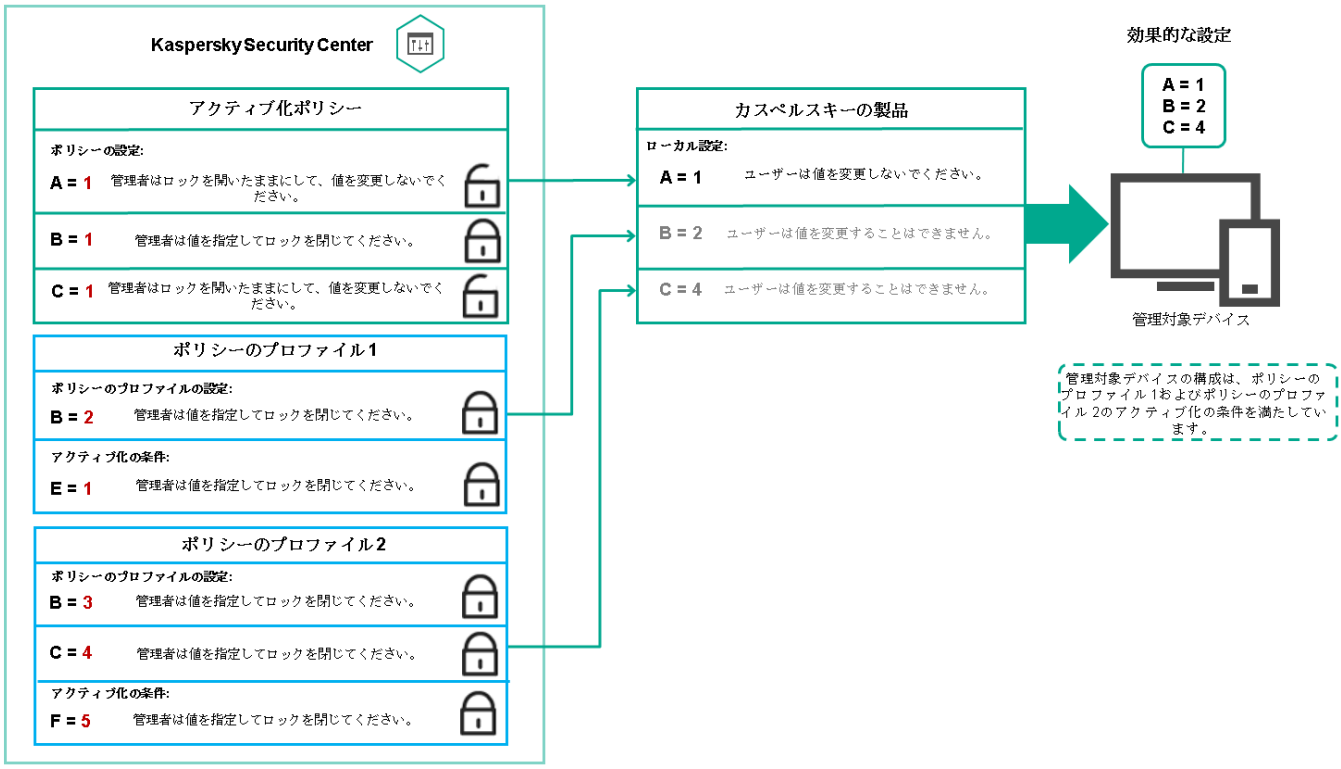
ポリシープロファイルでの優先順位の割り当て条件は次の通りです：

- ポリシープロファイルリスト内のプロファイルの位置は、そのプロファイルの優先度を示します。ポリシーのプロファイルの優先順位を変更できます。リストの一番上にある場合、優先順位が最も高くなります（下の図を参照）。



ポリシープロファイルの優先度の定義

- ポリシープロファイルの有効化条件は相互に依存しません。複数のポリシープロファイルを同時に有効化できます。複数のポリシープロファイルが同じ設定に影響を与える場合、デバイスは最も優先度の高いポリシープロファイルから設定値を取得します（下の図を参照）。

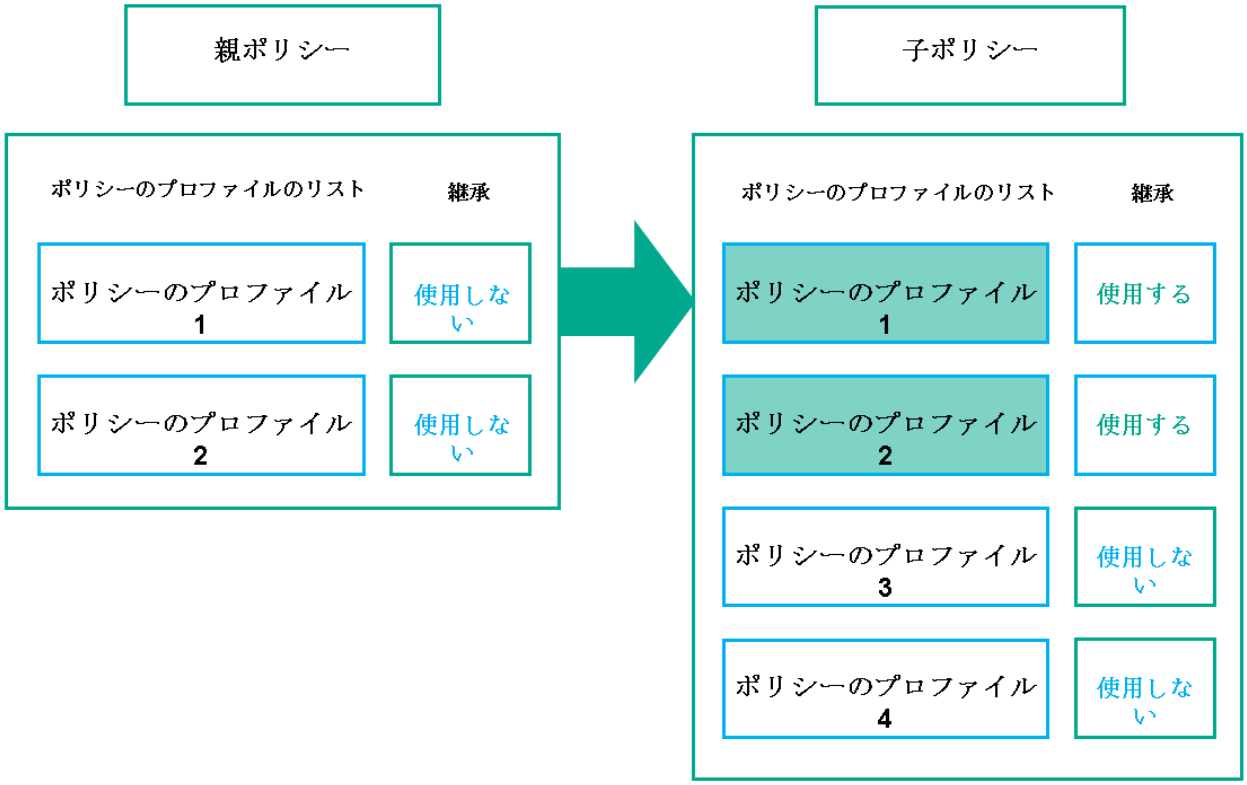


管理対象デバイスの構成が、複数のポリシープロファイルの有効化条件を満たしている

継承の階層におけるポリシープロファイル

様々な階層レベルにあるポリシーのポリシープロファイルは、次の条件を満たします：

- 下位のポリシーは、上位のポリシーからポリシープロファイルを継承します。上位のポリシーから継承されたポリシープロファイルは、元のポリシープロファイルのレベルよりも優先度が高くなります。
- 継承されたポリシープロファイルの優先度を変更することはできません（下の図を参照）。

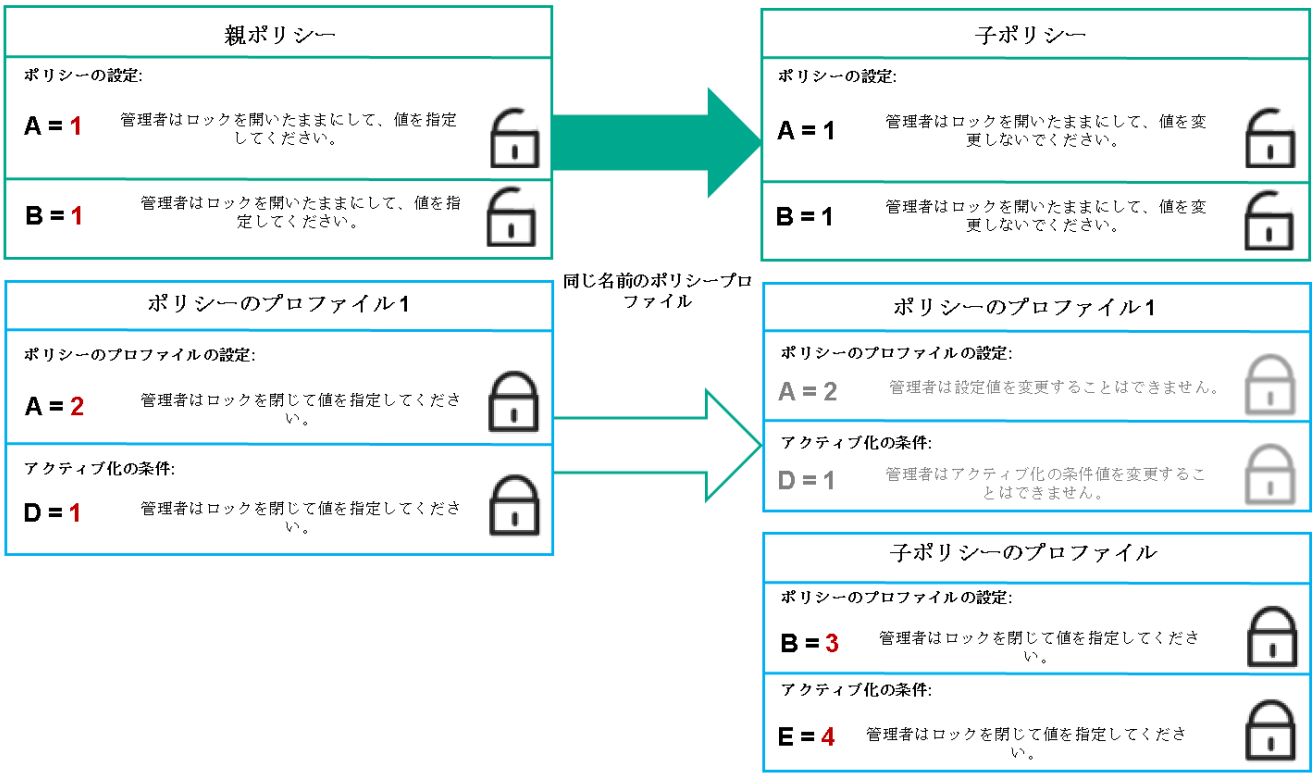


ポリシープロファイルの継承

同じ名前のポリシープロファイル

異なる階層レベルに、同じ名前の 2 つのポリシーがある場合、これらのポリシーは次のルールに従って機能します：

- ロックされた設定および上位のポリシープロファイルのプロファイル有効化条件により、下位のポリシープロファイルの設定およびプロファイル有効化条件が変更されます（下図を参照）。



子プロファイルは親ポリシープロファイルから設定値を継承する

- ロック解除された設定および上位のポリシープロファイルのプロファイル有効化条件により、下位のポリシープロファイルの設定およびプロファイル有効化条件が変更されません。

管理対象デバイスに設定が実装される方法

管理対象デバイスでの有効な設定の実装は、次のように説明できます：

- ロックされていないすべての設定の値は、有効なポリシーから取得されます。
- 次に、管理対象アプリケーション設定の値で上書きされます。
- 次に、有効なポリシーのロックされた設定値が適用されます。ロックされた設定値は、ロックされていない有効な設定値を変更します。

ポリシーの管理

このセクションでは、ポリシーの管理について説明します。ポリシーのリストの表示、ポリシーの作成、ポリシーの変更、ポリシーのコピー、ポリシーの移動、強制同期、ポリシー導入ステータス図の表示、およびポリシーの削除に関する情報を提供します。

ポリシーのリストの表示

管理サーバーまたは任意の管理グループを対象に作成されたポリシーのリストを表示できます。

ポリシーのリストを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. 管理グループのリストで、ポリシーのリストを表示する管理グループを選択します。

ポリシーのリストが表形式で表示されます。ポリシーが存在しない場合、表は空です。表の列の表示と非表示の切り替え、列の順序の変更、指定した値を含む行のみの表示、検索の使用などを実行できます。

ポリシーの作成

ポリシーの作成と、既存のポリシーの変更と削除を行うことができます。

管理サーバーのポリシーは作成できません。

ポリシーを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. ［**追加**］をクリックします。
   ［**アプリケーションの選択**］ウィンドウが表示されます。
3. ポリシーを作成するアプリケーションを選択します。
4. ［**次へ**］をクリックします。
   新規ポリシーの設定ウィンドウの［**全般**］タブが表示されます。
5. 必要に応じて、ポリシーの既定の名前、ステータス、継承設定を変更します。
6. ［**アプリケーション設定**］タブをクリックします。
   あるいは、［**保存**］をクリックして作成を完了します。ポリシーのリストに新しいポリシーが表示されます。ポリシーの設定は後で編集できます。
7. ［**アプリケーション設定**］タブの左側のペインで目的のカテゴリを選択し、右側の結果ペインでポリシーの設定を編集します。ポリシーの各カテゴリ（セクション）の設定を編集できます。
   作成するポリシーの対象となるアプリケーションに応じて、設定可能なアプリケーション設定は異なります。詳細は、次を参照してください：
   - 管理サーバーの設定
   - ネットワークエージェントのポリシー設定
   - Kaspersky Endpoint Security for Windows のヘルプ
   その他のカスペルスキー製品の設定の詳細については、該当する製品のヘルプまたはガイドを参照してください。
   設定の編集時、［**キャンセル**］をクリックすると、最後に行った操作を取り消すことができます。
8. ［**保存**］をクリックしてポリシーを保存します。

ポリシーのリストに新しいポリシーが表示されます。

ポリシーの変更

ポリシーを変更するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. 変更するポリシーを選択します：
   ポリシーの設定ウィンドウが表示されます。
3. 作成するポリシーの一般設定とアプリケーションの設定を指定します。詳細については、次を参照してください：
   - 管理サーバーの設定
   - ネットワークエージェントのポリシー設定
   - Kaspersky Endpoint Security for Windows のヘルプ
   その他のカスペルスキー製品の設定の詳細については、該当する製品のヘルプまたはガイドを参照してください。
4. ［**保存**］をクリックします。

ポリシーに加えた変更は、ポリシーのプロパティに保存され、［**変更履歴**］セクションに表示されます。

ポリシーの全般的な設定

全般

［**全般**］タブでは、ポリシーステータスを変更したり、継承ポリシーを設定したりすることができます：

- ［**ポリシーのステータス**］セクションで、ポリシーのステータスを選択します：
  - **アクティブ**
  - **モバイルユーザー**
    このオプションをオンにすると、デバイスが企業ネットワークから離れるとポリシーがアクティブになります。
  - **非アクティブ**
    このオプションをオンにすると、ポリシーは非アクティブになりますが［**ポリシー**］フォルダーに保持されます。必要に応じて、ポリシーをアクティブにすることができます。

- ［**設定の継承**］セクションでは、ポリシーの継承を設定できます。
  - **親ポリシーから設定を継承する**

    このオプションをオンにすると、ポリシーの設定値は上位レベルグループのポリシーから継承されるため、ロックされます。

    既定では、このオプションはオンです。

  - **設定を子ポリシーへ強制的に継承させる**

    このオプションをオンにすると、ポリシーの変更を適用した後に次の処理が実行されます：
    - 管理サブグループのポリシー（子ポリシー）に、ポリシーの設定値が継承されます。
    - 各子ポリシーのプロパティウィンドウの［**全般**］セクションにある［**設定の継承**］ブロックで、［**親ポリシーから設定を継承する**］が自動的にオンになります。

    このオプションをオンにすると、子ポリシーの設定はロックされます。

    既定では、このオプションはオフです。

イベントの設定

［**イベントの設定**］タブでは、イベントの記録と通知を設定できます。イベントは、重要度に応じて次のタブに分類されます：

- **緊急**

  ［**緊急**］セクションは、ネットワークエージェントのポリシーのプロパティに表示されません。
- **機能エラー**
- **警告**
- **情報**

それぞれのセクションのリストには、イベントの種別と、管理サーバーでイベントが保存される既定の日数が表示されます。イベントの種別をクリックすると、次の設定を指定できます：

- **イベント登録**

  イベントの保存期間を指定し、保存場所を選択できます：
  - **管理サーバーのデータベースに保存（日）**
  - **デバイスの OS イベントログに保存**
- **イベント通知**

  イベントについてメールで通知を受け取るかどうかを選択できます。

  既定では、通知に利用する設定（受信アドレスなど）は、管理サーバーのプロパティで指定された設定を使用します。必要に応じて、これらの設定を［**メール**］タブで変更できます。

変更履歴

［**変更履歴**］タブでは、必要に応じて、ポリシーのリビジョンのリストを表示したり、ポリシーで行われた変更をロールバックすることができます。

ポリシー継承オプションの有効化と無効化

ポリシーで継承オプションを有効または無効にするには：

1. 必要なポリシーを開きます。
2. ［**全般**］タブを開きます。
3. ポリシーの継承をオンまたはオフにします。
   - 子ポリシーで［**親ポリシーから設定を継承する**］をオンにし、管理者が親ポリシーの設定の一部をロック状態にすると、子ポリシーでこれらの設定を変更することはできません。
   - 子ポリシーで［**親ポリシーから設定を継承する**］をオフにすると、親ポリシーでロック状態の設定も含めて、子ポリシー側ですべての設定を変更できます。
   - 親グループで［**設定を子ポリシーへ強制的に継承させる**］をオンにすると、各子ポリシーで［**親ポリシーから設定を継承する**］がオンになります。この場合、子ポリシーの側でこのオプションをオフにすることはできません。親ポリシーでロックされている設定はすべて強制的に子ポリシーに継承され、子グループ側でこれらの設定を変更することはできません。
4. ［**保存**］ボタンをクリックして変更を保存するか、［**キャンセル**］ボタンをクリックして変更を破棄します。

既定では、新規に作成したポリシーでは［**親ポリシーから設定を継承する**］はオンです。

ポリシーにポリシープロファイルが存在する場合、子ポリシーでもこれらのプロファイルが継承されます。

ポリシーのコピー

ポリシーを任意の管理グループから別の管理グループにコピーできます。

ポリシーを別の管理グループにコピーするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. コピーするポリシーに隣接するチェックボックスをオンにします。
3. ［**コピー**］をクリックします。
   画面の右側に管理グループのツリーが表示されます。
4. ツリーで、ポリシーのコピー先となるグループ（ターゲットグループ）を選択します。
5. ページの一番下にある［**コピー**］をクリックします。
6. ［**OK**］をクリックして処理内容を確定します。

すべてのプロファイルと合わせてターゲットグループにポリシーのコピーが作成されます。ターゲットグループにコピーして作成したポリシーのステータスは［**非アクティブ**］です。いつでもステータスを［**アクティブ**］に変更できます。

新たに移動されるポリシー名と同じ名前のポリシーがターゲットグループに既に存在している場合、新たに移動されるポリシー名に、たとえば (1)、(2) のようなインデックス「(<次の連番>)」が追加されます。

ポリシーの移動

ポリシーを任意の管理グループから別の管理グループに移動できます。たとえば、削除したいグループがあるが、そのグループのポリシーは別のグループで使用したいとします。その場合、グループを削除する前に、ポリシーを別のグループに移動できます。

ポリシーを別の管理グループに移動するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. 移動するポリシーに隣接するチェックボックスをオンにします。
3. ［**移動**］をクリックします。
   画面の右側に管理グループのツリーが表示されます。
4. ツリーで、ポリシーの移動先となるグループ（ターゲットグループ）を選択します。
5. ページの一番下にある［**移動**］をクリックします。
6. ［OK］をクリックして処理内容を確定します。

ポリシーがソースグループから継承されていない場合、ポリシーはすべてのプロファイルと合わせてターゲットグループに（コピーではなく）移動されます。ターゲットグループに作成したポリシーのステータスは［**非アクティブ**］です。いつでもステータスを［**アクティブ**］に変更できます。

ポリシーがソースグループから継承されている場合、ポリシーは元のグループにも残ります。そして、すべてのプロファイルと合わせてターゲットグループにコピーが作成されます。ターゲットグループに作成したポリシーのステータスは［**非アクティブ**］です。いつでもステータスを［**アクティブ**］に変更できます。

新たに移動されるポリシー名と同じ名前のポリシーがターゲットグループに既に存在している場合、新たに移動されるポリシー名に、たとえば (1)、(2) のようなインデックス「(<次の連番>)」が追加されます。

ポリシーのエクスポート

Kaspersky Security Center Cloud コンソールを使用すると、ポリシーとその設定、ポリシープロファイルを KLP ファイルに保存できます。この KLP ファイルを使用して、Kaspersky Security Center Windows と Kaspersky Security Center Linux の両方に保存したポリシーをインポートできます。

ポリシーをエクスポートするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. エクスポートするポリシーの横のチェックボックスをオンにします。

複数のポリシーを同時にエクスポートすることはできません。複数のポリシーを選択すると、［**エクスポート**］が無効になります。

3. ［**エクスポート**］をクリックします。

4. 表示される［**名前を付けて保存**］ウィンドウで、ポリシーファイルの名前とパスを指定します。［**保存**］をクリックします。

   ［**名前を付けて保存**］ウィンドウは、Google Chrome、Microsoft Edge、または Opera を使用している場合にのみ表示されます。別のブラウザーを使用する場合、ポリシーファイルは自動的に［**Downloads**］フォルダーに保存されます。

ポリシーのインポート

Kaspersky Security Center Cloud コンソールを使用すると、KLP ファイルからポリシーをインポートできます。KLP ファイルには、エクスポートされたポリシー、その設定、およびポリシープロファイルが含まれています。

ポリシーをインポートするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. ［**インポート**］をクリックします。

3. ［**参照**］をクリックして、インポートするポリシーファイルを選択します。

4. 表示されたウィンドウで、KLP ポリシーファイルのパスを指定し、［**開く**］をクリックします。選択できるポリシーファイルは 1 つだけです。

   ポリシーの処理が始まります。

5. ポリシーが正常に処理されたら、ポリシーを適用する管理グループを選択します。

6. ［**完了**］をクリックしてポリシーのインポートを完了します。

インポート結果の通知が表示されます。ポリシーが正常にインポートされた場合は、［**詳細**］をクリックして、ポリシーのプロパティを表示できます。

インポートが成功すると、ポリシーがポリシーリストに表示されます。ポリシーの設定とプロファイルもインポートされます。エクスポート中に選択されたポリシーステータスにかかわらず、インポートされたポリシーは非アクティブです。ポリシーのプロパティでポリシーステータスを変更できます。

新しくインポートされたポリシーと同じ名前のポリシーが既に存在している場合、インポートされたポリシーの名前に、たとえば **(1)**、**(2)** のようなインデックス「**(<次の連番>)**」が付きます。

ポリシー導入ステータス図の表示

Kaspersky Security Center Cloud コンソールでは、各デバイスのポリシー適用のステータスをポリシー導入ステータス図で表示できます。

各デバイスのポリシー導入ステータスを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. デバイスの導入ステータスを表示するポリシーの名前に隣接するチェックボックスをオンにします。
3. 表示されたメニューで、［**導入**］をクリックします。
   ［**<ポリシー名> 導入結果**］ウィンドウが開きます。
4. 開いた［**<ポリシー名> 導入結果**］ウィンドウに、**ステータスの説明（使用可能な場合）**の説明が表示されます。

ポリシーの導入結果のリストに表示されるデバイス数を変更できます。推奨されるデバイス数の上限は、100,000 台です。

ポリシーの導入結果のリストに表示されるデバイスの数を変更するには：

1. メインメニューで、アカウント設定に移動して、［**インターフェイスのオプション**］をオンにします。
2. ［**ポリシーの導入結果に表示するデバイス台数の上限**］に、デバイスの数（最大 100,000）を入力します。
   既定では、この数は 5,000 です。
3. ［**保存**］をクリックします。

設定が保存され、適用されます。

［ウイルスアウトブレイク］イベント発生時におけるポリシーの自動アクティブ化

［ウイルスアウトブレイク］イベント発生時にポリシーの自動アクティベーションを実行するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウの［**全般**］タブが表示されます。
2. ［**ウイルスアウトブレイク**］セクションを選択します。
3. 右側のペインで、［［**ウイルスアウトブレイク］イベント発生時にアクティブ化するポリシーの設定**］をクリックします。
   ［**ポリシーのアクティブ化**］ウィンドウが表示されます。
4. ウイルスアウトブレイクを検知するコンポーネントの対象領域ごとに（ワークステーションおよびファイルサーバー向けアンチウイルス製品、メールサーバー向けアンチウイルス製品、境界防御向けアンチウイルス製品）、［**追加**］をクリックします。
   ［**管理対象デバイス**］管理グループウィンドウが表示されます。
5. ［**管理対象デバイス**］の横にあるアイコン（）をクリックします。
   管理グループの階層とそれぞれの管理グループのポリシーが表示されます。
6. 管理グループの階層とポリシーから、ウイルスアウトブレイクの検知時にアクティブにするポリシーを選択します。
   1つのグループのすべてのポリシーを有効にする場合は、該当するグループ名の横のチェックボックスをオンにします。

7. ［**保存**］をクリックします。

   管理グループの階層とポリシーのウィンドウが閉じます。

選択したポリシーが、ウイルスアウトブレイクの検知時にアクティブ化されるポリシーのリストに追加されます。選択したポリシーは、その時点でアクティブか非アクティブかに関係なく、ウイルスアウトブレイクの発生時にアクティブになります。

［ウイルスアウトブレイク］イベントでポリシーがアクティブ化された場合は、手動モードを使用することによってのみ前のポリシーに戻ることができます。

強制同期

Kaspersky Security Center Cloud コンソールでは、管理対象デバイスのステータス、設定、タスク、ポリシーは自動的に同期されます。定められた時点で、特定のデバイスで同期が実行されているかどうかを正確に把握する必要がある場合があります。

単一デバイスの同期

管理サーバーと管理対象デバイスの同期を強制的に実行するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
2. 管理サーバーと同期させるデバイスの名前をクリックします。

   プロパティウィンドウの［**全般**］セクションが表示されます。
3. ［**強制同期**］をクリックします。

   指定したデバイスと管理サーバーの同期が実行されます。

複数デバイスの同期

管理サーバーと複数の管理対象デバイスの同期を強制的に実行するには：

1. 管理グループまたはデバイスの抽出からデバイスリストを開きます：
   - メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］→［**グループ**］の順に選択して、同期するデバイスを含んだ管理グループを選択します。
   - デバイスの抽出を実行してデバイスリストを表示します。
2. 管理サーバーと同期するデバイスに隣接するチェックボックスをオンにします。
3. ［**強制同期**］をクリックします。

   指定したデバイスと管理サーバーの同期が実行されます。
4. デバイスリストで、指定したデバイスでの前回の管理サーバーへの接続の時間が現在の時間に変更されていることが確認できます。時間が変更されていない場合は、［**更新**］をクリックしてページの内容を更新します。

選択したデバイスのデータが管理サーバーと同期します。

ポリシーの配信時間の表示

管理サーバーでカスペルスキー製品のポリシーを変更した後、変更後のポリシーが特定の管理対象デバイスに配信されたかどうかを確認できます。ポリシーは、定期的な同期または強制的な同期によって配信されます。

管理対象デバイスに製品ポリシーが配信された日時を表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
2. 管理サーバーと同期させるデバイスの名前をクリックします。
   プロパティウィンドウの［**全般**］セクションが表示されます。
3. ［**アプリケーション**］タブをクリックします。
4. ポリシーを同期した日時を表示する製品を選択します。

   製品ポリシーのプロパティウィンドウの［**全般**］セクションが表示され、ポリシーの配信日時を確認できます。

ポリシーの削除

必要ないポリシーは削除できます。ただし、削除できるのは上位のグループから継承されたのではないポリシーのみです。上位のグループから継承されたポリシーは、そのポリシーが作成された上位のグループでのみ削除できます。

ポリシーを削除するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. 削除するポリシーの横のチェックボックスをオンにし、［**削除**］をクリックします。
   上位のポリシーから設定を継承したポリシーを選択した場合、［**削除**］はグレーアウトされ選択できなくなります。
3. ［**OK**］をクリックして処理内容を確定します。

   ポリシーとそのすべてのプロファイルが削除されます。

ポリシーのプロファイルの管理

このセクションでは、ポリシープロファイルの管理について説明します。ポリシーのプロファイルの表示、ポリシープロファイルの優先度の変更、ポリシープロファイルの作成、ポリシープロファイルの変更、ポリシープロファイルのコピー、ポリシープロファイルの有効化ルールの作成、およびポリシープロファイルの削除に関する情報を提供します。

ポリシーのプロファイルの表示

ポリシーのプロファイルを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. プロファイルを表示するポリシーの名前をクリックします：
   ポリシーのプロパティウィンドウの［**全般**］タブが表示されます。
3. ［**ポリシーのプロファイル**］タブを開きます。

ポリシーのプロファイルのリストが表形式で表示されます。ポリシーにプロファイルが設定されていない場合、表は空です。

ポリシーのプロファイルの優先順位の変更

ポリシーのプロファイルの優先順位を変更するには：

1. 目的のポリシーのプロファイルのリストに移動します。
   ポリシーのプロファイルのリストが表示されます。
2. ［**ポリシーのプロファイル**］タブで、優先度を変更するポリシープロファイルの横にあるチェックボックスをオンにします。
3. ［**優先度を高く設定**］または［**優先度を低く設定**］をクリックして、ポリシープロファイルの新しい位置を指定します。
   リスト内でポリシーの位置が上にあるほど、優先度も高くなります。
4. ［**保存**］をクリックします。

選択したポリシーのプロファイルの優先順位が変更され、適用されます。

ポリシーのプロファイルの作成

ポリシーのプロファイルを作成するには：

1. 目的のポリシーのプロファイルのリストに移動します。
   ポリシーのプロファイルのリストが表示されます。ポリシーにプロファイルが設定されていない場合、表は空です。
2. ［**追加**］をクリックします。
3. 必要に応じて、プロファイルの既定の名前と継承設定を変更します。
4. ［**アプリケーション設定**］タブを選択します。

または、［**保存**］をクリックして完了します。ポリシープロファイルのリストに作成したプロファイルが表示されます。プロファイルの設定は後で編集できます。

5. ［**アプリケーション設定**］タブの左側のペインで目的のカテゴリを選択し、右側の結果ペインでプロファイルの設定を編集します。ポリシーのプロファイルの各カテゴリ（セクション）の設定を編集できます。

   設定の編集時、［**キャンセル**］をクリックすると、最後に行った操作を取り消すことができます。

6. ［**保存**］をクリックしてプロファイルを保存します。

ポリシーのプロファイルのリストに新しいプロファイルが表示されます。

ポリシーのプロファイルの編集

ポリシーのプロファイルの編集機能は、Kaspersky Endpoint Security for Windows のポリシーにのみ使用可能です。

ポリシーのプロファイルを変更するには：

1. 目的のポリシーのプロファイルのリストに移動します。

   ポリシーのプロファイルのリストが表示されます。

2. ［**ポリシーのプロファイル**］タブで、変更するポリシープロファイルをクリックします。

   ポリシーのプロファイルのプロパティウィンドウが開きます。

3. プロパティウィンドウでプロファイルを設定します。

   - 必要に応じて、［**全般**］タブでプロファイル名を変更したり、プロファイルを有効または無効にします。
   - プロファイルの有効化ルールを編集します。
   - アプリケーション設定を編集します。

   カスペルスキー製品の設定の詳細については、該当する製品のヘルプまたはガイドを参照してください。

4. ［**保存**］をクリックします。

デバイスが管理サーバーと同期した後（ポリシーのプロファイルが有効な場合）、または有効化ルールが適合した時（ポリシーのプロファイルが無効な場合）、変更した設定が有効になります。

ポリシーのプロファイルのコピー

ポリシーのプロファイルを現在の割り当て先のポリシーや別のポリシーにコピーして、同じポリシーを別のポリシーで使用できます。また、プロファイルのコピー機能は、一部の設定だけが異なる複数のプロファイルを作成する場合にも活用できます。

ポリシーのプロファイルをコピーするには：

1. 目的のポリシーのプロファイルのリストに移動します。
   ポリシーのプロファイルのリストが表示されます。ポリシーにプロファイルが設定されていない場合、表は空です。
2. ［**ポリシーのプロファイル**］タブで、コピーするポリシープロファイルを選択します。
3. ［**コピー**］をクリックします。
4. 表示されるウィンドウで、プロファイルのコピー先にするポリシーを選択します。
   ポリシーのプロファイルを、現在割り当てられているのと同じポリシーまたは指定した別のポリシーにコピーできます。
5. ［**コピー**］をクリックします。

ポリシーのプロファイルが指定したポリシーにコピーされます。コピーして作成された新しいプロファイルには、最も低い優先度が設定されます。プロファイルを現在割り当てられているのと同じポリシーにコピーした場合、プロファイル名に (1)、(2) のようなインデックス「<数字>」が追加されます。

コピーの完了後、プロファイル名や優先度も含めてプロファイルの設定を変更できます。この変更によりコピー元のプロファイルが影響を受けることはありません。

ポリシーのプロファイルの有効化ルールの作成

ポリシーのプロファイルの有効化ルールを作成するには：

1. 目的のポリシーのプロファイルのリストに移動します。
   ポリシーのプロファイルのリストが表示されます。
2. ［**ポリシーのプロファイル**］タブで、有効化ルールを作成するポリシープロファイルをクリックします。
   ポリシープロファイルのリストが空の場合は、ポリシーのプロファイルを作成できます。
3. ［**有効化ルール**］タブで、［**追加**］をクリックします。
   ポリシーのプロファイルの有効化ルールのウィンドウが表示されます。
4. ルールの名前を入力します。
5. 作成しているポリシープロファイルの有効化に作用する条件の横にあるチェックボックスをオンにします：

   - **ポリシープロファイルの有効化に対する全般ルール**

     このチェックボックスをオンにすると、デバイスのオフラインモードのステータス、管理サーバーへの接続ルール、デバイスに割り当てられているタグに応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

     このオプションでは、次の項目を設定できます：

     - **デバイスのステータス**

ネットワーク内にデバイスが存在するかどうかを指定します：

- **オンライン** - デバイスはネットワーク内にあるため、管理サーバーを使用できます。
- **オフライン** - デバイスは外部ネットワーク内にあるため、管理サーバーは使用できません。
- **該当なし** - 基準は適用されません。

- **管理サーバー接続のルールがこのデバイスでアクティブです**

  ポリシーのプロファイルを有効化する条件（ルールを実行する条件）を選択し、ルールの名前を指定します。

  ルールでは、管理サーバーへの接続に関するデバイスのネットワークロケーションを指定します。ポリシープロファイルを有効にするためにネットワークロケーションの説明の条件を満たす（または満たさない）必要があります。

  管理サーバーへの接続に関するデバイスのネットワークロケーションの説明は、ネットワークエージェント切り替えルールで作成または設定できます。

- **特定のデバイス所有者向けのルール**

  このオプションでは、次の項目を設定できます：

  - **デバイスの所有者**

    このオプションをオンにして、デバイスの所有者に応じたプロファイルの有効化ルールを設定を有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

    - デバイスが特定の所有者のものである（「=」記号）
    - デバイスが特定の所有者のものでない（「≠」記号）

      ユーザーリストはフィルタリングされており、内部ユーザーであるデバイスの所有者が表示されることに注意してください。

      このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。このオプションをオンにすると、デバイスの所有者を指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

  - **デバイスの所有者が属する内部セキュリティグループ**

このオプションをオンにして、デバイスの所有者の Kaspersky Security Center Cloud コンソールの内部セキュリティグループの所属に応じたプロファイルの有効化ルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

- デバイスの所有者が特定のセキュリティグループのメンバーである（「=」記号）
- デバイスの所有者が特定のセキュリティグループのメンバーでない（「≠」記号）

  ユーザーリストはフィルタリングされており、内部ユーザーであるデバイスの所有者が表示されることに注意してください。

  このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。Kaspersky Security Center Cloud コンソールのセキュリティグループを指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **ハードウェアの仕様のルール**

  このチェックボックスをオンにすると、メモリサイズと論理プロセッサの数に応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

  このオプションでは、次の項目を設定できます：

  - **RAM サイズ（MB）**

    このオプションをオンにして、デバイスで使用可能な RAM サイズに応じたプロファイルの有効化のルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

    - デバイスの RAM サイズは指定された値以下である（「<」記号）。
    - デバイスの RAM サイズは指定された値以上である（「>」記号）。

    このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。デバイスの RAM ボリュームを指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

  - **論理プロセッサの数**

    このオプションをオンにして、デバイスの論理プロセッサの数に応じたプロファイルの有効化ルールを有効にします。このチェックボックスの下のドロップダウンリストで、プロファイルの有効化の基準を選択できます：

    - デバイスの論理プロセッサの数は指定された値以下である（「<」記号）。
    - デバイスの論理プロセッサの数は指定された値以上である（「>」記号）。

    このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。デバイス上の論理プロセッサの数を指定できます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **ロールの割り当てルール**

  このオプションでは、次の項目を設定できます：

  デバイス所有者のロールに応じてポリシープロファイルを有効化する

このオプションをオンにすると、デバイスの所有者のロールに応じたプロファイルの有効化ルールを設定し、オンにすることができます。既存のロールのリストからロールを手動で選択して追加します。

このオプションをオンにすると、設定された基準に従ってデバイス上でプロファイルが有効化されます。

- **タグの使用ルール**

  このチェックボックスをオンにすると、デバイスに割り当てられたタグに応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。選択したタグが割り当てられているデバイスまたは割り当てられていないデバイスのいずれかで、ポリシーのプロファイルを有効にできます。

  このオプションでは、次の項目を設定できます：

  - **タグ**

    このタグのリストで、目的のタグのチェックボックスをオンにすると、ポリシーのプロファイルにデバイスを含めるためのルールを指定できます。

    リストの上のフィールドに新しいタグを入力して、［**追加**］をクリックすると、新しいタグをリストに追加できます。

    選択したタグのすべてを説明に含むデバイスがポリシーのプロファイルに含まれます。チェックボックスをオフにすると、基準は適用されません。既定では、これらのチェックボックスはオフです。

  - **指定したタグのないデバイスに適用する**

    タグの選択状態を反転させる必要がある場合は、このオプションをオンにします。

    このオプションをオンにすると、選択されたタグのいずれも説明に含まないデバイスがポリシープロファイルに含まれます。このオプションをオフにすると、基準が適用されません。

    既定では、このオプションはオフです。

- **Active Directory 使用のルール**

  このチェックボックスをオンにすると、Active Directory 組織単位（OU）内にデバイスが属しているか、または Active Directory セキュリティグループにデバイス（またはその所有者）が属しているかに応じて、デバイス上でポリシープロファイルの有効化ルールを設定できます。

  このオプションでは、次の項目を設定できます：

  - **Active Directory セキュリティグループのデバイス所有者メンバーシップ**

    このオプションを有効にすると、所有者が指定されたセキュリティグループに所属しているデバイスで、ポリシーのプロファイルが有効化されます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

  - **デバイスが属している Active Directory セキュリティグループ**

このオプションを有効にすると、デバイスでポリシープロファイルが有効化されます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。既定では、このオプションはオフです。

- **デバイスが割り当てられている Active Directory 組織単位**

  このオプションを有効にすると、指定された Active Directory 組織単位（OU）に属するデバイスで、ポリシーのプロファイルが有効化されます。このオプションをオフにすると、プロファイルの有効化の基準は適用されません。

  既定では、このオプションはオフです。

ウィザードで表示されるウィンドウ数は、最初のステップで選択した設定によります。ポリシープロファイルの有効化ルールは後で変更することができます。

6. 設定したパラメータのリストを確認します。リストのパラメータが正しいことが確認できたら、［**作成**］をクリックします。

プロファイルが保存されます。プロファイルは、有効化ルールが適合すると、デバイスで有効になります。

プロファイル用に作成したポリシープロファイルの有効化ルールが、［**有効化ルール**］タブのポリシープロファイルのプロパティに表示されます。ポリシープロファイルの有効化ルールはいずでも変更または削除することができます。

複数の有効化ルールを同時に適合させることができます。

ポリシーのプロファイルの削除

ポリシーのプロファイルを削除するには：

1. 目的のポリシーのプロファイルのリストに移動します。

   ポリシーのプロファイルのリストが表示されます。

2. ［**ポリシーのプロファイル**］タブで、削除するポリシープロファイルに隣接するチェックボックスをオンにし、［**削除**］をクリックします。

3. 表示されるウィンドウで、もう一度［**削除**］をクリックします。

ポリシープロファイルが削除されます。下位のグループでこのポリシーが継承されている場合、該当する下位のグループでプロファイルが維持されますが、プロファイルの所属先がこの下位のグループのポリシーに変更されます。この処理は、下位グループのデバイスにインストールされている管理対象製品の設定が大幅に変更されてしまわないようにするために実装されています。

データ暗号化と保護機能

データ暗号化により、ノート PC やハードディスクの盗難や紛失、不正なユーザーやアプリケーションによるアクセスなどによる思いがけない情報漏洩の危険性を低減できます。

以下のカスペルスキー製品が暗号化をサポートします：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

ユーザーインターフェイス設定を使用して、暗号化管理の機能に関連するインターフェイス要素の一部を表示または非表示にすることができます。

Kaspersky Endpoint Security for Windows でのデータ暗号化

サーバーまたはワークステーション用の Windows オペレーティングシステムを実行しているデバイスで、BitLocker ドライブ暗号化テクノロジーを管理できます。

Kaspersky Endpoint Security for Windows のこれらのコンポーネントを使用すると、暗号化を有効または無効にする、暗号化されたドライブのリストを表示する、暗号化に関するレポートを生成して表示する、などの操作を実行できます。

Kaspersky Security Center Cloud コンソールで Kaspersky Endpoint Security for Windows のポリシーを設定することで、暗号化の設定を編集できます。Kaspersky Endpoint Security for Windows は、アクティブなポリシーに基づいて、暗号化と復号化を実行します。ルールの編集方法と暗号化機能の詳細については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

Kaspersky Endpoint Security for Mac でのデータ暗号化

macOS デバイスで FileVault 暗号化を使用できます。Kaspersky Endpoint Security for Mac の使用中に、暗号化を有効化または無効化できます。

Kaspersky Security Center Cloud コンソールで Kaspersky Endpoint Security for Mac のポリシーを設定することで、暗号化の設定を編集できます。Kaspersky Endpoint Security for Mac は、アクティブなポリシーに基づいて、暗号化と復号化を実行します。詳細は、Kaspersky Endpoint Security for Mac のヘルプを参照してください。

暗号化されたドライブのリストの表示

Kaspersky Security Center Cloud コンソールでは、暗号化されたドライブの詳細や、ドライブレベルで暗号化されたデバイスの詳細を表示できます。ドライブ上の情報が復号されると、そのドライブはリストから自動的に削除されます。

暗号化されたドライブのリストを表示するには、

メインメニューで、［**操作**］→［**データ暗号化と保護機能**］→［**暗号化されたドライブ**］の順に移動します。

セクションがメニューにない場合、非表示になっています。セクションを表示させるには、ユーザーインターフェイスの設定で、［**データ暗号化と保護機能の表示**］を有効にします。

暗号化されたドライブのリストを CSV ファイルまたは TXT ファイルにエクスポートできます。これを行うには、［**CSV へエクスポート**］または［**TXT へエクスポート**］をクリックします。

暗号化レポートの作成と表示

次のレポートを作成できます：

- 管理対象デバイスの暗号化ステータスレポート：様々な管理対象デバイスのデータ暗号化について詳細を確認できます。たとえば、暗号化ルールが設定されたポリシーが適用されるデバイスの数が表示されます。また、再起動が必要なデバイスの数なども確認できます。さらに、各デバイスの暗号化技術とアルゴリズムに関する情報も含まれています。
- 大容量ストレージデバイスの暗号化ステータスレポート：管理対象デバイスの暗号化ステータスレポートと類似の情報が含まれますが、大容量ストレージデバイスとリムーバブルドライブのデータのみが表示されます。
- 暗号化されたドライブへのアクセス権に関するレポート：暗号化されたドライブへのアクセス権を持つユーザーアカウントが表示されます。
- ファイル暗号化のエラーに関するレポート：デバイスでデータの暗号化または復号化タスクを実行した時に発生したエラーの情報を含みます。
- 暗号化されたファイルへのアクセスのブロックに関するレポート：暗号化されたファイルへのアクセスのブロックに関する情報を含みます。このレポートは、暗号化されたファイルやドライブに不正なユーザーまたはアプリケーションがアクセスしようとした場合に役立ちます。

［**監視とレポート**］→［**レポート**］セクションの順に移動して、レポートを生成できます。または、［**操作**］→［**データ暗号化と保護機能**］セクションの順に移動して、次の暗号化レポートを生成できます：

- 大容量ストレージデバイスの暗号化ステータスレポート
- 暗号化されたドライブへのアクセス権に関するレポート
- ファイル暗号化のエラーに関するレポート

*［**データ暗号化と保護機能**］セクションで暗号化レポートを生成するには：*

1. インターフェイスのオプションで、［**データ暗号化と保護機能の表示**］がオンであることを確認します。
2. メインメニューで、［**操作**］→［**データ暗号化と保護機能**］の順に移動します。
3. ［**暗号化されたドライブ**］セクションで、大容量ストレージデバイスの暗号化ステータスレポート、または暗号化されたドライブへのアクセス権に関するレポートを生成します。
4. 生成するレポートの名前をクリックします。

レポート作成が開始されます。

暗号化されたドライブへのオフラインモードでのアクセス権の付与

管理対象デバイスに Kaspersky Endpoint Security for Windows がインストールされていない場合などに、ユーザーは、暗号化されたデバイスへのアクセスを要求できます。要求を受信したら、アクセスキーファイルを作成してユーザーに送信できます。すべてのユースケースと詳細な手順については、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

暗号化されたドライブへのオフラインモードでのアクセス権を付与するには：

1. ユーザーからアクセス要求ファイル（拡張子が FDERTC のファイル）を取得します。Kaspersky Endpoint Security for Windows でファイルを生成するには、Kaspersky Endpoint Security for Windows のヘルプの指示に従ってください。
2. メインメニューで、［**操作**］→［**データ暗号化と保護機能**］→［**暗号化されたドライブ**］の順に移動します。

   暗号化されたドライブのリストが表示されます。
3. ユーザーがアクセスを要求したドライブを選択します。
4. ［**オフラインモードでのデバイスへのアクセスを許可**］をクリックします。
5. 表示されるウィンドウで、選択したドライブの暗号化に使用したカスペルスキー製品に対応するプラグインを選択します。

   > Kaspersky Security Center Cloud コンソールでサポートされないカスペルスキー製品を使用して暗号化されたドライブの場合は、MMC ベースの管理コンソールを使用してオフラインモードでのアクセス権を付与します。
6. Kaspersky Endpoint Security for Windows のヘルプの指示に従ってください（セクションの最後にある項目を展開して参照してください）。

その後、受信したファイルを適用して暗号化されたドライブにアクセスし、ドライブに保存されているデータを読み取ることができます。

ユーザーとユーザーロール

このセクションでは、ユーザーとユーザーロールの概要および作成と編集の手順、ユーザーへのロールとグループの割り当て方法、ポリシーのプロファイルとロールの関連付けの方法について説明しています。

ユーザーアカウントについて

Kaspersky Security Center Cloud コンソールを使用して、ユーザーアカウントとアカウントのグループを管理できます。次の 2 種類のアカウントをサポートしています。

- 組織の従業員のアカウント。管理サーバーは、組織のネットワークをポーリングする時に、ローカルユーザーのアカウントのデータを取得します。
- Kaspersky Security Center Cloud コンソールの内部ユーザーのアカウント。ポータルで内部ユーザーのアカウントを作成できます。これらのアカウントは、Kaspersky Security Center Cloud コンソール内でのみ使用されます。

ユーザーアカウントとセキュリティグループのテーブルを表示するには、次の手順を実行します：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動します。

2. ［**ユーザー**］タブまたは［**グループ**］タブを選択します。

ユーザーまたはセキュリティグループのテーブルが開きます。既定では、開いたテーブルは［**サブタイプ**］列と［**ロール割り当て済み**］列によってフィルターされます。このテーブルには、役割が割り当てられている内部ユーザーまたはグループが表示されます。

ローカルユーザーのアカウントのみを含むテーブルを表示する場合は、［**サブタイプ**］フィルター条件を［**ローカル**］に設定します。

セカンダリ管理サーバーのバージョン 14.2 以前に切り替えて、ユーザーまたはセキュリティグループのリストを開くと、開いたテーブルは［**サブタイプ**］列によってのみフィルターされます。［**ロール割り当て済み**］列によるフィルターは、既定では適用されません。フィルターされたテーブルには、割り当てられたロールを持つすべての内部ユーザーまたはセキュリティグループと、割り当てられていない内部ユーザーまたはセキュリティグループが含まれます。

内部ユーザーのアカウントの追加

必要に応じて、ポータルにワークスペースの内部ユーザーを追加できます。内部ユーザーを追加した後、Kaspersky Security Center Cloud コンソールでそのユーザーにロールを割り当てることができます。

ユーザーロールの概要

ユーザーロール（省略して「*ロール*」とも表記）は、複数の権限をまとめたものと捉えることができます。ロールは、ユーザーのデバイスにインストールされているカスペルスキー製品の設定と関連付けることができます。ロールは、管理グループ、管理サーバー、または特定のオブジェクトのレベルのユーザーまたはセキュリティグループの階層構造の任意のレベルに位置する一連のユーザーまたは一連のセキュリティグループに割り当てることができます。

> 仮想管理サーバーを含む管理サーバーの階層を介してデバイスを管理する場合は、物理管理サーバーからのみユーザーロールを作成、変更、または削除できることに注意してください。次に、仮想サーバーを含むセカンダリ管理サーバーにユーザーロールを適用できます。

ユーザーロールはポリシーのプロファイルに関連付けることができます。ユーザーにロールを割り当てることで、このユーザーには、担当業務を実行する上で必要なセキュリティ設定が適用されます。

ユーザーロールは、特定の管理グループのデバイスのユーザーに関連付けることができます。

ユーザーロールの対象範囲

*ユーザーロールの対象範囲*は、「ユーザーへの割り当て」と「管理グループへの関連付け」の 2 つの要素の組み合わせとして定義されます。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

ロールを使用する利点

ロールを使用する利点として、管理対象デバイスごとあるいはユーザーごとに個別にセキュリティ設定を指定しなくて済む点があります。社内のユーザー数とデバイス数は組織の規模に応じて膨大になる場合がありますが、個別のセキュリティ設定を指定すべき担当業務の区分の数はそれほど多くはないはずです。

ポリシーのプロファイルの使用との相違点と関連性

ポリシーのプロファイルは、各カスペルスキー製品に対して個別に作成されているポリシーのプロパティとして指定されています。ロールは、そうした様々なカスペルスキー製品に対して作成されている多数のプロファイルに1つのロールを関連付けることができます。つまり、ロールは、特定の種別のユーザーを対象とする複数の製品の設定を一元的に管理する目的で使用できます。

製品機能のアクセス権の設定：ロールベースのアクセス制御

Kaspersky Security Center Cloud コンソールは、Kaspersky Security Center Cloud コンソールおよび管理対象のカスペルスキー製品の機能にロールベースでアクセスするための機能を提供します。

次のいずれかの方法で、Kaspersky Security Center Cloud コンソールのユーザーのアプリケーション機能へのアクセス権を設定できます：

- 各ユーザーまたはユーザーグループに対する権限を個別に設定します。
- 事前定義された一連の権限を持つ標準のユーザーロールを作成し、職務の範囲に応じてそれらのロールをユーザーに割り当てる。

ユーザーロールの適用は、アプリケーション機能に対するユーザーのアクセス権を設定する定型的な手順を簡素化および短縮することを目的としています。ロール内のアクセス権は、標準タスクとユーザーの職務範囲に従って設定されます。

ユーザーロールには、それぞれの目的に対応する名前を割り当てることができます。作成できるロール数に制限はありません。

事前定義されたユーザーロールを設定済みの権限セットで使用することも、新しいロールを作成して必要な権限を自分で設定することもできます。

製品機能のアクセス権

次の表に、関連するタスク、レポート、設定を管理し、関連するユーザーの操作を実行するアクセス権を持つKaspersky Security Center Cloud コンソールの機能を示します。

表に一覧表示されているユーザー操作を実行するには、ユーザーは操作内容の横に指定された権限を有している必要があります。

［**読み取り**］、［**書き込み**］、および［**実行**］の各権限は、あらゆるタスク、レポート、設定に適用されます。これらの権限に加えて、ユーザーは、デバイスの抽出でタスクとレポートおよび設定を管理するため、**デバイスの抽出操作を実行**する権限を持っている必要があります。

表にないすべてのタスク、レポート、設定、およびインストールパッケージは、**一般的な機能：基本機能**にあります。

製品機能のアクセス権

機能領域	権限	ユーザー操作：操作を実行するために必要な権限	タスク	レポート	その他
一般的な機能：管理グループの管理	**書き込み**	• デバイスを管理グループに追加：**書き込み** • 管理グループからデバイスを削除：**書き込み** • 管理グループを別の管理グループに追加：**書き込み** • 別の管理グループから管理グループを削除：**書き込み**	なし	なし	なし
一般的な機能：ACL にかかわらずオブジェクトにアクセスする	**読み取り**	すべてのオブジェクトへの読み取り権限の取得：**読み取り**	なし	なし	なし
一般的な機能：基本的な機能	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• 仮想サーバーのデバイス移動ルール（作成、変更、または削除）：**書き込み**、**デバイスの選択に対する操作を実行** • モバイル（LWNGT）プロトコルのカスタム証明書の取得：**読み取り** • モバイル（LWNGT）プロトコルのカスタム証明書の取得：**書き込み** • NLA 定義のネットワークリストの取得：**読み取り** • NLA 定義のネットワークリストの追加、変更、または削除：**書き込み**	• ［管理サーバーのリポジトリへのアップデートのダウンロード］ • ［レポートの配信］ • ［インストールパッケージの配布］ • ［セカンダリ管理サーバーへのアプリケーションのリモートインストール］	• ［保護ステータスレポート］ • ［脅威レポート］ • ［感染が多いデバイスのレポート］ • ［定義データベースのステータスレポート］ • ［エラーレポート］ • ［ネットワーク攻撃のレポート］ • ［インストールされているメールシステム保護製品のサ	なし

		• グループのアクセスコントロールリストの表示：**読み取り** • Kaspersky イベントログの表示：**読み取り**		マリーレポート］ • ［インストールされている境界防御製品のサマリーレポート］ • ［インストールされているアプリケーションの種別のサマリーレポート］ • ［感染したデバイスのユーザーに関するレポート］ • 「セキュリティ問題に関するレポート」 • ［イベントのレポート］ • ［ディストリビューションポイントのアクティビティレポート］ • 「セカンダリ管理サーバーのレポート」 • ［デバイスコントロールイベントのレポート］ • ［脆弱性レポート］ • ［ブロック対象アプリケーション	

				のレポート] • 「ウェブコントロールレポート」 • [管理対象デバイスの暗号化ステータスレポート] • [大容量ストレージデバイスの暗号化ステータスレポート] • [ファイル暗号化エラーのレポート] • [暗号化されたファイルへのアクセスのブロックに関するレポート] • [暗号化されたドライブへのアクセス権に関するレポート] • 「有効なユーザー権限のレポート」 • [ユーザー権限のレポート]	
一般的な機能：**削除されたオブジェクト**	• **読み取り** • **書き込み**	• ごみ箱に削除されたオブジェクトの表示：**読み取り** • ごみ箱からオブジェクトを削除：**書き込み**	なし	なし	なし

一般的な機能：イベント処理	• **イベントの削除** • **イベント通知設定の編集** • **イベントログ設定の編集** • **書き込み**	• イベント登録設定の変更：**イベントログ設定の編集** • イベント通知設定の変更：**イベント通知設定の編集** • イベントの削除：**イベントの削除**	なし	なし	設定： • ウイルスアウトブレイク の設定：ウイルスアウトブレイクイベントの作成に必要なウイルスアウトブレイクの検知数 • ウイルスアウトブレイクの設定：ウイルス検知の評価期間 • データベース内に保存されるイベント数の上限 • 削除されたデバイスからのイベントを保存する期間
一般的な機能：カスペルスキー製品の導入	• **カスペルスキー製品のパッチの管理** • **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	パッチのインストールの承認または拒否：**カスペルスキー製品のパッチの管理**	なし	• ［仮想管理サーバーによるライセンス使用のレポート］ • ［カスペルスキー製品バージョンレポート］ • ［互換性のないアプリケーションのレポート］ • ［カスペルスキー製品のモジュールアップデートのバージョンに関するレポート］ • ［製品導入レポート］	インストールパッケージ：「カスペルスキー」
全般的な機能：ラ	• **ライセンス情報ファ**	• ライセンス情報ファイルのエクスポート：**ライセンス**	なし	なし	なし

イセンス管理	**イルのエクスポート** • **書き込み**	**情報ファイルのエクスポート** • 管理サーバーのライセンス設定を変更：**書き込み**			
一般的な機能：適用されたレポートの管理	• **読み取り** • **書き込み**	• ACL にかかわらずレポートを作成：**書き込み** • ACL にかかわらずレポートを実行：**読み取り**	なし	なし	なし
一般的な機能：管理サーバーの階層構造	**管理サーバー階層の設定**	セカンダリ管理サーバーの登録、アップデート、または削除：**管理サーバー階層の設定**	なし	なし	なし
一般的な機能：ユーザー権限	**オブジェクト ACL の変更**	• 任意のオブジェクトのセキュリティプロパティの変更：**オブジェクト ACL の変更** • ユーザーロールの管理：**オブジェクト ACL の変更** • 内部ユーザーの管理：**オブジェクト ACL の変更** • セキュリティグループの管理：**オブジェクト ACL の変更** • エイリアスの管理：**オブジェクト ACL の変更**	なし	なし	なし
一般的な機能：仮想管理サーバー	• **仮想管理サーバーの管理** • **読み取り** • **書き込み**	• 仮想管理サーバーのリストの取得：**読み取り** • 仮想管理サーバーに関する情報の取得：**読み取り** • 仮想管理サーバーの作成、更新、ま	なし	［サードパーティソフトウェアのアップデートのインストール結果に関するレポート］	なし

	• **実行** • **デバイスの抽出での操作の実行**	たは削除：**仮想管理サーバーの管理** • 仮想管理サーバーの別のグループへの移動：**仮想管理サーバーの管理** • 仮想管理サーバーの権限の設定：**仮想管理サーバーの管理**			
全般的な機能：暗号化鍵の管理	**書き込み**	暗号化鍵をインポート：**書き込み**	なし	なし	なし
システム管理：接続性	• **RDP セッションの開始** • **既存の RDP セッションへの接続** • **トンネリングの開始** • **デバイスから管理者のワークステーションへのファイルの保存** • **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• デスクトップ共有セッションの作成：**デスクトップ共有セッションの作成権限** • RDPセッションの作成：**既存の RDP セッションへの接続** • トンネルの作成：**トンネリングの開始** • コンテンツネットワークリストの保存：**デバイスから管理者のワークステーションへのファイルの保存**	なし	［デバイスのユーザーに関するレポート］	なし

システム管理：ハードウェアインベントリ	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• ハードウェアインベントリオブジェクトの取得またはエクスポート：**読み取り** • ハードウェアインベントリオブジェクトの追加、設定、または削除：**書き込み**	なし	• ［ハードウェアレジストリレポート］ • ［設定変更レポート］ • ［ハードウェアレポート］	なし
システム管理：ネットワークアクセスコントロール	• **読み取り** • **書き込み**	• CISCO の設定の表示：**読み取り** • CISCO の設定の変更：**書き込み**	なし	なし	なし
システム管理：オペレーティングシステムの導入	• **PXE サーバーの導入** • **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• PXE サーバーの導入：**PXE サーバーの導入** • PXE サーバーのリストの表示：**読み取り** • PXE クライアントでのインストールプロセスの開始または停止：**実行** • WinPE およびオペレーティングシステムイメージのドライバーの管理：**書き込み**	［基準デバイスの OS イメージに基づくインストールパッケージの作成］	なし	インストールパッケージ：［OS イメージ］
システム管理：脆弱性とパッチ管理	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• サードパーティのパッチプロパティの表示：**読み取り** • サードパーティのパッチプロパティを変更：**書き込み**	• ［Windows Update の同期の実行］ • ［Windows Update 更新プログラムのインストール］ • ［脆弱性の修正］	［ソフトウェアアップデートレポート］	なし

			• ［アップデートのインストールと脆弱性の修正］		
システム管理：リモートインストール	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	• サードパーティの脆弱性とパッチ管理に基づくインストールパッケージのプロパティの表示：**読み取り** • サードパーティの脆弱性とパッチ管理に基づくインストールパッケージのプロパティの変更：**書き込み**	なし	なし	インストールパッケージ： • ［カスタムアプリケーション］ • ［VAPM パッケージ］
システム管理：ソフトウェアインベントリ	• **読み取り** • **書き込み** • **実行** • **デバイスの抽出での操作の実行**	なし	なし	• ［インストール済みアプリケーションのレポート］ • ［アプリケーションのレジストリ履歴のレポート］ • ［ライセンス認証済みアプリケーショングループのステータスレポート］ • ［サードパーティ製品のライセンスに関するレポート］	なし

事前定義済みのユーザーロール

Kaspersky Security Center Cloud コンソールのユーザーに割り当てられるユーザーロールは、製品機能の一連のアクセス権をユーザーに提供します。

仮想サーバー上で作成されたユーザーには、管理サーバー上のロールを割り当てることはできません。

一連の権限が既に設定されている事前定義済みのユーザーロールを使用するか、新規のロールを作成して必要な権限を自分で設定できます。Kaspersky Security Center Cloud コンソールで使用できる事前定義されたユーザーロールの一部は、**監査**、**セキュリティ責任者**、**上長・監督者**（これらのロールは Kaspersky Security Center Cloud コンソールのバージョン 11 以降に存在します）など、特定の職務に関連付けることができます。これらのロールのアクセス権は、関連する役職の標準タスクと職務の範囲に従って事前設定されています。次の表に、役割を特定の職位に関連付ける方法を示します。

特定の職位の役割の例

ロール	コメント
監査	削除されたオブジェクトの表示を含む、すべてのタイプのレポートでのすべての操作、すべての表示操作を許可します（［**削除されたオブジェクト**］領域で［**読み取り**］および［**書き込み**］の許可を付与します）。他の操作は許可されません。このロールは、組織の監査を実行する人に割り当てることができます。
上長・監督者	すべての表示操作を許可します。他の操作は許可されません。組織の IT セキュリティを担当しているセキュリティ責任者やその他のマネージャーにこのロールを割り当てることができます。
セキュリティ責任者	すべての表示操作を許可し、レポート管理を許可します。**システム管理**：**接続**領域で制限付きのアクセス許可を付与します。組織の IT セキュリティを担当しているセキュリティ責任者にこのロールを割り当てることができます。

次の表に、事前定義された各ユーザーロールに割り当てられているアクセス権を示します。

事前定義されたユーザーロールのアクセス権

ロール	説明
管理サーバーの管理者	次の機能領域でのすべての操作を許可します： • **一般的な機能**： • **基本機能** • **イベント処理** • **管理サーバーの階層構造** • **仮想管理サーバー** • **システム管理**： • **接続** • **ハードウェアインベントリ** • **ソフトウェアインベントリ** **一般的な機能：暗号化鍵の管理**機能領域における［**読み取り**］と［**書き込み**］の権限を付与します。

管理サーバーのオペレーター	次のすべての機能領域で**読み取り**および**実行**権限を付与します： • **一般的な機能**： • **基本機能** • **仮想管理サーバー** • **システム管理**： • **接続** • **ハードウェアインベントリ** • **ソフトウェアインベントリ**
監査	［**一般的な機能**］の次の機能領域におけるすべての操作を許可します： • **ACL にかかわらずオブジェクトにアクセスする** • **削除されたオブジェクト** • **適用されたレポートの管理** このロールは、組織の監査を実行する人に割り当てることができます。
インストールの管理者	次の機能領域でのすべての操作を許可します： • **一般的な機能**： • **基本機能** • **カスペルスキー製品の導入** • **ライセンス管理** • **システム管理**： • **オペレーティングシステムの導入：** • **脆弱性とパッチ管理** • **リモートインストール** • **ソフトウェアインベントリ** ［**一般的な機能：仮想管理サーバー**］機能領域における**読み取り**と**実行**の権限を付与します。
インストールのオペレーター	次のすべての機能領域で**読み取り**および**実行**権限を付与します： • **一般的な機能**： • **基本機能** • **カスペルスキー製品の導入**（この領域で**カスペルスキー製品のパッチの管理**も許可されます） • **仮想管理サーバー**

	• **システム管理**： • **オペレーティングシステムの導入：** • **脆弱性とパッチ管理** • **リモートインストール** • **ソフトウェアインベントリ**
Kaspersky Endpoint Security の管理者	次の機能領域でのすべての操作を許可します： • **一般的な機能：基本的な機能** • すべての機能を含む Kaspersky Endpoint Security のエリア **一般的な機能：暗号化鍵の管理**機能領域における［**読み取り**］と［**書き込み**］の権限を付与します。
Kaspersky Endpoint Security オペレーター	次のすべての機能領域で**読み取り**および**実行**権限を付与します： • **一般的な機能：基本的な機能** • すべての機能を含む Kaspersky Endpoint Security のエリア
メインの管理者	［**一般的な機能**］の次の領域を*除く*機能領域でのすべての操作を許可します。 • **ACL にかかわらずオブジェクトにアクセスする** • **適用されたレポートの管理** **一般的な機能：暗号化鍵の管理**機能領域における［**読み取り**］と［**書き込み**］の権限を付与します。
メインのオペレーター	次のすべての機能領域で**読み取り**および**実行**（該当する場合）権限を付与します： • **一般的な機能**： • **基本機能** • **削除されたオブジェクト** • **管理サーバー上での操作** • **カスペルスキー製品の導入** • **仮想管理サーバー** • **モバイルデバイス管理：全般** • すべての機能を含む**システム管理** • すべての機能を含む Kaspersky Endpoint Security のエリア
モバイルデバイス管理の管理者	次の機能領域でのすべての操作を許可します： • **一般的な機能：基本的な機能**

	• **モバイルデバイス管理：全般**
モバイルデバイス管理のオペレーター	**一般的な機能**：**基本機能**機能領域で**読み取り**および**実行**権限を付与します。 ［**モバイルデバイス管理**：**全般**］機能領域における**読み取り**権限と**モバイルデバイスに情報コマンドのみを送信する**権限を付与します。
セキュリティ責任者	［**一般的な機能**］の次の機能領域におけるすべての操作を許可します： • **ACL にかかわらずオブジェクトにアクセスする** • **適用されたレポートの管理** **システム管理：接続**機能領域の［**読み取り**］、［**書き込み**］、［**実行**］、［**デバイスから管理者のワークステーションにファイルを保存**］、［**デバイスの抽出を対象に処理を実行**］の各権限を付与します。 組織の IT セキュリティを担当しているセキュリティ責任者にこのロールを割り当てることができます。
シニアセキュリティアナリスト	**読み取り**権限を、［**一般的な機能**：**基本機能**］の機能領域で許可します。 システム管理：**接続**機能領域の［**読み取り**］、［**書き込み**］、［**実行**］、［**デバイスから管理者のワークステーションにファイルを保存**］、［**デバイスの抽出を対象に処理を実行**］の各権限を付与します。 Kaspersky Endpoint Detection and Response Expert ソリューションへのアクセス権を許可します。
セルフサービスポータルのユーザー	［**モバイルデバイス管理：セルフサービスポータル**］機能領域におけるすべての操作を許可します。この機能は、Kaspersky Security Center 11 以降ではサポートされていません。
上長・監督者	［**一般的な機能**：**ACL にかかわらずオブジェクトにアクセスする**］および［**一般的な機能**：**適用されたレポートの管理**］機能領域で**読み取り**権限を付与します。 組織の IT セキュリティを担当しているセキュリティ責任者やその他のマネージャーにこのロールを割り当てることができます。
脆弱性とパッチ管理の管理者	［**一般的な機能**：**基本機能**］および［**システム管理**］（すべての機能を含む）機能領域でのすべての操作を許可します。
脆弱性とパッチ管理機能のオペレーター	［**一般的な機能**：**基本機能**］および［**システム管理**］（すべての機能を含む）機能領域で、**読み取り**および**実行**（該当する場合）の権限を付与します。

特定のオブジェクトへのアクセス権の割り当て

サーバーレベルでのアクセス権の割り当てに加えて、特定のオブジェクト（特定のタスクなど）へのアクセスを構成できます。本製品では、次のオブジェクトタイプへのアクセス権を指定できます：

- 管理グループ
- タスク
- レポート
- デバイスの抽出

- イベントの抽出

特定のオブジェクトへのアクセス権を割り当てるには：

1. オブジェクトタイプに応じて、メインメニューで、対応するセクションに移動します：
   - ［**アセット（デバイス）**］→［**グループ階層構造**］
   - ［**アセット（デバイス）**］→［**タスク**］
   - ［**監視とレポート**］→［**レポート**］
   - ［**アセット（デバイス）**］→［**デバイスの抽出**］
   - ［**監視とレポート**］→［**イベントの抽出**］
2. アクセス権を設定するオブジェクトのプロパティを開きます。

   管理グループまたはタスクのプロパティウィンドウを開くには、オブジェクト名をクリックします。ツールバーのボタンを使用して、他のオブジェクトのプロパティを開くことができます。
3. プロパティウィンドウで、［**アクセス権**］セクションを開きます。

   ユーザーリストが開きます。リストされたユーザーとセキュリティグループには、オブジェクトへのアクセス権があります。既定では、管理グループまたはサーバーの階層を使用する場合、リストとアクセス権は親管理グループまたはプライマリサーバーから継承されます。
4. リストを変更できるようにするには、［**カスタムの権限を使用する**］オプションを有効にします。
5. アクセス権を設定します：
   - リストを変更するには、［**追加**］と［**削除**］を使用します。
   - ユーザーまたはセキュリティグループのアクセス権を指定します。次のいずれかの手順を実行します：
     - アクセス権を手動で指定する場合は、ユーザーまたはセキュリティグループを選択し、［**アクセス権**］をクリックして、アクセス権を指定します。
     - ユーザーまたはセキュリティ グループにユーザーロールを割り当てる場合は、ユーザーまたはセキュリティグループを選択し、［**ロール**］をクリックして、割り当てるロールを選択します。
6. ［**保存**］をクリックします。

オブジェクトへのアクセス権が設定されます。

ユーザーまたはセキュリティグループへのロールの割り当て

ユーザーまたはセキュリティグループへロールを割り当てるには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］に移動し、［**ユーザー**］または［**グループ**］タブを選択します。
2. ロールを割り当てるユーザーまたはセキュリティグループの名前を選択します。

   複数の名前を選択できます。

3. メニュー行で、［**ロールの割り当て**］をクリックします。

   ロールの割り当てウィザードが開始します。

4. ウィザードの手順に従います：選択したユーザーまたはセキュリティグループに割り当てるロールを選択し、ロールの範囲を選択します。

   *ユーザーロールの対象範囲*は、「ユーザーへの割り当て」と「管理グループへの関連付け」の 2 つの要素の組み合わせとして定義されます。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

管理サーバーを操作する一連の権限を持つロールは、ユーザー（または複数のユーザー、またはセキュリティグループ）に割り当てられます。ユーザーまたはセキュリティグループのリストで、［**ロール割り当て済み**］列にチェックボックスが表示されます。

ユーザーロールの作成

ユーザーロールを作成するには：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. ［**追加**］をクリックします。
3. ［**新しいロール名**］ウィンドウが開いたら、新しいロールの名前を入力します。
4. ［**OK**］をクリックして変更を適用します。
5. ロールのプロパティウィンドウが開いたら、ロールの設定を変更します：

   - ［**全般**］タブで、ロール名を編集します。
     事前定義のロールの名前は編集できません。
   - ［**設定**］タブで、ロールの範囲とポリシー、ロールに関連付けられているプロファイルを編集します。
   - ［**アクセス権**］タブで、カスペルスキー製品へのアクセス権を編集します。

6. ［**保存**］をクリックして変更内容を保存します。

ユーザーロールのリストに新しいロールが表示されます。

ユーザーのアクセス権の編集

次のオブジェクトのユーザーアクセス権を編集できます：

- 管理サーバー
- 管理グループ
- タスク

- レポート
- イベントの抽出
- デバイスの抽出

ユーザーのアクセス権を編集するには：

1. 選択したオブジェクトの［**アクセス権**］タブに移動します。
2. アクセス権を編集するユーザーを選択します。

   自分のユーザーアカウントを選択した場合、自分のアクセス権を取り消すことはできません。変更は保存されません。

3. ［**アクセス権**］をクリックします。
4. 表示されたウィンドウで、選択したユーザーのアクセス権を編集します。
5. ［OK］をクリックします。

ユーザーのアクセス権が変更されました。

ユーザーロールの編集

ユーザーロールを編集するには：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. 編集するロールの名前をクリックします。
3. ロールのプロパティウィンドウが開いたら、ロールの設定を変更します：
   - ［**全般**］タブで、ロール名を編集します。
     事前定義のロールの名前は編集できません。
   - ［**設定**］タブで、ロールの範囲とポリシー、ロールに関連付けられているプロファイルを編集します。
   - ［**アクセス権**］タブで、カスペルスキー製品へのアクセス権を編集します。
4. ［**保存**］をクリックして変更内容を保存します。

ユーザーロールのリストに更新したロールが表示されます。

各ユーザーロールの対象範囲の編集

*ユーザーロールの対象範囲*は、「ユーザーへの割り当て」と「管理グループへの関連付け」の 2 つの要素の組み合わせとして定義されます。ユーザーロールと関連付けられた設定は、ロールに関連付けられたグループ（子グループを含む）にデバイスが属し、なおかつそのロールを割り当てられたユーザーが所有しているデバイスのみに適用されます。

ユーザーロールの対象範囲にユーザー、ユーザーグループ、管理グループを追加するには、次のいずれかの方法を使用できます：

方法 1：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］に移動し、［**ユーザー**］または［**グループ**］タブを選択します。
2. ユーザーロールの対象範囲に追加するユーザーまたはユーザーグループに隣接するチェックボックスをオンにします。
3. ［**ロールの割り当て**］をクリックします。

   ロールの割り当てウィザードが開始します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
4. ウィザードの［**ロールの選択**］ウィンドウで、割り当てるロールを選択します。
5. ウィザードの［**範囲の定義**］ウィンドウで、ユーザーロールの対象範囲に追加する管理グループを選択します。
6. ［**ロールの割り当て**］をクリックしてウィザードを終了します。

選択したユーザーまたはユーザーグループと、選択した管理グループが、ユーザーロールの対象範囲に追加されます。

方法 2：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. 対象範囲を指定するロールの名前をクリックします。
3. ロールのプロパティウィンドウが開いたら、［**設定**］タブをクリックします。
4. ［**ロールの対象範囲**］セクションで、［**追加**］をクリックします。

   ロールの割り当てウィザードが開始します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
5. ウィザードの［**範囲の定義**］ウィンドウで、ユーザーロールの対象範囲に追加する管理グループを選択します。
6. ウィザードの［**ユーザーを選択してください**］ウィンドウで、ユーザーロールの対象範囲に追加するユーザーとユーザーグループを選択します。
7. ［**ロールの割り当て**］をクリックしてウィザードを終了します。
8. ロールのプロパティウィンドウを閉じます。

選択したユーザーまたはユーザーグループと、選択した管理グループが、ユーザーロールの対象範囲に追加されます。

ユーザーロールの削除

ユーザーロールを削除するには：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. 削除するロールに隣接するチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**OK**］をクリックします。

   選択したユーザーロールが削除されます。

ポリシーのプロファイルとロールの関連付け

ユーザーロールはポリシーのプロファイルに関連付けることができます。この場合、ポリシーのプロファイルの有効化ルールがベースにしているのはロールです：ポリシーのプロファイルは、指定したロールを持つユーザーに対してアクティブにされます。

たとえば、管理グループ内のすべてのデバイスに対して GPS ナビゲーションソフトウェアの使用を禁止するポリシーがあるとします。管理グループ「ユーザー」内に配達担当者が所有するデバイスが 1 台存在しており、そのデバイスでのみ GPS ナビゲーションソフトウェアを使用する必要があるとします。この場合、デバイスの所有者に「配達担当者」ロールを割り当てて、「配達担当者」ロールが割り当てられた所有者のデバイスでのみ使用できるように、GPS ナビゲーションソフトウェアを許可するポリシーのプロファイルを作成できます。その他のポリシー設定はいずれも変更されません。「配達担当者」ロールが割り当てられたユーザーのみが、GPS ナビゲーションソフトウェアを使用できるようになります。後で別の担当者に「配達担当者」ロールを割り当てた場合、その新規担当者も組織のデバイスでナビゲーションソフトウェアを使用できるようになります。同じ管理グループ内の他のデバイスでは、GPS ナビゲーションソフトウェアの使用は禁止されたままになります。

ロールとポリシーのプロファイルを関連付けるには：

1. メインメニューで、［**ユーザーとロール**］→［**ロール**］の順に選択します。
2. ポリシーのプロファイルと関連付けるロール名をクリックします。

   ロールのプロパティウィンドウの［**全般**］タブが表示されます。
3. ［**設定**］タブを選択して、［**ポリシーとプロファイル**］セクションまでスクロールします。
4. ［**編集**］をクリックします。
5. ロールを関連付けるには：

   - **既存のポリシーのプロファイル**— 該当するポリシー名の横にあるアイコン（ ）をクリックして、ロールを関連付けるプロファイルの横にあるチェックボックスをオンにします。
   - **新しいポリシーのプロファイル**：

     a. プロファイルを作成するポリシーの横にあるチェックボックスをオンにします。

b. ［**ポリシーのプロファイルの新規作成**］をクリックします。

c. 新しいプロファイル名を指定して、プロファイルを設定します。

d. ［**保存**］をクリックします。

e. 新しいプロファイルの横にあるチェックボックスをオンにします。

6. ［**ロールへの割り当て**］をクリックします。

プロファイルがロールに関連付けられてロールのプロパティに表示されます。担当者が当該ロールに割り当てられているデバイスに対して、プロファイルが自動的に適用されます。

セキュリティグループの作成

セキュリティグループを作成するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**グループ**］タブを選択します。
2. ［**新規グループ**］をクリックします。
3. ［**新規グループ**］ウィンドウで、新しいセキュリティグループの次の設定を指定します：
   - **名前**
   - **説明**
4. ［OK］をクリックして変更内容を保存します。

新しいセキュリティグループがセキュリティグループリストに追加されます。

セキュリティグループの編集

セキュリティグループを編集するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**グループ**］タブを選択します。
2. 編集するセキュリティグループの名前をクリックします。
3. 開いたグループ設定ウィンドウで、セキュリティグループの設定を変更します：
   - ［**全般**］タブでは、［**名前**］と［**説明**］設定を変更できます。これらの設定は、内部セキュリティグループのみが使用できます。
   - ［**ユーザー**］タブでは、ユーザーをセキュリティグループに追加できます。この設定は、内部ユーザーおよび内部セキュリティグループのみが使用できます。
   - ［**ロール**］タブで、セキュリティグループにロールを割り当てることができます。

4. ［**保存**］をクリックして変更内容を保存します。

変更はセキュリティグループに適用されます。

内部グループへのユーザーアカウントの追加

内部グループに追加できるのは内部ユーザーのアカウントのみです。

ユーザーアカウントを内部グループに追加するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. グループに追加するユーザーアカウントに隣接するチェックボックスをオンにします。
3. ［**グループの割り当て**］をクリックします。
4. 表示される［**グループの割り当て**］ウィンドウで、ユーザーアカウントを追加するグループを選択します。
5. ［**割り当て**］をクリックします。

ユーザーアカウントがグループに追加されます。グループ設定を使用して、内部ユーザーをグループに追加することもできます。

セキュリティグループの削除

削除できるのは内部セキュリティグループのみです。

ユーザーグループを削除するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**グループ**］タブを選択します。
2. 削除するユーザーグループに隣接するチェックボックスをオンにします。
3. ［**削除**］をクリックし、開いたウィンドウで削除を確認します。

選択したユーザーグループが削除されます。

ADFS 統合の設定

組織の Active Directory（AD）に登録されているユーザーが Kaspersky Security Center Cloud コンソールにサインインできるようにするには、Active Directory フェデレーションサービス（ADFS）との統合を設定する必要があります。

Kaspersky Security Center Cloud コンソールは ADFS 3（Windows Server 2016）以降のバージョンをサポートします。

ADFS 統合の設定を変更するには、ユーザー権限を変更するためのアクセス権が必要です。

次に進む前に、Active Directory のポーリングを完了したことを確認してください。

ADFS 統合を設定するには：

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ADFS 連携の設定**］セクションを選択します。
3. コールバック URL をコピーします。
   この URL は、ADFS 管理コンソールで統合を設定するために必要です。
4. ADFS 管理コンソールで、新しいアプリケーショングループを追加し、**サーバーアプリケーション**テンプレートを選択して新しいアプリケーションを追加します（Microsoft のインターフェイス要素の名前は英語表記です）。
   ADFS 管理コンソールで、新しいアプリケーションのクライアント ID が生成されます。クライアント ID は、Kaspersky Security Center Cloud コンソールで統合を設定するために必要です。
5. リダイレクト URI として、管理サーバーのプロパティウィンドウでコピーしたコールバック URL を指定します。
6. クライアント秘密鍵を生成します。クライアント秘密鍵は、Kaspersky Security Center Cloud コンソールで統合を設定するために必要です。
7. 追加したアプリケーションのプロパティを保存します。
8. 作成したアプリケーショングループに、新しいアプリケーションを追加します。ここでは **Web API** テンプレートを選択します。
9. ［**識別子**］タブの［**証明書利用者の識別子**］リストに、先ほど追加したサーバーアプリケーションのクライアント ID を追加します。
10. ［**クライアントのアクセス許可**］タブの［**許可されているスコープ**］リストで、［**allatclaims**］と［**openid**］の範囲を選択します。
11. ［**発行変換規則**］タブで、［**LDAP 属性を要求として送信**］テンプレートを選択して新しい規則を追加します。
    a. 規則に名前を付けます。たとえば、「グループ SID」という名前を付けることができます。
    b. 属性ストアとして［**Active Directory**］を選択し、出力方向の要求の種類の LDAP 属性として［**Token-Groups（SID）**］を「グループ SID」にマッピングします。

12. ［**発行変換規則**］タブで、［**カスタム規則を使用して要求を送信**］テンプレートを選択して新しい規則を追加します：

    a. 規則に名前を付けます。たとえば、「ActiveDirectoryUserSID」という名前を付けることができます。

    b. ［**カスタム規則**］に、次を入力します：

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"), query =
";objectSID;{0}", param = c.Value);
```

13. Kaspersky Security Center Cloud コンソールで、再び［**ADFS 連携の設定**］セクションを開きます。

14. スイッチを［**ADFS 連携が［有効］です**］に切り替えます。

15. ［**設定**］をクリックして、フェデレーションサーバーの 1 つ以上の証明書を含むファイルを指定します。

16. ［**ADFS 連携の設定**］をクリックして、次の設定を指定します：

- **発行者の URL**

  組織で利用中のフェデレーションサーバーの URL アドレス。

  具体的には、Kaspersky Security Center Cloud コンソールが「/.well-known/openid-configuration」を発行者の URL アドレスに追加し、追加後の URL アドレス（issuer_URL/.well-known/openid-configuration）を開いて発行者の設定の自動検出を試行します。

- **クライアント ID**

  Kaspersky Security Center Cloud コンソールを識別するためにフェデレーションサーバーが生成するクライアント ID。ADFS 管理コンソールの、Kaspersky Security Center Cloud コンソールに対応するサーバーアプリケーションのプロパティウィンドウで、クライアント ID を確認できます。

- **クライアント秘密鍵**

  クライアント秘密鍵は、Kaspersky Security Center Cloud コンソールに対応するサーバーアプリケーションのプロパティの指定時に、ADFS 管理コンソールで生成します。

- **ユーザーを認証するドメイン**

  選択したドメインのメンバーは、ドメインアカウントの資格情報を使用して Kaspersky Security Center Cloud コンソールにサインインできるようになります。ネットワークポーリングの完了後に、ドメイン名がリストに表示されます。

- **ID トークンのユーザー SID のフィールド名**

  ID トークンのユーザー SID を参照するフィールドの名前。フィールド名は、Kaspersky Security Center Cloud コンソールでユーザーを識別するために必要です。既定では、ID トークンのこのフィールドは「primarysid」と呼ばれます。

- **ID トークンのユーザーグループ SID 配列のフィールド名**

ユーザーが含まれる Active Directory セキュリティグループの SID 配列を参照するフィールドの名前。既定では、ID トークンのこのフィールドは「groupsid」と呼ばれます。

17. ［**保存**］をクリックします。

ADFS との統合が完了します。AD アカウントの資格情報で Kaspersky Security Center Cloud コンソールにサインインするには、［**ADFS 連携の設定**］セクションで確認できるリンク（［**Kaspersky Security Center Cloud コンソールへのログインリンク（ADFS 使用）**］）を使用します。

ADFS を使用した初回の Kaspersky Security Center Cloud コンソールへのサインイン時には、コンソールの応答が遅延する場合があります。

デバイスの所有者ユーザーの指定

ユーザーをモバイルデバイスの所有者として割り当てる方法の詳細については、Kaspersky Security for Mobile のヘルプを参照してください。

デバイスの所有者ユーザーを指定するには：

1. 仮想管理サーバーに接続されたデバイスの所有者を割り当てる場合は、まず仮想管理サーバーに切り替えます：

   a. メインメニューで、現在の管理サーバー名の右側にあるシェブロンアイコン（）をクリックします。

   b. 必要な管理サーバーを選択します。

2. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。

   ユーザーリストが開きます。現在、仮想管理サーバーに接続している場合、リストには現在の仮想管理サーバーとプライマリ管理サーバーのユーザーが含まれています。

3. デバイスの所有者に割り当てるユーザーアカウントの名前をクリックします。

4. ユーザー設定ウィンドウが表示されたら、［**デバイス**］を選択します。

5. ［**追加**］をクリックします。

6. デバイスリストから、ユーザーに割り当てるデバイスを選択します。

7. ［**OK**］をクリックします。

選択したデバイスが、ユーザーに割り当てられているデバイスのリストに追加されます。

［**アセット（デバイス）**］→［**管理対象デバイス**］で割り当てるデバイスをクリックし、［**デバイスの所有者の管理**］をクリックする方法でも、同じ処理を実行できます。

オブジェクトリビジョンの管理

このセクションでは、オブジェクトのリビジョン管理について説明します。

リビジョン管理に対応するオブジェクトは次の通りです：

- 管理サーバー
- ポリシー
- タスク
- 管理グループ
- ユーザーアカウント
- インストールパッケージ

オブジェクトリビジョンについて

Kaspersky Security Center Cloud コンソールでは、オブジェクトの変更を追跡できます。オブジェクトに変更を加えるたびに、*リビジョン*が作成されます。各リビジョンには番号が付いています。

オブジェクトのリビジョンには次の処理を行うことができます：

- 選択したリビジョンを表示する
- オブジェクトに対して行った変更を、選択したリビジョンにロールバックする

リビジョン管理に対応するオブジェクトのプロパティウィンドウの［**変更履歴**］セクションには、オブジェクトのリビジョンのリストが次の詳細とともに表示されます：

- オブジェクトのリビジョン番号
- オブジェクトが変更された日時
- オブジェクトを変更したユーザーの名前
- オブジェクトに対する操作
- オブジェクト設定に対して行われた変更に関連するリビジョンの説明

  既定では、オブジェクトのリビジョンの説明は空になっています。リビジョンに説明を追加するには、関連するリビジョンを選択して、［**説明の編集**］をクリックします。表示されたウィンドウに、リビジョンの説明を入力します。

変更のロールバック

必要に応じて、オブジェクトの変更をロールバックできます。たとえば、ポリシーの設定を特定の日付の状態まで戻さなければならない場合があります。

オブジェクトの変更をロールバックするには：

1. オブジェクトの［**変更履歴**］セクションに移動します。
2. オブジェクトのリビジョンのリストで、変更のロールバック先となるリビジョンの番号を選択します。
3. ［**ロールバック**］をクリックします。

オブジェクトが、選択したリビジョンにロールバックされます。オブジェクトのリビジョンのリストには、実行された処理の記録が表示されます。リビジョンの説明には、オブジェクトを元に戻したリビジョン番号に関する情報が表示されます。

リビジョンの説明の追加

リスト内でリビジョンが検索しやすくなるように、リビジョンに説明を追加することができます。

リビジョンに説明を追加するには：

1. オブジェクトの［**変更履歴**］セクションに移動します。
2. オブジェクトのリビジョンのリストから、説明を追加するリビジョンを選択します。
3. ［**説明の編集**］をクリックします。
4. 表示されたウィンドウに、リビジョンの説明を入力します。
   既定では、オブジェクトのリビジョンの説明は空になっています。
5. ［**保存**］をクリックします。

新しい説明が、変更履歴の表の［**説明**］列に表示されます。

オブジェクトの削除

次のオブジェクトを削除できます：

- ポリシー
- タスク
- インストールパッケージ
- 仮想管理サーバー
- ユーザー
- セキュリティグループ

- 管理グループ

オブジェクトを削除しても、オブジェクトの情報はデータベースに保存されます。削除されたオブジェクトの情報の保存期間は、オブジェクトの履歴の保存期間（推奨期間は 90 日）と同じです。［**削除されたオブジェクト**］領域の権限で**変更**権限を付与されたユーザーのみが、保存期間を変更できます。

クライアントデバイスの削除について

管理グループから管理対象デバイスを削除すると、アプリケーションはそのデバイスを未割り当てデバイスグループに移動します。デバイスの削除後、インストールされているカスペルスキー製品（ネットワークエージェント、Kaspersky Endpoint Security などのセキュリティ製品）はデバイス上に残ります。

Kaspersky Security Center Cloud コンソールは、次のルールに従って、未割り当てデバイスグループ内のデバイスを処理します：

- デバイス移動ルールを設定しており、デバイスが移動ルールの基準を満たしている場合、デバイスはルールに従って管理グループに自動的に移動されます。

- デバイスは未割り当てデバイスグループに保存され、デバイス保持ルールに従ってグループから自動的に削除されます。

  デバイスの保持ルールは、ディスク全体の暗号化で暗号化された 1 つ以上のドライブを備えたデバイスには影響しません。このようなデバイスは自動的に削除されず、手動でのみ削除できます。暗号化されたドライブを含むデバイスを削除する必要がある場合は、まずドライブを復号化してから、デバイスを削除します。

  暗号化されたドライブを含むデバイスを削除すると、ドライブの復号化に必要なデータも削除されます。この場合、ドライブを復号化するには、次の条件を満たす必要があります：

  - デバイスは管理サーバーに再接続され、ドライブの復号化に必要なデータが復元されます。
  - デバイスのユーザーは復号化パスワードを覚えています。
  - ドライブの暗号化に使用されたセキュリティ製品（Kaspersky Endpoint Security for Windows など）は、デバイスにまだインストールされています。

  ドライブが Kaspersky Disk Encryption 技術によって暗号化されている場合は、FDERT 復元ユーティリティを使用してデータの回復を試行することもできます。

未割り当てデバイスグループからデバイスを手動で削除すると、アプリケーションはそのデバイスをリストから削除します。デバイスを削除した後、インストールされているカスペルスキー製品はデバイス上に残ります。その後、デバイスがまだ管理サーバーに表示されており、定期的なネットワークポーリングを設定している場合、Kaspersky Security Center Cloud コンソールはネットワークポーリング中にデバイスを検出し、未割り当てデバイスグループに追加します。したがって、デバイスが管理サーバーに表示されない場合にのみ、デバイスを手動で削除することが合理的です。

定義データベースとカスペルスキー製品のアップデート

このセクションでは、次の対象の定期的なアップデートに必要な手順について説明します。

- 定義データベースとソフトウェアモジュール
- インストール済みのカスペルスキー製品（Kaspersky Security Center Cloud コンソールコンポーネントとセキュリティ製品を含む）

シナリオ：定義データベースとカスペルスキー製品の定期的なアップデート

このセクションでは、定義データベース、ソフトウェアモジュール、カスペルスキー製品の定期的なアップデートを行う手順について説明します。ネットワーク保護の設定シナリオの完了後は、保護システムの信頼性を維持する必要があります。このメンテナンスにより、ウイルス、ネットワーク攻撃、フィッシング攻撃を含むあらゆる脅威に対して、管理対象デバイスの保護を安定させることができます。

Kaspersky Security Center Cloud コンソールコンポーネントとセキュリティ製品に対するアップデートのインストールには、複数のスキームを使用できます。ネットワークの要件に最も合致するスキームを1つ以上選択してください。

次のシナリオでは、ディストリビューションポイントのリポジトリにアップデートをダウンロードするアップデートのスキームについて説明します。管理対象デバイスがディストリビューションポイントに接続していない場合は、定義データベース、ソフトウェアモジュール、カスペルスキー製品の手動アップデート、またはカスペルスキーのアップデートサーバーからの直接アップデートを検討してください。

このシナリオを完了すると、次のような結果になります：

- Kaspersky Security Center Cloud コンソールが自動的にアップデートされるか、アップデートに*承認*ステータスを指定した場合にアップデートされます。
- 指定したスケジュールに応じて、カスペルスキーのセキュリティ製品、定義データベース、ソフトウェアモジュールがアップデートされます。既定では、カスペルスキーのセキュリティ製品はユーザーが承認したアップデートのみインストールします。

2つのいずれかの方法でアップデートをダウンロードしてインストールするよう、アップデート処理を設定できます：

- 自動

  この場合は、このシナリオを1度だけ実行します。［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスク（存在する場合）と、カスペルスキーのセキュリティ製品のアップデートタスクにスケジュールを設定し、ネットワークエージェントのプロパティの既定のアップデート設定を維持する必要があります。

- 手動

  ［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスク（存在する場合）とカスペルスキーのセキュリティ製品のアップデートタスクを手動で実行するように、アップデート処理を設定できます。アップデートに*承認*ステータスを指定した場合のみ、Kaspersky Security Center Cloud コンソールコンポーネントのアップデートをインストールするように、ネットワークエージェントを設定することもできます。

必須条件

導入を開始する前に、次が完了していることを確認してください：

1. Kaspersky Security Center Cloud コンソールを使用したカスペルスキー製品の導入手順に従って、カスペルスキーのセキュリティ製品を管理対象デバイスに導入した。そのシナリオの実行時、管理対象デバイスの数とネットワークトポロジーに従って、適切な数のディストリビューションポイントを割り当てた。

2. ネットワーク保護の設定手順に従って、必要なすべてのポリシー、ポリシーのプロファイル、タスクを作成して設定した。

実行するステップ

定義データベースとカスペルスキー製品の定期的なアップデートの設定は、段階的に進行します：

1 ［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの作成

［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを作成します。このタスクを実行すると、Kaspersky Security Center Cloud コンソールは、カスペルスキーのアップデートサーバーからディストリビューションポイントにアップデートを直接ダウンロードします。

実行手順の説明：［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの作成

2 ディストリビューションポイントの設定

すべての必要なディストリビューションポイントのプロパティで、［**アップデートの配信**］がオンになっていることを確認します。ディストリビューションポイントでこのオプションがオフになっていると、ディストリビューションポイントの範囲内のデバイスは、ローカルリソースからのみ、またはカスペルスキーのアップデートサーバーから直接、アップデートをダウンロードできます。

管理対象デバイスがディストリビューションポイントからのみアップデートを受信するようにする場合は、ネットワークエージェントポリシーで［**ディストリビューションポイント経由でのみファイルを配信する**］をオンにします。

3 差分ファイルを使用したアップデート処理の最適化（任意）

この機能を有効にすると、ディストリビューションポイントと管理対象デバイス間のトラフィックを削減できます。この機能を使用するには、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクのプロパティで［**差分ファイルのダウンロード**］をオンにします。

実行手順の説明：カスペルスキー製品の定義データベースとソフトウェアモジュールのアップデートでの差分ファイルの使用

4 インストールするアップデートの定義

既定では、ダウンロードされたソフトウェアアップデートのステータスは「*未定義*」です。このアップデートをネットワーク接続されたデバイスにインストールするかどうかを定義するには、ステータスを「*承認*」または「*拒否*」に変更します。承認されたアップデートは常にインストールされます。未定義のアップデートは、ネットワークエージェントポリシーの設定に従って、ネットワークエージェントとその他の Kaspersky Security Center Cloud コンソールコンポーネントにのみインストールできます。「*拒否*」のステータスを設定したアップデートはデバイスにインストールされません。

実行手順の説明：

- アップデートのステータスについて
- ソフトウェアアップデートの拒否と承認

5 Kaspersky Security Center Cloud コンソールコンポーネントのアップデートとパッチの自動インストールの設定

既定では、ネットワークエージェントとその他の Kaspersky Security Center Cloud コンソールコンポーネント用にダウンロードされたアップデートとパッチは自動的にインストールされます。ネットワークエージェントのプロパティで［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオンのままにした場合、アップデートはすべて、リポジトリにダウンロードされた後に自動的にインストールされます。このオプションをオフにすると、ダウンロードされたパッチのうちステータスが「*未定義*」のものは、管理者がステータスを「*承認*」に変更しない限りインストールされません。

実行手順の説明：Kaspersky Security Center Cloud コンソールコンポーネントの自動アップデートおよびパッチ適用の有効化と無効化

6. **セキュリティ製品のアップデートとパッチの自動インストールの設定**

管理対象の製品のアップデートタスクを作成して、製品、ソフトウェアモジュール、および定義データベースをタイムリーにアップデートします。タスクスケジュールの設定時に［**新しいアップデートがリポジトリにダウンロードされ次第**］をオンにすることを推奨します。これにより、できるだけ早く新しいアップデートがインストールされます。

既定では、アップデートのステータスを「*承認*」に変更した後にのみ、管理対象製品のアップデートがインストールされます。Kaspersky Endpoint Security for Windows では、アップデートタスクでアップデート設定を変更できます。

使用許諾契約書の条項の確認と同意がアップデートに必要な場合は、最初に条項に同意する必要があります。その後、アップデートを管理対象デバイスに配信できます。

実行手順の説明：Kaspersky Endpoint Security のアップデートをデバイスに自動インストール

シナリオを完了したら、ネットワークステータスの監視に進むことができます。

定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデートの概要

管理対象デバイスの保護が最新の状態であるようにするには、次の項目のタイムリーなアップデートが必要です：

- 定義データベースとソフトウェアモジュール

  Kaspersky Security Center Cloud コンソールは、定義データベースとソフトウェアをダウンロードする前にカスペルスキーのサーバーがアクセス可能かどうかをチェックします。システム DNS を使用したサーバーへのアクセスが不可能な場合は、パブリック DNS サーバーが使用されます。これは、定義データベースを最新の状態に保ち、管理対象デバイスのセキュリティレベルを確実に管理するために必要です。

- インストール済みのカスペルスキー製品（Kaspersky Security Center Cloud コンソールコンポーネントとセキュリティ製品を含む）

ネットワークの設定に応じて、管理対象デバイスへの必要なアップデートのダウンロードと配信に次のスキームを使用できます：

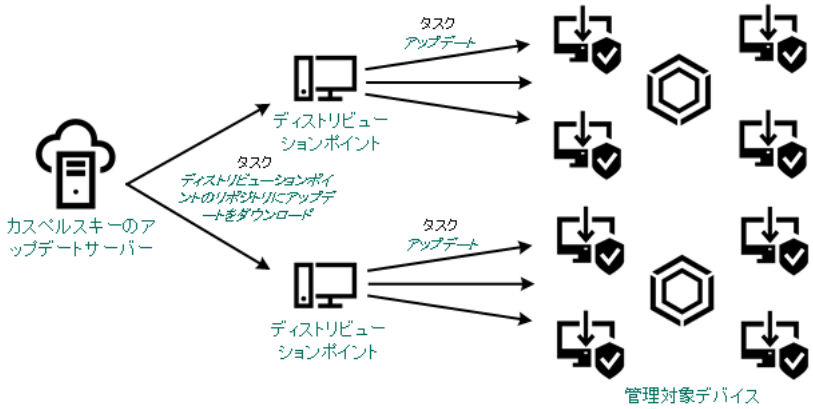
- *ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクの使用
- ローカルフォルダー、共有フォルダー、または FTP サーバーを使用して手動で実行
- カスペルスキーのアップデートサーバーから管理対象デバイスのセキュリティ製品を直接アップデート

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

このスキームでは、Kaspersky Security Center Cloud コンソールは*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを使用してアップデートをダウンロードします。ディストリビューションポイントの範囲に含まれる管理対象デバイスは、ディストリビューションポイントのリポジトリからアップデートをダウンロードします（次の図を参照）。

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

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



ディストリビューションポイントのリポジトリにアップデートをダウンロードタスクを使用したアップデート

*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクが完了すると、次のアップデートがディストリビューションポイントのリポジトリにダウンロードされます。

- 管理対象デバイスのセキュリティ製品用の定義データベースとソフトウェアモジュール

  これらのアップデートは、Kaspersky Endpoint Security for Windows のアップデートタスクを使用してインストールされます。

- Kaspersky Security Center Cloud コンソールコンポーネント用のアップデート

  既定では、これらのアップデートは自動的にインストールされます。ネットワークエージェントポリシーで設定を変更できます。

- セキュリティ製品用のアップデート

  既定では、Kaspersky Endpoint Security for Windows はユーザーが承認したアップデートのみインストールします。アップデートはアップデートタスクを使用してインストールされ、このタスクのプロパティで設定できます。

各カスペルスキー製品は、管理サーバーに必要なアップデートを要求します。管理サーバーはこれらの要求を集計した上で、いずれかの製品で要求されたアップデートのみをディストリビューションポイントのリポジトリにダウンロードします。これにより、同一のアップデートが複数回ダウンロードされたり、不必要なアップデートがダウンロードされることを防ぐことができます。*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを実行中、関連するバージョンの定義データベースとソフトウェアモジュールのダウンロードを確実に行うため、次の情報が管理サーバーからカスペルスキーのアップデートサーバーに自動的に送信されます：

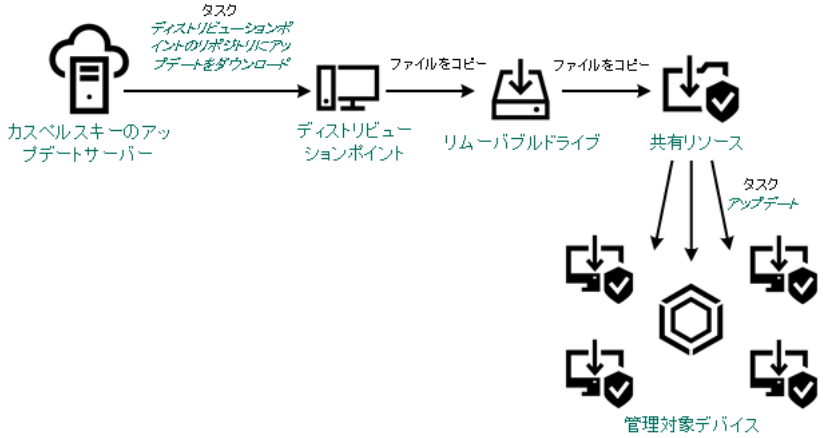
- 製品 ID およびバージョン
- アプリケーションのインストール ID

- 現在のライセンス ID
- ダウンロードタスクの実行 ID

送信される情報には、個人データや機密データは含まれません。カスペルスキーでは、法律で定められた要件に従って情報を保護しています。

ローカルフォルダー、共有フォルダー、または FTP サーバーを使用して手動で実行

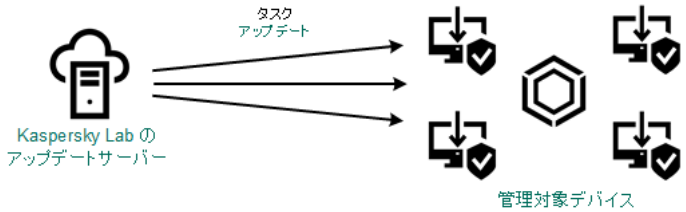
クライアントデバイスがディストリビューションポイントに接続できない場合、ローカルフォルダーまたは共有リソースを使用して定義データベース、ソフトウェアモジュール、カスペルスキー製品をアップデートできます。このスキームでは、ディストリビューションポイントのリポジトリからリムーバブルドライブに必要なアップデートをコピーして、Kaspersky Endpoint Security for Windows の設定でアップデート元として指定したローカルフォルダーまたは共有リソースにアップデートをコピーする必要があります（次の図を参照）。



ローカルフォルダー、共有フォルダー、または FTP サーバーを使用したアップデート

カスペルスキーのアップデートサーバーから管理対象デバイスの Kaspersky Endpoint Security for Windows を直接アップデート

管理対象デバイスで、カスペルスキーのアップデートサーバーから直接アップデートを受信するように Kaspersky Endpoint Security for Windows を設定できます（次の図を参照）。



カスペルスキーのアップデートサーバーからセキュリティ製品を直接アップデート

このスキームでは、セキュリティ製品は Kaspersky Security Center Cloud コンソールが提供するリポジトリを使用しません。カスペルスキーのアップデートサーバーからアップデートを直接受信するには、セキュリティ製品のインターフェイスでカスペルスキーのアップデートサーバーをアップデート元として指定します。これらの設定の詳細な説明は、Kaspersky Endpoint Security for Windows のヘルプを参照してください。

［ディストリビューションポイントのリポジトリにアップデートをダウンロード］タスクの作成

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

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

*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを管理グループに対して作成できます。このタスクは、指定の管理グループ内のディストリビューションポイントに対して実行されます。

このタスクは、カスペルスキーのアップデートサーバーからディストリビューションポイントのリポジトリにアップデートをダウンロードするために必要です。アップデートのリストには次の内容が含まれます：

- カスペルスキーのセキュリティ製品の定義データベースおよびソフトウェアモジュールのアップデート
- Kaspersky Security Center Cloud コンソールコンポーネントのアップデート
- カスペルスキーのセキュリティ製品のアップデート

アップデートのダウンロード後、管理対象デバイスにこれらのアップデートを配信できます。

*［**ディストリビューションポイントのリポジトリにアップデートをダウンロード**］タスクを、特定の管理グループに対して作成するには：*

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. Kaspersky Security Center Cloud コンソールアプリケーションの場合は、［**タスク種別**］で［**ディストリビューションポイントのリポジトリにアップデートをダウンロード**］を選択します。
4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクの適用対象として、管理グループ、デバイスの抽出、または指定したデバイスを選択します。
6. ［**タスク作成の終了**］ウィンドウで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
7. ［**作成**］をクリックします。

   タスクが作成され、タスクリストに表示されます。
8. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。
9. タスクのプロパティウィンドウの［**アプリケーション設定**］タブで、次の設定を指定します：

- **アップデート元**

  ディストリビューションポイントのアップデート元として、使用できるものは次の通りです：

  - カスペルスキーのアップデートサーバー

    カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。

    既定ではこのオプションが選択されます。

  - プライマリ管理サーバー

    セカンダリ管理サーバーまたは仮想管理サーバーを対象とするタスクに適用されます。

  - ローカルまたはネットワーク上のフォルダー

    最新のアップデートが保存されたローカルフォルダーまたはネットワークフォルダー：ネットワークフォルダーとしては FTP サーバー、HTTP サーバー、または SMB 共有を指定できます。ネットワークフォルダーに認証が必要な場合、SMB プロトコルのみがサポートされています。ローカルフォルダーの選択時には、管理サーバーがインストールされているデバイスのフォルダーを指定する必要があります。

    > アップデート元で使用される FTP/HTTP サーバーまたはネットワークフォルダーは、アップデートを含み、フォルダーの構造がカスペルスキーのアップデートサーバーの使用時に作成された構造と一致する必要があります。

- **アップデート保存先フォルダー**

  保存したアップデートを保管するためのフォルダーのパス。指定したフォルダーのパスをクリップボードにコピーすることができます。グループタスクに対して指定されたフォルダーのパスを変更することはできません。

- **差分ファイルのダウンロード**

  このオプションで差分ファイルのダウンロードを有効にすることができます。

  既定では、このオプションはオフです。

- **旧スキームを使用してアップデートをダウンロード**

Kaspersky Security Center Cloud コンソールでは、定義データベースのアップデートとソフトウェアモジュールのダウンロードに新しいスキームを使用します。新しいスキームを使用してアップデートをダウンロードするには、アップデート元に、新しいスキームと互換性のあるメタデータを持つアップデートファイルが含まれている必要があります。アップデート元のアップデートファイルのメタデータが旧スキームのみと互換性がある場合は、［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。オフにした場合、アップデートのダウンロードタスクは失敗します。

たとえば、アップデート元としてローカルまたはネットワークフォルダーが指定されており、そのフォルダー内のアップデートファイルが次のアプリケーションによってダウンロードされた場合にはこのオプションをオンにする必要があります：

- Kaspersky Update Utility

  このユーティリティは旧スキームを使用してアップデートをダウンロードします。

- Kaspersky Security Center 13.2 以前のバージョン

たとえば、ディストリビューションポイントがローカルまたはネットワークフォルダーからアップデートを取得するように設定されているものとします。この場合、インターネットに接続できる管理サーバーを使用してアップデートをダウンロードし、このアップデートをディストリビューションポイントのローカルフォルダーに配置します。管理サーバーに Kaspersky Security Center 13.2 以前のバージョンがインストールされている場合、*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクで［**旧スキームを使用してアップデートをダウンロード**］をオンにしてください。

既定では、このオプションはオフです。

10. タスクの開始スケジュール作成。必要に応じて、次の設定を指定します：

- **実行予定**

  タスクを実行するスケジュールを選択し、そのスケジュールを設定します。

  - **手動**（既定で選択）

    タスクは、自動的には実行されません。手動でのみ開始できます。
    既定では、このオプションはオンです。

  - **N 分ごと**

    タスク作成日の指定した時刻から、分単位で指定した間隔ごとにタスクを定期的に実行します。
    既定では、現在のシステム時刻から、30 分ごとにタスクが実行されます。

  - **N 時間ごと**

    指定した日時から、時間単位で指定した間隔ごとにタスクを定期的に実行します。
    既定では、現在のシステム日時から、6 時間ごとにタスクが実行されます。

  - **N 日ごと**

日単位で指定した間隔ごとにタスクを定期的に実行します。さらに、最初にタスクを実行する日時を指定できます。この詳細設定項目は、タスクを作成中の製品でこの項目の使用がサポートされている場合に利用できます。

既定では、現在のシステム日時から、1日ごとにタスクが実行されます。

- **N週間ごと**

  指定した日時から、週単位で指定した間隔ごとに、指定した曜日の指定した時刻にタスクを定期的に実行します。

  既定では、毎週、月曜日の現在のシステム時刻にタスクが実行されます。

- **毎日（サマータイムはサポートしていません）**

  日単位で指定した間隔ごとにタスクを定期的に実行します。このスケジュールではサマータイム（DST）の適用はサポートされません。つまり、サマータイムの開始または終了に伴い、時刻を1時間早めたまたは遅らせた場合でも、実際にタスクが開始される時刻は変化しません。

  このスケジュールの使用は推奨されません。Kaspersky Security Center Cloud コンソールの古いバージョンとの後方互換性を維持するために用意されているオプションとなります。

  既定では、毎日、現在のシステム時刻にタスクが実行されます。

- **毎週**

  毎週、指定した曜日の指定した時刻にタスクを実行します。

- **曜日ごと**

  指定した曜日（複数可）の指定した時刻にタスクを定期的に実行します。

  既定では、毎週金曜日の午後6時にタスクが実行されます。

- **毎月**

  毎月、指定した日付の指定した時刻にタスクを定期的に実行します。

  指定した日付が存在しない月には、月の最終日にタスクを実行します。

  既定では、各月の初日の現在のシステム時刻にタスクが実行されます。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にタスクを定期的に実行します。

  既定では、月内のいかなる日付も選択されておらず、開始時刻は午後6時です。

- **ウイルスアウトブレイク検知次第**

［*ウイルスアウトブレイク*］イベントの発生後にタスクを実行します。ウイルスアウトブレイクを監視するアプリケーションの種別を選択します。次のアプリケーション種別があります：

- ワークステーションとファイルサーバー向けアンチウイルス製品
- 境界防御向けアンチウイルス製品
- メールサーバー向けアンチウイルス製品

既定では、すべてのアプリケーション種別がオンです。

ウイルスアウトブレイクを検知したアンチウイルス製品の種別ごとに、異なるタスクを実行したい場合、該当するタスクで必要ないアプリケーションの種別をオフにします。

- **他のタスクが完了次第**

他のタスクが完了した後に、現在のタスクを開始します。現在のタスクを実行する条件として、先に実行されるタスクの実行結果（「正常終了」または「エラー終了」）を選択できます。これにより、たとえば［**デバイスの電源をオンにする**］を選択して［*デバイスの管理*］タスクを実行し、その完了後に［*ウイルススキャン*］タスクを実行できます。このパラメータは、両方のタスクが同じデバイスに割り当てられている場合にのみ機能します。

- **未実行のタスクを実行する**

このオプションは、タスクの開始予定時刻にクライアントデバイスがネットワーク上で可視でない場合のタスクの処理方法を指定します。

このオプションをオンにすると、クライアントデバイスでのカスペルスキー製品の次回起動時に、タスクの開始を試行します。タスクスケジュール設定が［**手動**］、［**1回**］または［**即時**］に設定されている場合、ネットワーク上でデバイスが認識されるかデバイスがタスク範囲に追加されるすぐにタスクが開始されます。

このオプションをオフにすると、スケジュール設定されたタスクだけがクライアントデバイス上で開始され、［**手動**］、［**1回**］、および［**即時**］に設定したタスクはネットワーク上で可視になっているクライアントデバイスでのみ開始されます。そのため、たとえばリソース消費量が多いので業務時間外にのみ実行したいタスクなどで、このオプションをオフにすることが有効な場合があります

既定では、このオプションはオンです。

- **タスクの開始を自動的かつランダムに遅延させる**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始され、*タスクの分散開始*を実現します。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

分散開始の開始時刻は、タスクの作成時に自動的に計算されます。計算の結果は、タスクに割り当てられるクライアントデバイスの台数によって異なります。以降は、タスクは常に計算された開始時刻に開始されます。ただし、タスクの設定が変更されたりタスクが手動で開始された場合、計算によるタスク開始時刻は変更されます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

- **タスクの開始を次の時間範囲内でランダムに遅延させる（分）**

このオプションをオンにすると、クライアントデバイス上のタスクは指定した時間内でランダムに開始されます。タスクの分散開始を使用すると、スケジュールされたタスクの開始時にクライアントデバイスから管理サーバーへの大量の要求が同時に発生するのを防ぐことができます。

このオプションをオフにすると、タスクはスケジュールに従ってクライアントデバイスで開始されます。

既定では、このオプションはオフです。既定の時間は1分です。

11. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。

タスクの作成時に指定した設定およびタスクのその他のプロパティは、いつでも変更できます。

*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを実行すると、定義データベースとソフトウェアモジュールのアップデートがアップデート元からダウンロードされ、共有フォルダーに保存されます。指定の管理グループに含まれていて、ディストリビューションポイントタスクが明示的に設定されていないディストリビューションポイントにしか、ダウンロードされたアップデートは使用されません。

管理対象デバイスでディストリビューションポイントのみからアップデートを取得するための設定

管理対象デバイスは、定義データベース、ソフトウェアモジュール、カスペルスキー製品のアップデートを、様々なアップデート元から（アップデートサーバーから直接、ディストリビューションポイントから、ローカルまたはネットワークフォルダーから）受信できます。ディストリビューションポイントを唯一のアップデート元として指定できます。

ディストリビューションポイントのみからアップデートを受信するよう、管理対象デバイスを設定するには

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. ネットワークエージェントのポリシーをクリックします。
3. ポリシーのプロパティウィンドウで［**アプリケーション設定**］タブを開きます。
4. ［**設定**］セクションで、［**ディストリビューションポイント経由でのみファイルを配信する**］切り替えスイッチをオンにします。
5. このスイッチの設定に「ロック（🔒）」を設定します。
6. ［**保存**］をクリックします。

選択したデバイスにポリシーが適用され、デバイスはディストリビューションポイントのみからアップデートを受信します。

Kaspersky Security Center Cloud コンソールコンポーネントの自動アップデートおよびパッチ適用の有効化と無効化

Kaspersky Security Center Cloud コンソールコンポーネントのアップデートとパッチの自動インストールは、デバイスにネットワークエージェントをインストールする際に既定で有効になります。ネットワークエージェントのインストール中、あるいはインストール後にポリシーを使用して無効にすることができます。

ネットワークエージェントをデバイスのローカルにインストール中、Kaspersky Security Center Cloud コンソールコンポーネントの自動アップデートとパッチを無効にするには：

1. デバイスへのネットワークエージェントのローカルインストールを開始します。
2. **詳細設定**ステップで、［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオフにします。
3. ウィザードの指示に従ってください。

Kaspersky Security Center Cloud コンソールコンポーネントの自動アップデートとパッチが無効にされたネットワークエージェントが、デバイスにインストールされます。ポリシーを使用して、自動アップデートとパッチを有効にできます。

インストールパッケージを介してネットワークエージェントをデバイスにインストール中に、Kaspersky Security Center Cloud コンソールコンポーネントの自動アップデートとパッチを無効にするには：

1. メインメニューで、［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］の順に選択します。
2. **Kaspersky Security Center ネットワークエージェント <バージョン番号>** パッケージをクリックします。
3. プロパティウィンドウで［**設定**］タブを選択します。
4. ［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオフにします。

Kaspersky Security Center Cloud コンソールコンポーネントの自動アップデートとパッチが無効にされたネットワークエージェントが、このパッケージからインストールされます。ポリシーを使用して、自動アップデートとパッチを有効にできます。

デバイスにネットワークエージェントをインストール中に、ステップ 4 でチェックボックスをオン（またはオフ）にすると、その後ネットワークエージェントポリシーを使用して自動アップデートを有効（または無効）にできます。

ネットワークエージェントポリシーを使用して、Kaspersky Security Center Cloud コンソールコンポーネントの自動アップデートとパッチを有効または無効にするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. ネットワークエージェントのポリシーをクリックします。
3. ポリシーのプロパティウィンドウで［**アプリケーション設定**］タブを選択します。
4. ［**パッチとアップデートの管理**］セクションで、［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオンまたはオフにして、自動アップデートとパッチを有効または無効にします。
5. この切り替えスイッチには必ずロック（🔒）を設定（［**強制適用**］）します。

選択したデバイスにポリシーが適用され、Kaspersky Security Center Cloud コンソールコンポーネントの自動アップデートとパッチがデバイス上で有効（または無効）になります。

Kaspersky Endpoint Security for Windows のアップデートの自動インストール

クライアントデバイスでの Kaspersky Endpoint Security for Windows の定義データベースとソフトウェアモジュールの自動アップデートを設定できます。

デバイスでの Kaspersky Endpoint Security for Windows のアップデートのダウンロードおよび自動インストールを設定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. Kaspersky Endpoint Security for Windows を対象アプリケーションとするタスクから、［**アップデート**］タスク種別を選択します。
4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスク範囲を選択します。
6. タスクの適用対象として、管理グループ、デバイスの抽出、または指定したデバイスを選択します。
7. ［**タスク作成の終了**］ウィンドウで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
8. ［**作成**］をクリックします。

   タスクが作成され、タスクリストに表示されます。
9. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。
10. タスクのプロパティウィンドウの［**アプリケーション設定**］タブで、アップデートタスクの設定をローカルモードかモバイルモードで指定します：

    - **ローカルモード**：このタブの設定で、デバイスと管理サーバー間の接続が確立された場合に、デバイスがアップデートを受信する方法を指定します。
    - **モバイルモード**：このタブの設定で、Kaspersky Security Center Cloud コンソールとデバイス間の接続が確立されない場合（たとえば、デバイスがインターネットに接続されていない場合）に、デバイスがアップデートを受信する方法を指定します。
11. Kaspersky Endpoint Security for Windows の定義データベースとソフトウェアモジュールのアップデートに使用するアップデート元を有効にします。必要に応じて、［**上へ**］と［**下へ**］を使用して、リスト内のアップデート元の順序を変更できます。複数のアップデート元が有効な場合は、リスト上位のリソースから次々に接続が試行され、最初に使用可能なソースからアップデートパッケージが取得されて、アップデートタスクが実行されます。

Kaspersky Security Center Cloud コンソールをアップデート元として設定すると、管理サーバーのリポジトリではなく、ディストリビューションポイントのリポジトリからアップデートがダウンロードされます。ディストリビューションポイントを割り当て、*ディストリビューションポイントのリポジトリにアップデートをダウンロード*タスクを作成したことを確認します。

12. ［**承認されたソフトウェアモジュールのアップデートのインストール**］をオンにすると、定義データベースとともに、ソフトウェアモジュールのアップデートをダウンロードしてインストールできます。

    このオプションをオンにすると、Kaspersky Endpoint Security for Windows によって適用可能なソフトウェアモジュールのアップデートについてユーザーに通知され、アップデートタスクの実行時に、アップデートパッケージにソフトウェアモジュールのアップデートが追加されます。Kaspersky Endpoint Security for Windows では、*承認*ステータスが付与されたアップデートのみがインストールされます。ローカルへのインストールは、製品インターフェイスまたは Kaspersky Security Center Cloud コンソールを経由して実行されます。

    ［**ソフトウェアモジュールの重要なアップデートを自動的にインストール**］をオンにすることもできます。ソフトウェアモジュールのアップデートが使用可能な時、Kaspersky Endpoint Security for Windows は「*緊急*」ステータスのアップデートのみを自動的にインストールし、残りのアップデートは承認後にインストールします。

    ソフトウェアモジュールのアップデートで使用許諾契約書とプライバシーポリシーの条項を確認して同意する必要がある場合、カスペルスキー製品では、使用許諾契約書とプライバシーポリシーの条項をユーザーが同意した後にアップデートがインストールされます。

13. フォルダーへダウンロード済みのアップデートを保存するには［**アップデートをフォルダーにコピー**］をオンにし、保存先のフォルダーのパスを指定します。

14. タスクのスケジュールを設定します。確実にタイムリーにアップデートされるようにするため、［**新しいアップデートがリポジトリにダウンロードされ次第**］をオンにすることを推奨します。

15. ［**保存**］をクリックします。

［**アップデート**］タスクの実行時、製品からカスペルスキーのアップデートサーバーにリクエストが送信されます。

アップデートによっては、最新バージョンの管理プラグインをインストールする必要があります。

アップデートのステータスについて

*ステータス*は、特定のソフトウェアのアップデートをネットワーク接続されたデバイスにインストールする必要があるかどうかを定義する、ソフトウェアのアップデートの属性です。

アップデートには次のステータスがあります：

- *未定義*

  既定では、ダウンロードされたソフトウェアアップデートのステータスは「*未定義*」です。未定義のアップデートは、ネットワークエージェントポリシーの設定に従って、ネットワークエージェントとその他の Kaspersky Security Center Cloud コンソールコンポーネントにのみインストールできます。

- *承認*

承認されたアップデートは常にインストールされます。使用許諾契約書の条項の確認と同意がアップデートに必要な場合は、最初に条項に同意する必要があります。

- *拒否*

  「*拒否*」のステータスを設定したアップデートはデバイスにインストールされません。

次のソフトウェアのアップデートのステータスを変更できます：

- ネットワークエージェントとその他の Kaspersky Security Center Cloud コンソールコンポーネント

  既定では、その他の Kaspersky Security Center Cloud コンソールコンポーネント用にダウンロードされたアップデートとパッチは自動的にインストールされます。ネットワークエージェントのプロパティで［**コンポーネントに適用可能でステータスが「未定義」であるアップデートとパッチを自動的にインストールする**］をオンのままにした場合、アップデートはすべて、リポジトリにダウンロードされた後に自動的にインストールされます。このオプションをオフにすると、ダウンロードされたパッチのうちステータスが「*未定義*」のものは、管理者がステータスを「*承認*」に変更しない限りインストールされません。

  Kaspersky Security Center Cloud コンソールコンポーネントのアップデートは、アップデートに「*拒否*」ステータスを設定した場合でもアンインストールできません。

- カスペルスキーのセキュリティ製品

  既定では、アップデートのステータスを「*承認*」に変更した後にのみ、管理対象製品のアップデートがインストールされます。拒否に設定したセキュリティ製品のアップデートが以前にインストールされている場合、Kaspersky Security Center Cloud コンソールはすべてのデバイスからのアップデートのアンインストールを試行します。

ソフトウェアアップデートの拒否と承認

アップデートのインストールタスクの設定によっては、インストールするアップデートの承認が必要な場合があります。インストールする必要のあるアップデートを承認し、インストールしないアップデートを拒否します。

たとえば、最初にテスト環境にアップデートをインストールしてデバイスのオペレーティングシステムとの互換性の問題が生じないかを確認してから、クライアントデバイスへのこれらのアップデートのインストールを許可することができます。

1 つ以上のアップデートを承認または拒否するには：

1. メインメニューで、［**操作**］→［**カスペルスキー製品**］→［**シームレスアップデート**］の順に移動します。

   適用可能なアップデートのリストが表示されます。

   > 管理対象の製品のアップデートには、Kaspersky Security Center の特定の最小バージョンをインストールする必要がある場合があります。この最小バージョンが現在のバージョンよりも新しい場合、これらのアップデートは表示されますが、承認はできません。また、Kaspersky Security Center をアップグレードするまでは、このようなアップデートからインストールパッケージを作成することもできません。Kaspersky Security Center インスタンスを必要な最小バージョンにアップグレードするように要求されます。

2. 承認または拒否するアップデートを選択します。

3. 選択したアップデートを承認する場合は［**承認**］を、拒否する場合は［**承認却下**］を選択します。

   既定値は［*未定義*］です。

［*承認*］ステータスを割り当てたアップデートは、インストールを待機するキューに置かれます。

［*拒否*］ステータスを割り当てたアップデートは、アップデートをインストール済みのすべてのデバイスからアンインストールされます（可能な場合）。また、今後これらのアップデートは他のデバイスに新規にインストールされません。

カスペルスキー製品の一部のアップデートはアンインストールできません。アンインストールできないカスペルスキー製品のアップデートに［*拒否*］ステータスを設定した場合、これらのアップデートはインストール済みのデバイスからアンインストールされません。しかし、今後これらのアップデートが他のデバイスに新規にインストールされることはありません。

サードパーティ製のソフトウェアアップデートに［*拒否*］ステータスを設定すると、このアップデートは、アップデートのインストールを予定しているがまだ完了していないデバイスにはインストールされません。アップデートをインストール済みのデバイスには、これらのアップデートがそのまま残ります。アップデートを削除する時は、手動でローカル削除できます。

カスペルスキー製品の定義データベースとソフトウェアモジュールのアップデートでの差分ファイルの使用

差分ファイルには、定義データベースファイルまたはソフトウェアモジュールファイルの異なる 2 バージョン間の変更点のみが含まれています。完全な定義データベースファイルまたはソフトウェアモジュールファイルよりも差分ファイルの方が容量が小さいため、差分ファイルを使用することで社内ネットワークのトラフィック量を制限できます。ディストリビューションポイントで［*差分ファイルのダウンロード*］機能が有効になっている場合、該当するディストリビューションポイントに差分ファイルが保存されます。これにより、このディストリビューションポイントからアップデートを取得するデバイスでは、保存されている差分ファイルを使用して定義データベースとソフトウェアモジュールのアップデートを実行できます。

差分ファイルをより効果的に使用するには、デバイス側でのアップデートスケジュールを、アップデートの取得元となるディストリビューションポイント側のアップデートスケジュールと同期することを推奨します。ただし、このような設定を行わなくても、デバイス側のアップデート頻度がアップデートの取得元となるディストリビューションポイント側のアップデート頻度より低いだけでもトラフィックの軽減につながります。

ディストリビューションポイントは差分ファイルの自動配信に IP マルチキャストを使用しません。

差分ファイルのダウンロード機能を有効にするには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. ［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクをクリックして、タスクのプロパティを開きます。
3. ［**アプリケーション設定**］タブで、［**差分ファイルのダウンロード**］をオンにします。
4. ［**保存**］をクリックします。

差分ファイルのダウンロード機能が有効になります。［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを実行するたびに、アップデートファイルに加えてアップデートの差分ファイルもダウンロードされます。

［差分ファイルのダウンロード］機能が有効になっているかどうかを確認する方法としては、これらの手順を実行する前後での内部トラフィックを測定することができます。

オフラインデバイスの定義データベースとソフトウェアモジュールのアップデート

管理対象デバイスの定義データベースとソフトウェアモジュールのアップデートは、ウイルスやその他の脅威からデバイスを継続して保護するために重要なタスクです。通常、管理者はディストリビューションポイントのリポジトリを使用して、定期的なアップデートを設定します。

ディストリビューションポイントまたはインターネットのいずれにも接続されていないデバイス（またはデバイスのグループ）のデータベースとソフトウェアモジュールをアップデートする必要がある場合は、FTP サーバーまたはローカルフォルダーなどの代替のアップデート元を使用する必要があります。この場合、フラッシュドライブまたは外付けハードディスクなどの大容量ストレージデバイスを使用して必要なアップデートのファイルを受け渡しする必要があります。

必要なアップデートは次のソースからコピーできます：

- ディストリビューションポイント：

  オフラインデバイスにインストールされているセキュリティ製品に必要なアップデートがディストリビューションポイントのリポジトリに含まれるようにするには、ディストリビューションポイントの範囲内にある少なくとも 1 台のオンラインの管理対象デバイスに同じセキュリティ製品がインストールされている必要があります。また、この製品が［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを使用してディストリビューションポイントのリポジトリからアップデートを受信するように設定されている必要があります。

- 同じセキュリティ製品がインストールされていて、ディストリビューションポイントのリポジトリからアップデートを受信するか、カスペルスキーのアップデートサーバーからアップデートを直接受信するように設定されている任意のデバイス。

ディストリビューションポイントのリポジトリからアップデートをコピーして、データベースおよびソフトウェアモジュールのアップデートを設定する例を次に示します。

オフラインデバイスの定義データベースとソフトウェアモジュールをアップデートするには：

1. リムーバブルドライブをディストリビューションポイントデバイスに接続します。
2. アップデートファイルをリムーバブルドライブにコピーします。

   既定では、%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\Updates にアップデートが存在します。
3. オフラインデバイスで、ローカルフォルダーまたは FTP サーバーや共有フォルダーなどの共有リソースからアップデートを受信するように、セキュリティ製品（たとえば Kaspersky Endpoint Security for Windows）を設定します。
4. リムーバブルドライブからローカルフォルダーまたはアップデート元として使用する共有リソースにアップデートファイルをコピーします。
5. アップデートのインストールが必要なオフラインデバイスで、Kaspersky Endpoint Security for Windows のアップデートタスクを開始します。

アップデートタスクが完了すると、デバイスの定義データベースとソフトウェアモジュールが最新の状態になります。

Kaspersky Security for Windows Server データベースのアップデート

Kaspersky Security for Windows Server は管理対象デバイスにインストールでき、この製品によるファイルのリアルタイム保護を起動できます。ただし、この製品が正しく機能するために必要なデータベースは製品に付属していません。データベースは、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクの完了後にのみ、管理対象デバイスにダウンロードされます。

Kaspersky Security for Windows Server を管理対象デバイスにインストールした直後にファイルのリアルタイム保護を開始する場合は、その製品用のデータベースがダウンロード済みで、最新であることを確認する必要があります。そうしないと、タスクが正しく機能しない可能性があります。

Kaspersky Security for Windows Server データベースが最新であることを確認するには：

1. ［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクを管理サーバーで完了したことを確認します。

2. 次のいずれかの手順を実行します：

   - ファイルのリアルタイム保護タスクの設定で、開始を［*製品起動時*］に設定し、管理対象デバイスを再起動します。

   - ファイルのリアルタイム保護タスクの設定で、任意の開始時刻を手動で設定します。

Kaspersky Security for Windows Server のファイルのリアルタイム保護タスクが正しく機能する準備が完了しました。

クライアントデバイス上のサードパーティ製品の管理

このセクションでは、クライアントデバイスにインストールされているサードパーティ製ソフトウェアの管理に関わる Kaspersky Security Center Cloud コンソールの機能について説明します。

サードパーティ製品について

Kaspersky Security Center Cloud コンソールを使用してクライアントデバイスにインストールされたサードパーティ製のソフトウェアをアップデートしたり脆弱性を修正したりできます。Kaspersky Security Center Cloud コンソールはサードパーティ製ソフトウェアを最新バージョンにのみアップデートします。以下のリストに、Kaspersky Security Center Cloud コンソールを使用してアップデートできるサードパーティ製ソフトウェアを記載します。

サードパーティ製ソフトウェアのリストはアップデートまたは新しい製品で拡張されることがあります。ユーザーのデバイスにインストールされたサードパーティ製ソフトウェアを Kaspersky Security Center Cloud コンソールでアップデートできるかどうかは、Kaspersky Security Center Cloud コンソールで適用可能なアップデートのリストで確認できます。

- 7-Zip Developers：7-Zip
- Adobe Systems：
  - Adobe Acrobat DC
  - Adobe Acrobat Reader DC
  - Adobe Acrobat
  - Adobe Reader
  - Adobe Shockwave Player
- AIMPDevTeam：AIMP
- ALTAP：Altap Salamander
- Apache Software Foundation：Apache Tomcat
- Apple：
  - Apple iTunes
  - Apple QuickTime
- Armory Technologies, Inc.：Armory
- Cerulean Studios：Trillian Basic
- Ciphrex Corporation：mSIGNA
- Cisco：Cisco Jabber

- Code Sector：TeraCopy
- Codec Guide：
  - K-Lite Codec Pack Basic
  - K-Lite Codec Pack Full
  - K-Lite Codec Pack Mega
  - K-Lite Codec Pack Standard
- DbVis Software AB：DbVisualizer
- Decho Corp.：
  - Mozy Enterprise
  - Mozy Home
  - Mozy Pro
- Dominik Reichl：KeePass Password Safe
- Don HO don.h@free.fr：Notepad++
- DoubleGIS：2GIS
- Dropbox, Inc.：Dropbox
- EaseUs：EaseUS Todo Backup Free
- Electrum Technologies GmbH：Electrum
- Enter Srl：Iperius Backup
- Eric Lawrence：Fiddler
- EverNote：EverNote
- Exodus Movement Inc：Exodus
- EZB Systems：UltraISO
- Famatech:
  - Radmin
  - Remote Administrator
- Far Manager：FAR Manager
- FastStone Soft：FastStone Image Viewer
- FileZilla Project：FileZilla

- Firebird Developers：Firebird
- Foxit Corporation：
  - Foxit Reader
  - Foxit Reader Enterprise
- Free Download Manager.ORG：Free Download Manager
- GIMP project：GIMP
- GlavSoft LLC.：TightVNC
- GNU Project：Gpg4win
- Google：
  - Google Earth
  - Google Chrome
  - Google Chrome Enterprise
  - Google Earth Pro
- Inkscape Project：Inkscape
- IrfanView：IrfanView
- iterate GmbH：Cyberduck
- Logitech：SetPoint
- LogMeIn, Inc.：
  - LogMeIn
  - Hamachi
  - LogMeIn Rescue Technician Console
- Martin Prikryl：WinSCP
- Mozilla Foundation：
  - Mozilla Firefox
  - Mozilla Firefox ESR
  - Mozilla SeaMonkey
  - Mozilla Thunderbird
- New Cloud Technologies Ltd：MyOffice Standard.Home Edition

- OpenOffice.org: OpenOffice
- Opera Software：Opera
- Oracle Corporation：
  - Oracle Java JRE
  - Oracle VirtualBox
- PDF44：PDF24 MSI / EXE
- Piriform：
  - CCleaner
  - Defraggler
  - Recuva
  - Speccy
- Postgresql：PostgreSQL
- RealNetworks：RealPlayer Cloud
- RealVNC：
  - RealVNC Server
  - RealVNC Viewer
- Right Hemisphere Inc.：SAP Visual Enterprise Viewer (Complete/Minimum)
- Simon Tatham：PuTTY
- Skype Technologies：Skype for Windows
- Sober Lemur S.a.s.：
  - PDFsam Basic
  - PDFsam Visual
- Softland：FBackup
- Splashtop Inc.：Splashtop Streamer
- Stefan Haglund, Fredrik Haglund, Florian Schmitz：CDBurnerXP
- Sublime HQ Pty Ltd：Sublime Text
- TeamViewer GmbH：
  - TeamViewer Host

    - TeamViewer
- Telegram Messenger LLP：Telegram Desktop
- The Document Foundation：
    - LibreOffice
    - LibreOffice HelpPack
- The Git Development Community：
    - Git for Windows
    - Git LFS
- The Pidgin developer community：Pidgin
- TortoiseSVN Developers：TortoiseSVN
- VideoLAN：VLC media player
- VMware：
    - VMware Player
    - VMware Workstation
- WinRAR Developers：WinRAR
- WinZip：WinZip
- Wireshark Foundation：Wireshark
- Wrike：Wrike
- Zimbra：Zimbra Desktop

脆弱性とパッチ管理の制限事項

脆弱性とパッチ管理機能には、使用するライセンスと Kaspersky Security Center Cloud コンソールが機能しているモードに応じて、複数の制限事項があります。

次のライセンスでは、脆弱性とパッチ管理がサポートされません：

- Kaspersky Endpoint Security for Business Select
- Kaspersky Hybrid Cloud Security

次のライセンスでは、脆弱性とパッチ管理がサポートされます：

- Kaspersky Endpoint Security for Business Advanced

- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Total Security for Business
- Kaspersky Hybrid Cloud Security Enterprise

次の表で、脆弱性とパッチ管理がサポートされないライセンスと、サポートされるライセンスについて、試用モードの Kaspersky Security Center Cloud コンソールの制限事項を比較します。

脆弱性とパッチ管理の制限事項

制限	試用モード	製品モード：脆弱性とパッチ管理がサポートされないライセンス	製品モード：脆弱性とパッチ管理がサポートされるライセンス
［*Windows Update 更新プログラムのインストール*］タスクまたは［*脆弱性の修正*］タスク数の上限	4	4	0（この種別の新しいタスクは作成できません）
［*アップデートのインストールと脆弱性の修正*］タスク数の上限	2	サポートされていません	4
すべての［*アップデートのインストールと脆弱性の修正*］タスクにおけるルール数の上限	10	サポートされていません	50
同時に*承認*ステータスを設定できるソフトウェアのアップデート数の上限	100	サポートされていません	1000
手動でタスクに追加できるソフトウェアのアップデート数の上限	500	1000	1000
手動でタスクに追加できるソフトウェアの脆弱性の数の上限	500	1000	1000

試用モード、製品モード、および様々なライセンスオプションで使用できる脆弱性とパッチ管理機能

脆弱性とパッチ管理機能を Kaspersky Security Center Cloud コンソールで利用できるかどうかは、この製品を試用モードで利用するか、製品モードで利用するか、また選択したライセンスオプションによって異なります。表を使用して、脆弱性とパッチ管理のどの機能が使用可能かを確認してください。

脆弱性とパッチ管理機能の可用性

脆弱性とパッチ管理機能	試用モード	製品モード：Kaspersky Endpoint Security for Business Select	製品モード：Kaspersky Endpoint Security for Bu Kaspersky Endpoint Detection and R Kaspersky Total Security fo
Windows を実行している管理対象デバイスの Microsoft ソフトウェアに存在する脆	✓	✓	–

弱性の手動修正 ［*脆弱性の修正*］タスクの作成			
Windows を実行している管理対象デバイスの Microsoft ソフトウェアに対するアップデートの手動インストール ［*Windows Update 更新プログラムのインストール*］タスクを使用した、サードパーティ製ソフトウェアのアップデートのインストール	–	✓	✓
ルールベースによるサードパーティ製ソフトウェアのアップデートの自動インストールと脆弱性の自動修正 ［*アップデートのインストールと脆弱性の修正*］タスクの作成とアップデートのインストール	✓	–	✓

アップデートインストールのルールの追加			

サードパーティ製ソフトウェアのアップデートのインストール

このセクションでは、クライアントデバイスにインストールされているサードパーティ製ソフトウェアのアップデートのインストールに関わる Kaspersky Security Center Cloud コンソールの機能について説明します。

シナリオ：サードパーティ製ソフトウェアのアップデート

このセクションでは、クライアントデバイスにインストールされているサードパーティ製ソフトウェアをアップデートするシナリオについて説明します。「サードパーティ製ソフトウェア」とは、Microsoft およびその他の製造元が提供しているアプリケーションを指します。Microsoft 製品のアップデートの情報は、Windows Update サービスによって提供されます。

実行するステップ

サードパーティ製ソフトウェアのアップデートは段階的に進行します：

1. **必要なアップデートの検索**

   管理対象デバイスに必要なサードパーティ製ソフトウェアのアップデートを検索するには、［*脆弱性とアプリケーションのアップデートの検索*］タスクを実行します。タスクが完了すると、Kaspersky Security Center Cloud コンソールはタスクのプロパティで指定したデバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。

   ［*脆弱性とアプリケーションのアップデートの検索*］タスクは、管理サーバークイックスタートウィザードによって自動的に作成されます。ウィザードを実行していない場合は、次の手順に進む前にタスクを手動で作成するか、クイックスタートウィザードを実行してください。

   実行手順の説明：

   - 脆弱性とアプリケーションのアップデートの検索タスクの作成
   - 脆弱性とアプリケーションのアップデートの検索タスクの設定

2. **検出されたアップデートのリストの分析**

   ［**ソフトウェアのアップデート**］リストを確認して、どのアップデートをインストールするかを決定します。それぞれのアップデートの詳細情報を確認するには、リスト内のアップデートの名前をクリックします。リスト内のそれぞれのアップデートについて、管理対象デバイスへのアップデートのインストールに関する統計情報を表示できます。たとえば、選択したアップデートがインストールされていない、アップデートのインストール対象となっている、またはアップデートのインストールに失敗したデバイス数を表示できます。

   実行手順の説明：サードパーティ製品の使用可能なアップデートに関する情報の表示

3. **アップデートのインストールの設定**

Kaspersky Security Center Cloud コンソールでサードパーティ製ソフトウェアのアップデートのリストの取得が完了すると、［*アップデートのインストールと脆弱性の修正*］タスクまたは［*Windows Update 更新プログラムのインストール*］タスクを使用して、クライアントデバイスにアップデートをインストールできます。いずれかのタスクを作成してください。［**タスク**］タブまたは［**ソフトウェアのアップデート**］リストを使用してこれらのタスクを作成できます。

［*アップデートのインストールと脆弱性の修正*］タスクは、Windows Update サービス経由で提供される場合も含めた Microsoft アプリケーションのアップデートとその他の製造元の製品のアップデートのインストールに使用されます。

［*Windows Update 更新プログラムのインストール*］は Windows Update 更新プログラムのインストールにのみ使用できます。

ソフトウェアのアップデートのインストールタスクにはいくつかの制限があります。これらの制限は、Kaspersky Security Center Cloud コンソールで使用しているライセンスと、Kaspersky Security Center Cloud コンソールが機能しているモードによって異なります。

一部のソフトウェアのアップデートのインストールでは、インストールするために使用許諾契約書に同意する必要があります。使用許諾契約書に同意しない場合、アップデートはインストールされません。

実行手順の説明：

- ［アップデートのインストールと脆弱性の修正］タスクの作成
- ［Windows Update 更新プログラムのインストール］タスクの作成
- サードパーティ製品の使用可能なアップデートに関する情報の表示

4 タスクのスケジュール設定

アップデートのリストを最新の状態に維持するため、［*脆弱性とアプリケーションのアップデートの検索*］タスクが定期的に自動で実行されるようにスケジュールを指定してください。既定の実行頻度は週に 1 回です。

［*アップデートのインストールと脆弱性の修正*］タスクを作成している場合は、実行頻度を［*脆弱性とアプリケーションのアップデートの検索*］と同じかそれよりも少なくします。［*Windows Update 更新プログラムのインストール*］タスクのスケジュールを設定する場合は、タスクを実行する前に毎回、インストールするアップデートのリストを指定する必要があることに注意してください。

タスクのスケジュールを指定する場合は、［*脆弱性とアプリケーションのアップデートの検索*］タスクが完了してからこれらのタスクが開始するようにしてください。

実行手順の説明：タスクの全般的な設定

5 ソフトウェアアップデートの拒否と承認（必要に応じて実施）

［*アップデートのインストールと脆弱性の修正*］タスクを作成している場合は、タスクのプロパティでアップデートのインストールルールを指定できます。［*Windows Update 更新プログラムのインストール*］タスクを作成している場合は、この手順は省略してください。

それぞれのルールで、アップデートの次のようなステータスに応じて、インストールするアップデートを指定できます：*未定義*、*承認*、*拒否*。たとえば、サーバー向けのタスクとして、「*承認*」ステータスの Windows Update 更新プログラムのインストールのみを許可するようにルールを設定したタスクを設定するなどの使用方法が考えられます。この場合、インストールするアップデートに手動で「*承認*」ステータスを設定します。このように設定すると、Windows Update 更新プログラムでもステータスが「*未定義*」または「*拒否*」のアップデートは、タスクでインストール先に指定したサーバーにインストールされません。

既定では、ダウンロードされたソフトウェアアップデートのステータスは「*未定義*」です。［**ソフトウェアのアップデート**］リストで、アップデートのステータスを「*承認*」または「*拒否*」に変更できます（［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動して操作）。

実行手順の説明：サードパーティ製ソフトウェアのアップデートの拒否と承認

6 アップデートのインストールタスクの実行

［*アップデートのインストールと脆弱性の修正*］タスクまたは［*Windows Update 更新プログラムのインストール*］タスクを開始します。これらのタスクを開始すると、管理対象デバイスにアップデートがダウンロードされインストールされます。タスクが完了したら、タスクリストでのタスクのステータスが［*正常終了*］になっていることを確認します。

実行手順の説明：タスクの手動での開始

7. **サードパーティ製ソフトウェアのアップデートのインストール結果のレポートの作成（省略可能）**

   タスクが作成され、アップデートがインストールされていることを確認するには、［**サードパーティ製ソフトウェアのアップデートのインストール結果に関するレポート**］を作成して、このレポートでアップデートのインストールに関する詳細な統計情報を表示します。

   実行手順の説明：レポートの生成と表示

サードパーティ製ソフトウェアのアップデートについて

Kaspersky Security Center Cloud コンソールでは、管理対象デバイスにインストールされたサードパーティ製ソフトウェアのアップデートを管理し、Microsoft 製アプリケーションや他のソフトウェア会社の製品に含まれる脆弱性を、必要なアップデートをインストールすることで修正できます。

Kaspersky Security Center Cloud コンソールは、［*脆弱性とアプリケーションのアップデートの検索*］タスクでアップデートを検索します。タスクが完了すると、管理サーバーはタスクのプロパティで指定したデバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。適用可能なアップデートの情報を確認した後、アップデートをデバイスにインストールできます。

Kaspersky Security Center Cloud コンソールはいくつかのアプリケーションについて、古いバージョンを削除して新しいバージョンをインストールして更新します。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが起動している場合、終了するように指示される場合があります。

セキュリティ上の理由から、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートすべてに対して、カスペルスキーの技術によるマルウェアのスキャンが自動的に実行されます。この技術は自動的なファイルのチェックに使用され、ウイルススキャン、Sandbox 環境における静的分析、動的分析、ふるまい分析、機械学習が含まれます。

カスペルスキーは、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートを手動で分析することはありません。さらに、カスペルスキーの専門家は脆弱性（既知または未知）や文書化されていないアップデートの機能について確認したり、上記で指定されているもの以外のアップデートの分析を行ったりすることはありません。

サードパーティ製ソフトウェアのアップデートのインストールタスク

サードパーティ製ソフトウェアのアップデートのメタデータがリポジトリにダウンロードされると、以下のタスクを使用してクライアントデバイスにアップデートをインストールできます：

- ［*アップデートのインストールと脆弱性の修正*］タスク

  このタスクは、Windows Update サービス経由で提供される場合も含めた Microsoft アプリケーションのアップデートとその他の製造元の製品のアップデートのインストールに使用されます。

このタスクが完了すると、管理対象デバイスにアップデートが自動的にインストールされます。新しいアップデートのメタデータが管理サーバーのリポジトリにダウンロードされると、Kaspersky Security Center Cloud コンソールはそのアップデートがアップデートルールで指定されている条件を満たすかどうかをチェックします。条件を満たす新しいアップデートはすべて、次回のタスク実行時に自動的にダウンロードされてインストールされます。

- ［*Windows Update 更新プログラムのインストール*］タスク

  このタスクは、Windows Update 更新プログラムのインストールにのみ使用できます。

  このタスクが完了すると、タスクのプロパティで指定したアップデートのみがインストールされます。タスクの作成後、新しいアップデートをインストールする場合は、既存のタスクに目的のアップデートを追加するか、［*Windows Update 更新プログラムのインストール*］タスクを作成する必要があります。

ソフトウェアのアップデートのインストールタスクにはいくつかの制限があります。これらの制限は、Kaspersky Security Center Cloud コンソールで使用しているライセンスと、Kaspersky Security Center Cloud コンソールが機能しているモードによって異なります。

サードパーティ製ソフトウェアのアップデートのインストール

以下のタスクのいずれかを作成し実行して、管理対象デバイスにサードパーティ製ソフトウェアのアップデートをインストールできます：

- *アップデートのインストールと脆弱性の修正*

  このタスクを使用して、Microsoft が提供する Windows Update 更新プログラムと他の製造元による製品のアップデートの両方をインストールできます。

- *Windows Update 更新プログラムのインストール*

  このタスクは、Windows Update 更新プログラムのインストールにのみ使用できます。

ソフトウェアのアップデートのインストールタスクにはいくつかの制限があります。これらの制限は、Kaspersky Security Center Cloud コンソールで使用しているライセンスと、Kaspersky Security Center Cloud コンソールが機能しているモードによって異なります。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが起動している場合、終了するように指示される場合があります。

オプションとして、次の方法で必要なアップデートをインストールするタスクを作成できます：

- アップデートリストを開き、インストールするアップデートを指定する。

  その結果、選択したアップデートをインストールする新しいタスクが作成されます。オプションとして、選択したアップデートを既存のタスクに追加できます。

- アップデートのインストールウィザードを実行する。

  アップデートのインストールウィザードを使用できるかどうかは、Kaspersky Security Center Cloud コンソールのモードと現在のライセンスによって異なります。

このウィザードを使用すると、アップデートのインストールタスクの作成と設定手順が簡略化され、インストールするのと同じアップデートで構成される冗長なタスクを作成せずに済みます。

アップデートリストを使用してサードパーティ製ソフトウェアのアップデートをインストールする

アップデートのリストを使用して、サードパーティ製ソフトウェアのアップデートをインストールするには：

1. アップデートのリストの1つを開きます：

   - 一般的なアップデートのリストを開くには、メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動します。
   - 管理対象デバイスのアップデートのリストを開くには、メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］→［**<デバイス名>**］→［**詳細**］→［**適用可能なアップデート**］の順に移動します。
   - 特定のアプリケーションのアップデートのリストを開くには、メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］→［**<製品名>**］→［**適用可能なアップデート**］の順に移動します。

   適用可能なアップデートのリストが表示されます。

2. インストールするアップデートに隣接するチェックボックスをオンにします。

3. ［**アップデートのインストール**］をクリックします。

   インストールするソフトウェアのアップデートによっては、使用許諾契約書に同意する必要があります。使用許諾契約書に同意しない場合、アップデートはインストールされません。

4. 次のいずれかのオプションをオンにします：

   - **新規タスク**

     新規タスクウィザードが起動します。Kaspersky Security Center Cloud コンソールのモードと現在のライセンスに応じて、［*アップデートのインストールと脆弱性の修正*］タスクまたは［*Windows Update 更新プログラムのインストール*］タスクが事前に選択されています。ウィザードの手順に従って、タスクの作成を完了します。

   - **アップデートのインストール（指定したタスクにルールを追加）**

     選択したアップデートを追加するタスクを選択します。［*アップデートのインストールと脆弱性の修正*］タスクまたは［*Windows Update 更新プログラムのインストール*］タスクを選択します。［*アップデートのインストールと脆弱性の修正*］タスクを選択すると、選択したアップデートをインストールするための新しいルールが、選択したタスクに自動的に追加されます。［*Windows Update 更新プログラムのインストール*］タスクを選択すると、選択したアップデートはタスクのプロパティに追加されます。

     タスクのプロパティウィンドウが開きます。［**保存**］をクリックして変更を保存します。

タスクの作成を選択した場合は、タスクが作成され、タスクリスト（［**アセット（デバイス）**］→［**タスク**］）に表示されます。既存のタスクにアップデートを追加することを選択した場合、アップデートはタスクのプロパティに保存されます。

サードパーティ製ソフトウェアのアップデートをインストールするには、［*アップデートのインストールと脆弱性の修正*］タスク、または［*Windows Update 更新プログラムのインストール*］タスクを開始します。これらのタスクは手動によって、または開始するタスクのプロパティでスケジュール設定を指定することによって開始できます。タスクのスケジュールを指定する場合は、［*脆弱性とアプリケーションのアップデートの検索*］タスクが完了してからアップデートのインストールタスクが開始されるようにしてください。

アップデートのインストールウィザードを使用してサードパーティ製ソフトウェアのアップデートをインストールする

この機能を使用できるかどうかは、Kaspersky Security Center Cloud コンソールのモードと現在のライセンスによって異なります。

アップデートのインストールウィザードを使用して、サードパーティ製ソフトウェアのアップデートをインストールするタスクを作成するには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動します。
   適用可能なアップデートのリストが表示されます。
2. インストールするアップデートに隣接するチェックボックスをオンにします。
3. ［**アップデートのインストールウィザードを実行**］をクリックします。
   アップデートのインストールウィザードが起動します。［**アップデートのインストールタスクを選択する**］ページには、次の種別の既存の全タスクのリストが表示されます。
   - *アップデートのインストールと脆弱性の修正*
   - *Windows Update 更新プログラムのインストール*
   - *脆弱性の修正*

   最後の 2 つの種別のタスクを変更して新しいアップデートをインストールすることはできません。新しいアップデートをインストールする際に使用できるのは、［*アップデートのインストールと脆弱性の修正*］タスクのみです。
4. 選択したアップデートをインストールするタスクのみをウィザードに表示するには、［**このアップデートをインストールするタスクのリストを表示**］をオンにします。
5. 目的の対象を追加します：
   - タスクを開始するには、タスク名の横にあるチェックボックスをオンにして、［**開始**］をクリックします。
   - 既存のタスクに新しいルールを追加するには：
     a. タスク名に隣接するチェックボックスをオンにし、［**ルールの追加**］をクリックします。
     b. 開いたページで、新しいルールを構成します：
     - **この重要度レベルのアップデートのインストールルール**

ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

既定では、このオプションはオフです。

- **MSRC に基づく重要度レベルのアップデートのインストールルール**（Windows Update 更新プログラムでのみ使用可能）

  ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

  このオプションをオンにすると（Windows Update 更新プログラムでのみ使用可能）、MSRC（Microsoft Security Response Center）が設定する重要度レベルが、リストで選択した値（**低**、**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみがアップデートによって修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

  このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

  既定では、このオプションはオフです。

- **この製造元によるアップデートのインストールルール**（サードパーティ製品のアップデートでのみ使用可能）

  このオプションは、サードパーティ製アプリケーションのアップデートにのみ使用可能です。Kaspersky Security Center Cloud コンソールは、選択したアップデートと同じベンダーによって作成されたアプリケーションに関連するアップデートのみをインストールします。拒否された更新および他のベンダーが作成したアプリケーションの更新はインストールされません。

  既定では、このオプションはオフです。

- **種別「」のアップデートのインストールルール**
- **選択したアップデートのインストールルール**
- **選択したアップデートを承認**

  選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

  既定では、このオプションはオフです。

- **選択したアップデートのインストールに必要な以前のアップデートをすべて自動的にインストールする**

選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、このオプションをオンのままにします。

このオプションをオフにすると、選択したバージョンのアプリケーションのみがインストールされます。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、このオプションをオフにします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

たとえば、デバイスにアプリケーションのバージョン 3 がインストールされていて、バージョン 5 にアップデートしたいが、バージョン 5 はバージョン 4 経由のみでしかインストールできない状況を想定します。このオプションをオンにすると、先にバージョン 4 をインストールし、続いてバージョン 5 をインストールします。このオプションをオフにすると、アプリケーションのアップデートは失敗します。

既定では、このオプションはオンです。

c. ［**追加**］をクリックします。

- タスクを作成するには：

  a. ［**新規タスク**］をクリックします。

  b. 開いたページで、新しいルールを構成します：

  - **この重要度レベルのアップデートのインストールルール**

    ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

    このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

    このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

    既定では、このオプションはオフです。

  - **MSRC に基づく重要度レベルのアップデートのインストールルール**（Windows Update 更新プログラムでのみ使用可能）

    ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

    このオプションをオンにすると（Windows Update 更新プログラムでのみ使用可能）、MSRC（Microsoft Security Response Center）が設定する重要度レベルが、リストで選択した値（**低**、**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみがアップデートによって修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

    このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

    既定では、このオプションはオフです。

- **この製造元によるアップデートのインストールルール**（サードパーティ製品のアップデートでのみ使用可能）

  このオプションは、サードパーティ製アプリケーションのアップデートにのみ使用可能です。Kaspersky Security Center Cloud コンソールは、選択したアップデートと同じベンダーによって作成されたアプリケーションに関連するアップデートのみをインストールします。拒否された更新および他のベンダーが作成したアプリケーションの更新はインストールされません。

  既定では、このオプションはオフです。

- **種別「」のアップデートのインストールルール**

- **選択したアップデートのインストールルール**

- **選択したアップデートを承認**

  選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

  既定では、このオプションはオフです。

- **選択したアップデートのインストールに必要な以前のアップデートをすべて自動的にインストールする**

  選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、このオプションをオンのままにします。

  このオプションをオフにすると、選択したバージョンのアプリケーションのみがインストールされます。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、このオプションをオフにします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

  たとえば、デバイスにアプリケーションのバージョン 3 がインストールされていて、バージョン 5 にアップデートしたいが、バージョン 5 はバージョン 4 経由のみでしかインストールできない状況を想定します。このオプションをオンにすると、先にバージョン 4 をインストールし、続いてバージョン 5 をインストールします。このオプションをオフにすると、アプリケーションのアップデートは失敗します。

  既定では、このオプションはオンです。

c. ［**追加**］をクリックします。

タスクの開始を選択した場合は、ウィザードを閉じることができます。タスクはバックグラウンドモードで完了します。追加の操作は必要ありません。

ルールを既存のタスクに追加することを選択した場合は、タスクのプロパティウィンドウが開きます。新しいルールは既にタスクのプロパティに追加されています。ルールまたはその他のタスク設定を表示あるいは変更できます。［**保存**］をクリックして変更を保存します。

タスクの作成を選択した場合は、新規タスクウィザードで引き続きタスクを作成します。アップデートのインストールウィザードで追加した新しいルールが、新規タスクウィザードに表示されます。新規タスクウィザードを完了すると、［*アップデートのインストールと脆弱性の修正*］タスクがタスクリストに追加されます。

［脆弱性とアプリケーションのアップデートの検索］タスクの作成

脆弱性とアプリケーションのアップデートの検索タスクを使用して、Kaspersky Security Center Cloud コンソールは管理対象デバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。

［脆弱性とアプリケーションのアップデートの検索］タスクは、クイックスタートウィザードの実行時に自動作成されます。ウィザードを実行していない場合も、手動でタスクを作成できます。

［脆弱性とアプリケーションのアップデートの検索］タスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. Kaspersky Security Center Cloud コンソールを対象アプリケーションとするタスクから、［**脆弱性とアプリケーションのアップデートの検索**］タスク種別を選択します。
4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクを割り当てるデバイスを選択します。
6. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。
7. ［**作成**］をクリックします。

   タスクが作成され、タスクリストに表示されます。
8. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。
9. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。
10. ［**アプリケーション設定**］タブで、次の設定を指定します：

    - **Microsoft による脆弱性とアップデートのリストを検索する**

      脆弱性とアップデートの検索時に、Kaspersky Security Center Cloud コンソールは、現時点で使用可能な Microsoft Update のアップデート元からの該当する Microsoft Update の情報を使用します。

      Microsoft Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

      既定では、このオプションはオンです。

    - **アップデートサーバーに接続してアップデートを取得**

管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元として指定した場所に接続します。以下のサーバーを Microsoft Update のアップデート元として動作させることができます：

- Kaspersky Security Center Cloud コンソール管理サーバー（「ネットワークエージェントのポリシーの設定」を参照）
- 組織ネットワーク内で Microsoft Windows Server Update Services（WSUS）として機能している Windows Server
- Microsoft Update サーバー

このオプションをオンにすると、管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元に接続して、該当する Microsoft Windows Update の情報を最新にします。

このオプションをオフにすると、管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元から以前に入手してデバイス上のキャッシュに保存していた Microsoft Windows Update の情報を使用します。

Microsoft Update のアップデート元への接続は、多くのリソースを消費します。別のタスクまたはセクション［**ソフトウェアのアップデートと脆弱性**］のネットワークエージェントのポリシーのプロパティで、アップデート元へ定期的に接続するように設定している場合は、このオプションをオフにすることを検討してください。このオプションをオフにしない場合は、サーバーの負荷を下げるために、タスクの開始を 360 分以内でランダムに遅延させるようにタスクのスケジュールを設定できます。

既定では、このオプションはオンです。

ネットワークエージェントのポリシーの設定の各オプションの組み合わせに応じて、以下のようにアップデートの取得方法が異なります：

- 管理対象デバイス上の Windows Update エージェントが更新プログラムを取得するためにアップデートサーバーに接続するのは、［**アップデートサーバーに接続してアップデートを取得**］がオンで、［**Windows Update 検索モード**］セクションで［**アクティブ**］が選択されている場合のみです。
- 管理対象デバイス上の Windows Update エージェントが Microsoft Update のアップデート元から以前に入手してデバイス上のキャッシュに保存していた Microsoft Windows Update の情報を使用するのは［**アップデートサーバーに接続してアップデートを取得**］がオンでなおかつ［**Windows Update 検索モード**］セクションで［**パッシブ**］が選択されている場合か、［**アップデートサーバーに接続してアップデートを取得**］がオフでなおかつ［**Windows Update 検索モード**］セクションで［**アクティブ**］が選択されている場合です。
- ［**アップデートサーバーに接続してアップデートを取得**］がオンかオフかに関係なく、［**Windows Update 検索モード**］セクションで［**無効**］が選択されている場合、Kaspersky Security Center Cloud コンソールはアップデートに関する情報を要求しません。

- **カスペルスキーによるサードパーティ製品の脆弱性とアップデートのリストを検索する**

このオプションをオンにすると、Kaspersky Security Center Cloud コンソールは Windows のレジストリおよび［**ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**］で指定したフォルダーに存在するサードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）の脆弱性とアップデートを検索します。サポート対象のサードパーティ製品の全リストはカスペルスキーが管理しています。

このオプションをオフにすると、サードパーティ製品の脆弱性とアップデートの検索は行われません。Microsoft Windows Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

既定では、このオプションはオンです。

- **ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**

  Kaspersky Security Center Cloud コンソールが脆弱性の修正とアップデートのインストールが必要なアプリケーションを検索する時に対象とするフォルダーです。システム変数を使用できます。

  アプリケーションがインストールされているフォルダーを指定します。既定では、リストは空です。

- **詳細な診断を有効にする**

  このオプションをオンにすると、Kaspersky Security Center Cloud コンソールのリモート診断ユーティリティでネットワークエージェントによるトレースがオフになっていても、ネットワークエージェントがトレースを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

  このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center Cloud コンソールのリモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

  タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

  既定では、このオプションはオフです。

- **詳細な診断ファイルの最大サイズ（MB）**

  既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

11. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。

タスクの結果に 0x80240033「Windows Update Agent error 80240033（「License terms could not be downloaded.」）」エラーが含まれている場合、Windows レジストリを使用してこの問題を解決することができます。

脆弱性とアプリケーションのアップデートの検索タスクの設定

［*脆弱性とアプリケーションのアップデートの検索*］タスクは、クイックスタートウィザードの実行時に自動作成されます。ウィザードを実行していない場合も、手動でタスクを作成できます。

全般的なタスクの設定以外に、［*脆弱性とアプリケーションのアップデートの検索*］タスクでは、タスクの作成時または作成後に、作成したタスクのプロパティを編集する時に次の設定を指定できます：

- **Microsoft による脆弱性とアップデートのリストを検索する**

  脆弱性とアップデートの検索時に、Kaspersky Security Center Cloud コンソールは、現時点で使用可能な Microsoft Update のアップデート元からの該当する Microsoft Update の情報を使用します。

  Microsoft Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

  既定では、このオプションはオンです。

- **アップデートサーバーに接続してアップデートを取得**

管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元として指定した場所に接続します。以下のサーバーを Microsoft Update のアップデート元として動作させることができます：

- Kaspersky Security Center Cloud コンソール管理サーバー（「ネットワークエージェントのポリシーの設定」を参照）
- 組織ネットワーク内で Microsoft Windows Server Update Services（WSUS）として機能している Windows Server
- Microsoft Update サーバー

このオプションをオンにすると、管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元に接続して、該当する Microsoft Windows Update の情報を最新にします。

このオプションをオフにすると、管理対象デバイス上の Windows Update エージェントは Microsoft Update のアップデート元から以前に入手してデバイス上のキャッシュに保存していた Microsoft Windows Update の情報を使用します。

Microsoft Update のアップデート元への接続は、多くのリソースを消費します。別のタスクまたはセクション［**ソフトウェアのアップデートと脆弱性**］のネットワークエージェントのポリシーのプロパティで、アップデート元へ定期的に接続するように設定している場合は、このオプションをオフにすることを検討してください。このオプションをオフにしない場合は、サーバーの負荷を下げるために、タスクの開始を 360 分以内でランダムに遅延させるようにタスクのスケジュールを設定できます。

既定では、このオプションはオンです。

ネットワークエージェントのポリシーの設定の各オプションの組み合わせに応じて、以下のようにアップデートの取得方法が異なります：

- 管理対象デバイス上の Windows Update エージェントが更新プログラムを取得するためにアップデートサーバーに接続するのは、［**アップデートサーバーに接続してアップデートを取得**］がオンで、［**Windows Update 検索モード**］セクションで［**アクティブ**］が選択されている場合のみです。
- 管理対象デバイス上の Windows Update エージェントが Microsoft Update のアップデート元から以前に入手してデバイス上のキャッシュに保存していた Microsoft Windows Update の情報を使用するのは［**アップデートサーバーに接続してアップデートを取得**］がオンでなおかつ［**Windows Update 検索モード**］セクションで［**パッシブ**］が選択されている場合か、［**アップデートサーバーに接続してアップデートを取得**］がオフでなおかつ［**Windows Update 検索モード**］セクションで［**アクティブ**］が選択されている場合です。
- ［**アップデートサーバーに接続してアップデートを取得**］がオンかオフかに関係なく、［**Windows Update 検索モード**］セクションで［**無効**］が選択されている場合、Kaspersky Security Center Cloud コンソールはアップデートに関する情報を要求しません。

- **カスペルスキーによるサードパーティ製品の脆弱性とアップデートのリストを検索する**

このオプションをオンにすると、Kaspersky Security Center Cloud コンソールは Windows のレジストリおよび［**ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**］で指定したフォルダーに存在するサードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）の脆弱性とアップデートを検索します。サポート対象のサードパーティ製品の全リストはカスペルスキーが管理しています。

このオプションをオフにすると、サードパーティ製品の脆弱性とアップデートの検索は行われません。Microsoft Windows Update とサードパーティ製品それぞれで設定の異なるタスクを個別に作成する場合などに、このオプションをオフにすることを検討できます。

既定では、このオプションはオンです。

- **ファイルシステム内のアプリケーションを詳細検索するためのパスを指定します**

  Kaspersky Security Center Cloud コンソールが脆弱性の修正とアップデートのインストールが必要なアプリケーションを検索する時に対象とするフォルダーです。システム変数を使用できます。

  アプリケーションがインストールされているフォルダーを指定します。既定では、リストは空です。

- **詳細な診断を有効にする**

  このオプションをオンにすると、Kaspersky Security Center Cloud コンソールのリモート診断ユーティリティでネットワークエージェントによるトレースがオフになっていても、ネットワークエージェントがトレースを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

  このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center Cloud コンソールのリモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

  タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

  既定では、このオプションはオフです。

- **詳細な診断ファイルの最大サイズ（MB）**

  既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

タスクのスケジュールに関する推奨事項

［*脆弱性とアプリケーションのアップデートの検索*］タスクのスケジュールを設定する場合は、［**未実行のタスクを実行する**］と［**タスクの開始を自動的かつランダムに遅延させる**］の 2 つのオプションがオンになっていることを確認してください。

既定では、［*脆弱性とアプリケーションのアップデートの検索*］タスクは手動で開始するように設定されています。組織で採用されている規則などによりこの時刻にすべてのデバイスをシャットダウンするように定められている場合は、デバイスが再度電源オンになる時刻、つまり翌日の朝に、*脆弱性とアプリケーションのアップデートの検索*タスクが実行されます。脆弱性スキャン時には CPU とディスクサブシステムの負荷が増大するため、このように業務時間中に処理が実行されてしまうことが問題となる可能性があります。組織で採用されている職場のルールに基づいて、このタスクに対する最も効率的なスケジュールをセットアップする必要があります。

［アップデートのインストールと脆弱性の修正］タスクの作成

［*アップデートのインストールと脆弱性の修正*］タスクを利用できるかどうかは、Kaspersky Security Center Cloud コンソールのモードと現在のライセンスによって異なります。

［*アップデートのインストールと脆弱性の修正*］タスクは、管理対象デバイス上で Microsoft 製品やその他のサードパーティ製ソフトウェアの脆弱性をアップデートによって修正するために使用します。このタスクを使用することで、一定のルールに従って複数のアップデートをインストールしたり、複数の脆弱性を修正したりすることができます。

［*アップデートのインストールと脆弱性の修正*］タスクを使用してアップデートのインストールまたは脆弱性の修正を実行するには、次のうち1つの操作を実行します：

- アップデートのインストールウィザードまたは脆弱性修正ウィザードを実行します。
- ［*アップデートのインストールと脆弱性の修正*］タスクを作成します。
- 既存の［*アップデートのインストールと脆弱性の修正*］タスクにアップデートのインストールに関するルールを追加します。

ソフトウェアのアップデートのインストールタスクにはいくつかの制限があります。これらの制限は、Kaspersky Security Center Cloud コンソールで使用しているライセンスと、Kaspersky Security Center Cloud コンソールが機能しているモードによって異なります。

［アップデートのインストールと脆弱性の修正］タスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. Kaspersky Security Center Cloud コンソールを対象アプリケーションとするタスクから、［**アップデートのインストールと脆弱性の修正**］タスク種別を選択します。
4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクを割り当てるデバイスを選択します。
6. アップデートインストールのルールを指定してから、次の設定を指定します：

   - **デバイスの再起動時またはシャットダウン時にインストールを開始する**

     このオプションをオンにすると、デバイスの再起動時またはシャットダウン時にアップデートがインストールされます。オプションがオフの場合、アップデートのインストールはスケジュールに従って実行されます。

     アップデートのインストールによりデバイスのパフォーマンスに影響を与える可能性がある場合は、このオプションを使用します。

     既定では、このオプションはオフです。

   - **必要なシステムコンポーネントをインストールする**

     このオプションをオンにすると、アップデートのインストール前にインストールが必要な一般システムコンポーネントをすべて自動的にインストールします。インストールが必要な対象とは、たとえばオペレーティングシステムのアップデートなどです。

     このオプションをオフにすると、必須コンポーネントを手動でインストールすることが必要となる場合があります。

     既定では、このオプションはオフです。

- **アップデート中に新しい製品のバージョンのインストールを許可する**

  このオプションをオンにすると、製品の新しいバージョンをインストールするアップデートを許可できます。

  このオプションをオフにすると、製品はアップグレードされません。製品の新しいバージョンは手動でインストールするか、別のタスクを通してインストールできます。この設定は、所属企業のインフラストラクチャでソフトウェアの新しいバージョンがサポートされていなかったり、アップグレードをテスト環境で確認したい場合に使用します。

  既定では、このオプションはオンです。

  製品をアップデートすることにより、クライアントデバイスにインストールされた対象製品に依存するアプリケーションが正しく動作しなくなることがあります。

- **デバイスにアップデートをダウンロードするがインストールしない**

  このオプションをオンにすると、アップデートをデバイスにダウンロードしますが、自動ではインストールしません。ダウンロードされたアップデートを手動でインストールできます。

  Microsoft 製品のアップデートは、システム Windows フォルダーにダウンロードされます。サードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートは、［**アップデートのダウンロード先**］で指定したフォルダーにダウンロードされます。

  このオプションをオフにすると、アップデートはデバイスに自動的にインストールされません。

  既定では、このオプションはオフです。

- **アップデートのダウンロード用フォルダー**

  このフォルダーはサードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートのダウンロードに使用されます。

- **詳細な診断を有効にする**

  このオプションをオンにすると、Kaspersky Security Center Cloud コンソールのリモート診断ユーティリティでネットワークエージェントによるトレースがオフになっていても、ネットワークエージェントがトレースを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

  このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center Cloud コンソールのリモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

  タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

  既定では、このオプションはオフです。

- **詳細な診断ファイルの最大サイズ（MB）**

既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

7. OS の再起動設定：

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

- **通知の繰り返し間隔（分）**

  このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

  既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

  このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

- **再起動するまでの時間（分）**

  ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

  既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了するまで待機する時間（分）**

ユーザーのデバイスがロックされた場合にアプリケーションが強制終了されます（指定した非アクティブの時間が経過した後に自動で、または手動で）。

このオプションを有効にすると、入力フィールドに指定した時間を過ぎた時に、ロックされたデバイスでアプリケーションが強制的に終了します。

このオプションをオフにすると、ロックされたデバイスでアプリケーションは終了しません。

既定では、このオプションはオフです。

8. ［**タスク作成の終了**］ページで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

9. ［**終了**］をクリックします。

   タスクが作成され、タスクリストに表示されます。

10. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

11. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。

12. ［**保存**］をクリックします。

    タスクが指定した設定で作成されます。

タスクの結果に 0x80240033「Windows Update Agent error 80240033（「License terms could not be downloaded.」）」エラーが含まれている場合、Windows レジストリを使用してこの問題を解決することができます。

アップデートインストールのルールの追加

この機能を使用できるかどうかは、Kaspersky Security Center Cloud コンソールのモードと現在のライセンスによって異なります。

［*アップデートのインストールと脆弱性の修正*］タスクを使用してソフトウェアのアップデートをインストールする、またはソフトウェアの脆弱性を修正する場合は、アップデートインストールのルールを指定する必要があります。これらのルールにより、インストールするアップデートと修正する脆弱性が決定されます。

厳密な設定内容は、追加するルールがすべてのアップデート、Windows Update 更新プログラム、サードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートのいずれを対象とするのかによって異なります。Windows Update 更新プログラムまたはサードパーティ製品のアップデートのいずれかを対象にルールを追加する場合は、アップデートをインストールする特定のアプリケーションとバージョンを選択できます。すべてのアップデートのルールを追加する場合は、インストールする特定のアップデートおよびアップデートをインストールすることで修正する脆弱性を選択できます。

次の方法で、アップデートのインストールのルールを追加できます：

- 新規の［アップデートのインストールと脆弱性の修正］タスクの作成中にルールを追加する。
- 既存の［*アップデートのインストールと脆弱性の修正*］タスクの［**Application Settings**］タブでルールを追加する。

- アップデートのインストールウィザードまたは脆弱性修正ウィザード。

すべてのアップデートを対象とするルールを追加するには：

1. ［**追加**］をクリックします。
   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
2. ［**ルール種別**］ページで、［**すべてのアップデートのルール**］を選択します。
3. ［**全般基準**］ウィンドウで、ドロップダウンリストを使用して次の設定を指定します。
   - **インストールするアップデートの設定**

     クライアントデバイスにインストールする必要がある更新を選択します。
     - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
     - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
     - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。
   - **次のレベル以上の深刻度の脆弱性を修正する**

     ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

     このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

     このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

     既定では、このオプションはオフです。
4. ［**アップデート**］ウィンドウで、インストールするアップデートを選択します：
   - **すべての適用可能なアップデートをインストールする**

     ウィザードの［**全般基準**］ウィンドウで指定した基準に合致するソフトウェアアップデートをすべてインストールします。既定では、この項目が選択されます。
   - **リストのアップデートのみをインストールする**

     手動で選択したリストのソフトウェアアップデートのみをインストールします。追加できるアップデートには、使用可能なすべてのソフトウェアアップデートが含まれます。

     特定のアップデートを選択する状況としてはたとえば、テスト環境でのインストールの確認、重要なアプリケーションのみのアップデート、特定のアプリケーションのみのアップデートなどが考えられます。

- **選択したアップデートのインストールに必要な以前のアップデートをすべて自動的にインストールする**

  選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、このオプションをオンのままにします。

  このオプションをオフにすると、選択したバージョンのアプリケーションのみがインストールされます。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、このオプションをオフにします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

  たとえば、デバイスにアプリケーションのバージョン 3 がインストールされていて、バージョン 5 にアップデートしたいが、バージョン 5 はバージョン 4 経由のみでしかインストールできない状況を想定します。このオプションをオンにすると、先にバージョン 4 をインストールし、続いてバージョン 5 をインストールします。このオプションをオフにすると、アプリケーションのアップデートは失敗します。

  既定では、このオプションはオンです。

5. ［**脆弱性**］ウィンドウで、選択したアップデートのインストールで修正する脆弱性を選択します：

   - **他の基準に一致するすべての脆弱性を修正する**

     ウィザードの［**全般基準**］ウィンドウで指定した基準に合致する脆弱性をすべて修正します。既定では、この項目が選択されます。

   - **リストの脆弱性のみを修正する**

     手動で選択したリストの脆弱性のみをインストールします。追加できるアップデートには、検知されたすべての脆弱性が含まれます。

     特定の脆弱性を選択する状況としてはたとえば、テスト環境での脆弱性の修正の確認、重要なアプリケーションのみでの脆弱性の修正、特定のアプリケーションのみでの脆弱性の修正などが考えられます。

6. ［**名前**］ページで、追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**設定**］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが追加され、新規タスクウィザードまたはタスクのプロパティに表示されます。

Windows Update 更新プログラムを対象とする新しいルールを追加するには：

1. ［**追加**］をクリックします。

   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

2. ［**ルール種別**］ページで、［**Windows Update のルール**］を選択します。

3. ［**全般基準**］ウィンドウで、次の設定を指定します：

   - **インストールするアップデートの設定**

クライアントデバイスにインストールする必要がある更新を選択します。

- **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
- **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
- **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。

- **次のレベル以上の深刻度の脆弱性を修正する**

  ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

  このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

  このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

  既定では、このオプションはオフです。

- **次のレベル以上の MSRC 深刻度の脆弱性を修正する**

  ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

  このオプションをオンにすると、MSRC（Microsoft Security Response Center）が設定する重要度レベルが、リストで選択した値（**低**、**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

  このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

  既定では、このオプションはオフです。

4. ［**アプリケーション**］ウィンドウで、アップデートをインストールするアプリケーションとアプリケーションのバージョンを選択します。既定では、すべてのアプリケーションがオンです。

5. ［**アップデートのカテゴリ**］ウィンドウで、インストールするアップデートのカテゴリを選択します。これらのカテゴリは Microsoft Update カタログで使用されているのと同じカテゴリです。既定では、すべてのカテゴリがオンです。

6. ［**名前**］ページで、追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**設定**］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが追加され、新規タスクウィザードまたはタスクのプロパティに表示されます。

サードパーティ製品のアップデートを対象とする新しいルールを追加するには：

1. ［**追加**］をクリックします。
   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
2. ［**ルール種別**］ページで、［**サードパーティ製品のアップデートのルール**］を選択します。
3. ［**全般基準**］ウィンドウで、次の設定を指定します：

   - **インストールするアップデートの設定**

     クライアントデバイスにインストールする必要がある更新を選択します。
     - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
     - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
     - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。

   - **次のレベル以上の深刻度の脆弱性を修正する**

     ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

     このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

     このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

     既定では、このオプションはオフです。

4. ［**アプリケーション**］ウィンドウで、アップデートをインストールするアプリケーションとアプリケーションのバージョンを選択します。既定では、すべてのアプリケーションがオンです。
5. ［**名前**］ページで、追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［設定］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが追加され、新規タスクウィザードまたはタスクのプロパティに表示されます。

［Windows Update 更新プログラムのインストール］タスクの作成

［Windows Update 更新プログラムのインストール］タスクを使用することで、Windows Update サービス経由で提供されるソフトウェアのアップデートをクライアントデバイスにインストールできます。

ソフトウェアのアップデートのインストールタスクにはいくつかの制限があります。これらの制限は、Kaspersky Security Center Cloud コンソールで使用しているライセンスと、Kaspersky Security Center Cloud コンソールが機能しているモードによって異なります。

［Windows Update 更新プログラムのインストール］タスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. Kaspersky Security Center Cloud コンソールを対象アプリケーションとするタスクから、［**Windows Update 更新プログラムのインストール**］タスク種別を選択します。
4. 作成中のタスク名を入力します。
   タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクを割り当てるデバイスを選択します。
6. ［**追加**］をクリックします。
   アップデートのリストが表示されます。
7. インストールする Windows Update 更新プログラムを選択し、［**OK**］をクリックします。
8. OS の再起動設定を指定します。

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

- **通知の繰り返し間隔（分）**

このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

- **再起動するまでの時間（分）**

ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

既定では、このオプションはオフです。

9. 次のようにアカウントの設定を指定します。

- **既定のアカウント**

タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。

既定では、このオプションがオンです。

- **アカウントの指定**

［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

- **アカウント**

タスクを実行するアカウント。

- **パスワード**

タスクが実行されるアカウントのパスワード。

10. 既定のタスク設定を編集する場合、［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

11. ［**終了**］をクリックします。

    タスクが作成され、タスクリストに表示されます。

12. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

13. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。

14. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。

サードパーティ製品の使用可能なアップデートに関する情報の表示

クライアントデバイスにインストールされた Microsoft 製品やその他のサードパーティ製ソフトウェアに対して適用可能なアップデートのリストを表示できます。

クライアントデバイスにインストールされたサードパーティ製ソフトウェアに対して適用可能なアップデートのリストを表示するには、

メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動します。

適用可能なアップデートのリストが表示されます。

ソフトウェアアップデートのリストの表示では、フィルターを指定できます。ソフトウェアアップデートのリストの右上にある**フィルター**アイコン（）をクリックして、フィルターを指定してください。ソフトウェア脆弱性のリストの上の［**設定済みのフィルター**］ドロップダウンリストから、いずれかの設定済みのフィルターを選択することもできます。

アップデートのプロパティを表示するには：

1. 目的のソフトウェアのアップデートの名前をクリックします。

2. アップデートのプロパティウィンドウが開き、次のタブごとにまとめられた情報が表示されます：

   - **全般**

このタブには、選択したアップデートの一般的な詳細が表示されます。

- 承認ステータスのアップデート（ドロップダウンリストの新しいステータスをオンにすると、手動で変更できます）
- アップデートが属する Windows Server Update Services（WSUS）カテゴリ
- アップデートが登録された日時
- アップデートが作成された日時
- アップデートの重要度
- アップデートによって適用されるインストール要件
- アップデートが属するアプリケーションファミリー
- アップデートが適用されるアプリケーション
- アップデートのリビジョン番号

- **属性**

このタブには、選択したアップデートに関する詳細情報の取得に使用できる一連の属性が表示されます。表示される属性は、アップデートの公開元が Microsoft かサードパーティかによって異なります。

このタブには、Microsoft のアップデートに関する次の情報が表示されます：

- Microsoft Security Response Center（MSRC）によって定義されたアップデートの重要度
- アップデートについて説明しているマイクロソフトサポート技術情報の記事へのリンク
- アップデートについて説明しているマイクロソフトセキュリティ情報の記事へのリンク
- アップデートの識別子（ID）

このタブには、サードパーティの更新プログラムに関する次の情報が表示されます：

- アップデートがパッチか、または配布パッケージか
- アップデートのローカリゼーション言語
- アップデートが自動インストールか手動インストールか
- 適用後にアップデートが取り消されたかどうか
- アップデートをダウンロードするためのリンク

- **デバイス**

このタブには、選択したアップデートがインストールされているデバイスのリストが表示されます。

- **修正済みの脆弱性**

  このタブには、選択したアップデートで修正できる脆弱性のリストが表示されます。

- **アップデートの重複**

  このタブには、同じアプリケーションに対して公開された複数のアップデート間で起こり得るクロスオーバーが表示されます。つまり、選択したアップデートが他のアップデートより優先されるか、逆に他のアップデートが優先されるかを表示します（Microsoft のアップデートでのみ使用可能）。

- **このアップデートをインストールするタスク**

  このタブには、選択したアップデートのインストールをスコープに含むタスクのリストが表示されます。このタブでは、アップデート用の新しいリモートインストールタスクを作成することもできます。

アップデートのインストールの統計情報を表示するには：

1. 目的のソフトウェアのアップデートに隣接するチェックボックスをオンにします。
2. ［**アップデートのインストールステータスの統計**］をクリックします。

   アップデートのインストールステータスを示した図表が表示されます。それぞれのステータスをクリックすると、選択したステータスのアップデートが存在するデバイスのリストが表示されます。

Windows を使用している選択した管理対象デバイスにインストールされた Microsoft 製品やその他のサードパーティ製ソフトウェアに対して適用可能なアップデートのリストを表示できます。

選択した管理対象デバイスにインストールされているサードパーティ製ソフトウェアに対して適用可能なアップデートのリストを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。

   管理対象デバイスのリストが表示されます。

2. 管理対象デバイスのリストで、サードパーティ製ソフトウェアのアップデートを表示するデバイスの名前のリンクをクリックします。

   選択したデバイスのプロパティウィンドウが表示されます。

3. 選択したデバイスのプロパティウィンドウで、［**詳細**］タブを選択します。
4. 左側のペインで、［**適用可能なアップデート**］セクションを選択します。インストール済みのアップデートのみを表示する場合は、［**インストールされたアップデートの表示**］をオンにします。

   選択したデバイス上で適用可能なサードパーティ製ソフトウェアのアップデートのリストが表示されます。

使用可能なソフトウェアアップデートのリストのファイルへのエクスポート

Microsoft 製品やその他のサードパーティ製ソフトウェアに対するアップデートとして表示されているアップデートのリストを、CSV ファイルまたは TXT ファイルにエクスポートできます。エクスポートしたファイルは、情報セキュリティ部門に共有したり、統計情報を取得するために保存するなどの用途に使用できます。

管理対象デバイスにインストールされているサードパーティ製ソフトウェアに対して適用可能なすべてのアップデートのリストをファイルにエクスポートするには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動します。

   管理対象デバイスにインストールされているサードパーティ製ソフトウェアに対して適用可能なすべてのアップデートのリストが表示されます。

2. エクスポートするファイルの形式に応じて、［**TXT へエクスポート**］または［**CSV へエクスポート**］をクリックします。

   操作に使用しているデバイスに、Microsoft 製品やその他のサードパーティ製ソフトウェアに対して適用可能なアップデートのリストをエクスポートしたファイルがダウンロードされます。

選択した管理対象デバイスにインストールされているサードパーティ製ソフトウェアに対して適用可能なアップデートのリストをファイルにエクスポートするには：

1. 選択した管理対象デバイスに対して適用可能なサードパーティ製ソフトウェアのアップデートのリストが表示されます。

2. エクスポートするソフトウェアアップデート項目を選択します。

   ソフトウェアアップデートのリストをそのままエクスポートする場合は、この手順をスキップします。

   ただし、ソフトウェアアップデートのリストをそのままエクスポートする場合でも、エクスポートできるのはウィンドウで現在表示されているアップデート項目のみです。

   インストール済みのアップデートのみをエクスポートする場合、［**インストールされたアップデートの表示**］をオンにします。

3. エクスポートするファイルの形式に応じて、［**TXT へエクスポート**］または［**CSV へエクスポート**］をクリックします。

   操作に使用しているデバイスに、選択した管理対象デバイスにインストールされている Microsoft 製品やその他のサードパーティ製ソフトウェアに対して適用可能なアップデートのリストをエクスポートしたファイルがダウンロードされます。

サードパーティ製ソフトウェアのアップデートの拒否と承認

［*アップデートのインストールと脆弱性の修正*］タスクを設定する際には、アップデートに特定のステータスが割り当てられていることをインストールの要件とするルールを作成できます。たとえば、次のようなステータスのアップデートのインストールのみを許可するようにルールを設定できます：

- 承認済みのアップデートのみ
- 承認済みのアップデートとステータスが未定義のアップデートのみ
- すべてのアップデート（ステータスを考慮しない）

インストールする必要のあるアップデートを承認し、インストールしないアップデートを拒否します。

アップデートのインストールを管理するための「*承認*」ステータスの使用は、アップデート量が少ない場合に効率的です。複数のアップデートをインストールするには、［*アップデートのインストールと脆弱性の修正*］タスクで構成できるルールを使用します。ルールで指定された基準を満たさない特定のアップデートに対してのみ、「*承認*」ステータスを設定することを推奨します。大量のアップデートを手動で承認すると、管理サーバーのパフォーマンスが低下し、サーバーが過負荷状態になる場合があります。

1 つ以上のアップデートを承認または拒否するには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動します。
   適用可能なアップデートのリストが表示されます。
2. 承認または拒否するアップデートを選択します。
3. 選択したアップデートを承認する場合は［**承認**］を、拒否する場合は［**承認却下**］を選択します。
   既定値は［*未定義*］です。

   選択したアップデートのステータスが、指定したステータスに変更されます。

オプションとして、特定のアップデートのプロパティで承認ステータスを変更できます。

プロパティでアップデートを承認または拒否するには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアのアップデート**］の順に移動します。
   適用可能なアップデートのリストが表示されます。
2. 承認または拒否するアップデートの名前をクリックします。
   アップデートのプロパティウィンドウが開きます。
3. ［**全般**］セクションで、［**アップデート承認の状況**］を変更してアップデートのステータスを選択します。［*承認*］、［*承認却下*］、または［*未定義*］のいずれかのステータスを選択できます。
4. ［**保存**］をクリックして変更を保存します。

   選択したアップデートのステータスが、指定したステータスに変更されます。

サードパーティ製のソフトウェアアップデートに［**拒否**］ステータスを設定すると、このアップデートは、アップデートのインストールを予定しているがまだ完了していないデバイスにはインストールされません。アップデートをインストール済みのデバイスには、これらのアップデートがそのまま残ります。アップデートを削除する時は、手動でローカル削除できます。

サードパーティ製品の自動アップデート

一部のサードパーティ製品は自動的にアップデートできます。アプリケーションの製造元は、アプリケーションが自動アップデート機能をサポートするかどうかを定義します。管理対象デバイスにインストールされているサードパーティ製品が自動アップデートをサポートしている場合は、アプリケーションのプロパティで自動アップデートの設定を指定できます。自動アップデート設定の変更後、ネットワークエージェントは、アプリケーションがインストールされている各管理対象デバイスにその新しい設定を適用します。

自動アップデートの設定は、脆弱性とパッチ管理機能の他のオブジェクトと設定から独立しています。たとえば、この設定はアップデート承認の状況や、［*アップデートのインストールと脆弱性の修正*］、［*Windows Update 更新プログラムのインストール*］、［*脆弱性の修正*］などのアップデートのインストールタスクには依存しません。

サードパーティ製品の自動アップデート設定を行うには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。
2. 自動アップデート設定を変更するアプリケーションの名前をクリックします。
   検索を簡略化するには、［**自動アップデートのステータス**］列でリストをフィルタリングできます。
   アプリケーションプロパティのウィンドウが開きます。
3. ［**全般**］セクションで、次の設定の値を選択します：
   自動アップデートのステータス

   次のいずれかのオプションをオンにします：

   - **未定義**
     自動アップデート機能は無効になっています。Kaspersky Security Center Cloud コンソールは、［*アップデートのインストールと脆弱性の修正*］、［*Windows Update 更新プログラムのインストール*］、［*脆弱性の修正*］の各タスクを使用して、サードパーティ製品のアップデートをインストールします。
   - **許可**
     製造元がアプリケーションのアップデートをリリースすると、このアップデートは管理対象デバイスに自動的にインストールされます。追加の操作は必要ありません。
   - **ブロック**
     アプリケーションのアップデートは自動的にインストールされません。Kaspersky Security Center Cloud コンソールは、［*アップデートのインストールと脆弱性の修正*］、［*Windows Update 更新プログラムのインストール*］、［*脆弱性の修正*］の各タスクを使用して、サードパーティ製品のアップデートをインストールします。
4. ［**保存**］をクリックして変更を保存します。

選択したアプリケーションに自動アップデートの設定が適用されます。

サードパーティ製ソフトウェアの脆弱性の修正

このセクションでは、管理対象デバイスにインストールされているソフトウェアの脆弱性の修正に関連する Kaspersky Security Center Cloud コンソールの機能について説明します。

シナリオ：ソフトウェアの脆弱性の検知と修正

このセクションでは Windows オペレーティングシステムを使用しているデバイスで、脆弱性を検知し修正する方法について説明しています。オペレーティングシステムとサードパーティ製ソフトウェア（Microsoft 製品を含む）の脆弱性の検知と修正を実行できます。

必須条件

- 組織内に Kaspersky Security Center Cloud コンソールが導入されている。
- 組織内に Windows を使用している管理対象デバイスが存在する。

実行するステップ

ソフトウェアの脆弱性の検知と修正は、次の手順で進みます：

1. **クライアントデバイスにインストールされているソフトウェアの脆弱性のスキャン**

   管理対象デバイスにインストールされているソフトウェアの脆弱性を検知するには、［*脆弱性とアプリケーションのアップデートの検索*］タスクを実行します。タスクが完了すると、Kaspersky Security Center Cloud コンソールはタスクのプロパティで指定したデバイスにインストールされているサードパーティ製ソフトウェアについて、検知された脆弱性と必要なアップデートのリストを取得します。

   ［*脆弱性とアプリケーションのアップデートの検索*］タスクは、Kaspersky Security Center Cloud コンソールのクイックスタートウィザードによって自動的に作成されます。ウィザードを実行していない場合は、次の手順に進む前にウィザードを実行するか手動でタスクを作成してください。

   実行手順の説明：脆弱性とアプリケーションのアップデートの検索の作成

2. **検知されたソフトウェアの脆弱性の分析**

   ［**ソフトウェアの脆弱性**］リストを確認して、どの脆弱性を修正するかを決定します。それぞれの脆弱性の詳細情報を確認するには、リスト内の脆弱性の名前をクリックします。リスト内のそれぞれの脆弱性について、管理対象デバイス上の脆弱性に関する統計情報を表示することもできます。

   実行手順の説明：

   - ソフトウェアの脆弱性に関する情報の表示
   - 管理対象デバイス上の脆弱性に関する統計情報の表示

3. **脆弱性の修正の設定**

   管理対象デバイス上でソフトウェアの脆弱性が検知された場合、［*アップデートのインストールと脆弱性の修正*］タスクまたは［*脆弱性の修正*］タスクを使用して、ソフトウェア脆弱性を修正できます。

   ［*アップデートのインストールと脆弱性の修正*］タスクは、管理対象デバイス上で Microsoft 製品やその他のサードパーティ製ソフトウェアの脆弱性をアップデートによって修正するために使用します。このタスクを使用することで、一定のルールに従って複数のアップデートをインストールしたり、複数の脆弱性を修正したりすることができます。このタスクを使用できるかどうかは、Kaspersky Security Center Cloud コンソールのモードと現在のライセンスによって異なります。ソフトウェア脆弱性を修正するために、［*アップデートのインストールと脆弱性の修正*］タスクは推奨されるソフトウェアアップデートを使用します。

   ［*脆弱性の修正*］タスクは、推奨される Microsoft 製品の修正を使用します。

   脆弱性修正ウィザードを起動すると、これらのタスクのいずれかを自動的に作成できます。または、手動でタスクを作成することもできます。

   実行手順の説明：サードパーティ製ソフトウェアの脆弱性の修正、［アップデートのインストールと脆弱性の修正］タスクの作成

4. **タスクのスケジュール設定**

脆弱性のリストを最新の状態に維持するため、［*脆弱性とアプリケーションのアップデートの検索*］タスクが定期的に自動で実行されるようにスケジュールを指定してください。推奨される平均的なタスクの実行頻度は週に1回です。

［*アップデートのインストールと脆弱性の修正*］タスクを作成している場合は、実行頻度を［*脆弱性とアプリケーションのアップデートの検索*］と同じかそれよりも少なくします。［*脆弱性の修正*］タスクのスケジュールを設定する場合は、タスクを開始する前に、毎回 Microsoft 製品の修正を選択する必要があることに注意してください。

タスクのスケジュールを指定する場合は、［*脆弱性とアプリケーションのアップデートの検索*］タスクが完了してからこれらのタスクが開始するようにしてください。

5. **検知されたソフトウェアの脆弱性への非対応の判断（必要に応じて実施）**

   必要に応じて、すべてのデバイス上または選択した特定のデバイス上で、ソフトウェアの脆弱性を無視できます。

   実行手順の説明：ソフトウェアの脆弱性の無視

6. **脆弱性の修正タスクの実行**

   ［*アップデートのインストールと脆弱性の修正*］タスクまたは［*脆弱性の修正*］タスクを開始します。タスクが完了したら、タスクリストでのタスクのステータスが［*正常終了*］になっていることを確認します。

7. **ソフトウェアの脆弱性の修正結果のレポートの作成（省略可能）**

   脆弱性の修正に関する詳細な統計情報を確認するには、脆弱性レポートを生成します。レポートには、修正されなかったソフトウェアの脆弱性に関する情報が表示されます。これにより、組織内での Microsoft 製品やその他のサードパーティ製ソフトウェアの脆弱性の検知と修正の状況を把握することができます。

   実行手順の説明：レポートの生成と表示

8. **サードパーティ製ソフトウェアの脆弱性の検知と修正に関する設定の確認**

   以下を確認します：

   - 管理対象デバイスのソフトウェアの脆弱性のリストが空ではない。
   - 脆弱性を修正するタスクがタスクリストに含まれている。
   - ソフトウェアの脆弱性を検索するタスクの後に修正するタスクが開始されるように、スケジュールを指定した。スケジュールを比較するには、これらのタスクのプロパティを表示します。
   - ソフトウェアの脆弱性を修正するタスクが正常に完了した。タスクのプロパティウィンドウの［**履歴**］タブで情報を表示します。

結果

［*アップデートのインストールと脆弱性の修正*］タスクを作成した場合、管理対象デバイス上の脆弱性が自動的に修正されます。タスクの実行時に、適用可能なソフトウェアアップデートのリストとタスクの設定で指定されたルールとが照合されます。ルールの条件に一致するすべてのソフトウェアアップデートがディストリビューションポイントのリポジトリにダウンロードされ、ソフトウェアの脆弱性を修正するためにインストールされます。

［*脆弱性の修正*］タスクを作成した場合、Microsoft 製品のソフトウェア脆弱性のみが修正されます。

ソフトウェアの脆弱性の検知と修正

Kaspersky Security Center Cloud コンソールでは、Microsoft Windows オペレーティングシステムを実行している管理対象デバイスのソフトウェアの脆弱性を検知して修正することができます。オペレーティングシステムとサードパーティ製ソフトウェア（Microsoft 製品を含む）の脆弱性が検知されます。

ソフトウェア脆弱性の検知

Kaspersky Security Center Cloud コンソールは、既知の脆弱性のデータベースと Windows Update のデータベースに記録されている特性を使用して、ソフトウェアの脆弱性を検知します。既知の脆弱性のデータベースは、カスペルスキーの担当者によって作成および維持されます。データベースには、脆弱性の説明、脆弱性の検知日、脆弱性の深刻度などの情報が含まれています。アプリケーションの脆弱性に関する詳細情報は、カスペルスキーの Web サイトにあります。

Kaspersky Security Center Cloud コンソールは［*脆弱性とアプリケーションのアップデートの検索*］タスクを使用してソフトウェア脆弱性を検知します。

ソフトウェア脆弱性の修正

Kaspersky Security Center Cloud コンソールは、ソフトウェアの製造元から提供されているソフトウェアのアップデートを使用してソフトウェア脆弱性を修正します。ソフトウェア脆弱性のリストはいつでも表示できます。ソフトウェアアップデートのメタデータは管理サーバーのリポジトリに自動的にダウンロードされ、［*ディストリビューションポイントのリポジトリにアップデートをダウンロード*］タスクの実行結果としてディストリビューションポイントのリポジトリにダウンロードされます。このタスクは Kaspersky Security Center Cloud コンソールのクイックスタートウィザードで、または手動で作成できます。

脆弱性を修正するためのソフトウェアのアップデートは、配布パッケージまたはパッチの形式で提供されます。ソフトウェアの脆弱性を修正するソフトウェアのアップデートは、「*修正*」という名称で呼ばれます。Kaspersky Security Center Cloud コンソールでは、*推奨される修正*を使用して脆弱性を修正します。推奨される修正は、カスペルスキーの担当者がインストールを推奨するソフトウェアのアップデートです。

Kaspersky Security Center Cloud コンソールのモードと現在のライセンスに応じて、［*アップデートのインストールと脆弱性の修正*］タスクまたは［*脆弱性の修正*］タスクを使用してソフトウェアの脆弱性を修正できます。

［*アップデートのインストールと脆弱性の修正*］タスクは、推奨される修正をインストールすることで自動的に複数の脆弱性を修正します。このタスクを使用する場合、脆弱性を修正するためのルールを手動で指定できます。

［*脆弱性の修正*］タスクを使用すると、Microsoft 製品向けに推奨される修正をインストールして脆弱性を修正できます。

セキュリティ上の理由から、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートすべてに対して、カスペルスキーの技術によるマルウェアのスキャンが自動的に実行されます。この技術は自動的なファイルのチェックに使用され、ウイルススキャン、Sandbox 環境における静的分析、動的分析、ふるまい分析、機械学習が含まれます。

カスペルスキーは、脆弱性とパッチ管理機能を使用してインストールされたサードパーティ製品のアップデートを手動で分析することはありません。さらに、カスペルスキーの専門家は脆弱性（既知または未知）や文書化されていないアップデートの機能について確認したり、上記で指定されているもの以外のアップデートの分析を行ったりすることはありません。

ソフトウェアのアップデートのインストールタスクにはいくつかの制限があります。これらの制限は、Kaspersky Security Center Cloud コンソールで使用しているライセンスと、Kaspersky Security Center Cloud コンソールが機能しているモードによって異なります。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが起動している場合、終了するように指示される場合があります。

一部のソフトウェアに関する脆弱性の修正では、ソフトウェアのインストールについて使用許諾契約書（EULA）への同意を要求された場合、EULA に同意する必要があります。EULA に同意しない場合、ソフトウェアの脆弱性は修正されません。

修正された各脆弱性に関する情報は、管理サーバーに 90 日間保存されます。その後、自動的に削除されます。

ソフトウェア脆弱性の修正

ソフトウェアの脆弱性のリストの取得が完了すると、Windows オペレーティングシステムを使用している管理対象デバイスでソフトウェアの脆弱性を修正できます。Microsoft 製品を含めて、オペレーティングシステムとサードパーティ製ソフトウェアの脆弱性を修正するには、［*脆弱性の修正*］タスクまたは［*アップデートのインストールと脆弱性の修正*］タスクを作成して実行します。

ソフトウェアのアップデートのインストールタスクにはいくつかの制限があります。これらの制限は、Kaspersky Security Center Cloud コンソールで使用しているライセンスと、Kaspersky Security Center Cloud コンソールが機能しているモードによって異なります。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが起動している場合、終了するように指示される場合があります。

オプションとして、次の方法でソフトウェアの脆弱性を修正するタスクを作成できます：

- 脆弱性リストを開き、修正する脆弱性を指定する。

  その結果、ソフトウェアの脆弱性を修正する新しいタスクが作成されます。オプションとして、選択した脆弱性を既存のタスクに追加できます。

- 脆弱性修正ウィザードを実行する。

  この機能を使用できるかどうかは、Kaspersky Security Center Cloud コンソールのモードと現在のライセンスによって異なります。

  このウィザードを使用すると、脆弱性の修正タスクの作成と設定手順が簡略化され、インストールするのと同じアップデートで構成される冗長なタスクを作成せずに済みます。

脆弱性リストを使用してソフトウェアの脆弱性を修正する

ソフトウェアの脆弱性を修正するには：

1. 脆弱性のリストの 1 つを開きます：

   - 一般的な脆弱性のリストを開くには、メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアの脆弱性**］の順に移動します。

- 管理対象デバイスの脆弱性のリストを開くには、メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］→［**<デバイス名>**］→［**詳細**］→［**ソフトウェアの脆弱性**］の順に移動します。
- 特定のアプリケーションの脆弱性のリストを開くには、メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］→［**<製品名>**］→［**脆弱性**］の順に移動します。

サードパーティ製ソフトウェアの脆弱性のリストを掲載したページが表示されます。

2. リストから1つ以上の脆弱性を選択して、［**脆弱性の修正**］をクリックします。

選択した脆弱性の一部について推奨されるソフトウェアアップデートが存在しない場合、通知メッセージが表示されます。

一部のソフトウェアに関する脆弱性の修正では、ソフトウェアのインストールについて使用許諾契約書（EULA）への同意を要求された場合、EULA に同意する必要があります。使用許諾契約書に同意しない場合、脆弱性は修正されません。

3. 次のいずれかのオプションをオンにします：

- **新規タスク**

  新規タスクウィザードが起動します。Kaspersky Security Center Cloud コンソールのモードと現在のライセンスに応じて、［*アップデートのインストールと脆弱性の修正*］タスクまたは［*脆弱性の修正*］タスクが事前に選択されています。ウィザードの手順に従って、タスクの作成を完了します。

- **脆弱性の修正（指定したタスクにルールを追加）**

  選択した脆弱性を追加するタスクを選択します。Kaspersky Security Center Cloud コンソールのモードと現在のライセンスに応じて、［*アップデートのインストールと脆弱性の修正*］タスクまたは［*脆弱性の修正*］タスクを選択します。［*アップデートのインストールと脆弱性の修正*］タスクを選択すると、選択した脆弱性を修正するための新しいルールが、選択したタスクに自動的に追加されます。［*脆弱性の修正*］タスクを選択すると、選択した脆弱性がタスクのプロパティに追加されます。

  タスクのプロパティウィンドウが開きます。［**保存**］をクリックして変更を保存します。

タスクの作成を選択した場合は、タスクが作成され、タスクリスト（［**アセット（デバイス）**］→［**タスク**］）に表示されます。脆弱性を既存のタスクに追加することを選択した場合、脆弱性はタスクのプロパティに保存されます。

サードパーティ製ソフトウェアの脆弱性を修正するには、［*アップデートのインストールと脆弱性の修正*］タスク、または［*脆弱性の修正*］タスクを開始します。作成したタスクが［*脆弱性の修正*］タスクである場合は、タスクの設定リストに含まれているソフトウェアの脆弱性を修正するためのソフトウェアアップデートを手動で指定する必要があります。

脆弱性修正ウィザードを使用してソフトウェアの脆弱性を修正する

脆弱性修正ウィザードを使用できるかどうかは、使用するライセンスと Kaspersky Security Center Cloud コンソールが機能しているモードに応じて異なります。

脆弱性修正ウィザードを使用してソフトウェアの脆弱性を修正するには：

1. メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアの脆弱性**］の順に移動します。

管理対象デバイスにインストールされているサードパーティ製ソフトウェアの脆弱性のリストを掲載したページが表示されます。

2. 修正する脆弱性に隣接するチェックボックスをオンにします。

3. ［**脆弱性修正ウィザードを実行**］をクリックします。

   脆弱性修正ウィザードが起動します。［**脆弱性を修正するタスクを選択**］ページには、次の種別の既存の全タスクのリストが表示されます。

   - *アップデートのインストールと脆弱性の修正*
   - *Windows Update 更新プログラムのインストール*
   - *脆弱性の修正*

   最後の 2 つの種別のタスクを変更して新しいアップデートをインストールすることはできません。新しいアップデートをインストールする際に使用できるのは、［*アップデートのインストールと脆弱性の修正*］タスクのみです。

4. 選択した脆弱性を修正するタスクのみをウィザードに表示する場合は、［**この脆弱性を修正するタスクのみ表示**］をオンにします。

5. 目的の対象を追加します：

   - タスクを開始するには、タスク名の横にあるチェックボックスをオンにして、［**開始**］をクリックします。
   - 既存のタスクに新しいルールを追加するには：

     a. タスク名に隣接するチェックボックスをオンにし、［**ルールの追加**］をクリックします。

     b. 開いたページで、新しいルールを構成します：

     - **この深刻度の脆弱性すべてを修正するルール**

       ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

       このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

       このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

       既定では、このオプションはオフです。

     - **選択した脆弱性に対して推奨されるものとして定義されているアップデートと同じタイプのアップデートによって脆弱性を修正するためのルール**（Microsoftソフトウェアの脆弱性でのみ適用可能）
     - **選択した製造元のアプリケーションの脆弱性を修正するルール**（サードパーティ製ソフトウェアの脆弱性に対してのみ使用可能）
     - **選択したアプリケーションのすべてのバージョンの脆弱性を修正するルール**（サードパーティ製ソフトウェアの脆弱性に対してのみ使用可能）
     - **選択した脆弱性を修正するルール**
     - **この脆弱性を修正するアップデートを承認する**

選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

既定では、このオプションはオフです。

c. ［**追加**］をクリックします。

- タスクを作成するには：

a. ［**新規タスク**］をクリックします。

b. 開いたページで、新しいルールを構成します：

- **この深刻度の脆弱性すべてを修正するルール**

ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

既定では、このオプションはオフです。

- **種別「」のアップデートを使用して脆弱性を修正するルール**（Microsoft ソフトウェアの脆弱性でのみ適用可能）
- **選択した製造元のアプリケーションの脆弱性を修正するルール**（サードパーティ製ソフトウェアの脆弱性に対してのみ使用可能）
- **選択したアプリケーションのすべてのバージョンの脆弱性を修正するルール**（サードパーティ製ソフトウェアの脆弱性に対してのみ使用可能）
- **選択した脆弱性を修正するルール**
- **この脆弱性を修正するアップデートを承認する**

選択したアップデートのインストールが承認されます。アップデートのインストールルールの一部で、承認されたアップデートのみインストールが許可されている場合、このオプションをオンにします。

既定では、このオプションはオフです。

c. ［**追加**］をクリックします。

タスクの開始を選択した場合は、ウィザードを閉じることができます。タスクはバックグラウンドモードで完了します。追加の操作は必要ありません。

ルールを既存のタスクに追加することを選択した場合は、タスクのプロパティウィンドウが開きます。新しいルールは既にタスクのプロパティに追加されています。ルールまたはその他のタスク設定を表示あるいは変更できます。［**保存**］をクリックして変更を保存します。

タスクの作成を選択した場合は、新規タスクウィザードで引き続きタスクを作成します。脆弱性修正ウィザードで追加した新しいルールは、新規タスクウィザードに表示されます。新規タスクウィザードを完了すると、［*Install required updates and fix vulnerabilities*］タスクがタスクリストに追加されます。

脆弱性の修正タスクの作成

［*脆弱性の修正*］タスクを使用すると、Windows を実行している管理対象デバイスの Microsoft ソフトウェアの脆弱性を修正できます。

この機能を使用できるかどうかは、Kaspersky Security Center Cloud コンソールのモードと現在のライセンスによって異なります。［*アップデートのインストールと脆弱性の修正*］タスクを、［*脆弱性の修正*］の代わりに使用することを推奨します。［*アップデートのインストールと脆弱性の修正*］タスクを使用すると、定義したルールに従って、複数の更新をインストールし、複数の脆弱性を自動的に修正できます。

ソフトウェアのアップデートのインストールタスクにはいくつかの制限があります。これらの制限は、Kaspersky Security Center Cloud コンソールで使用しているライセンスと、Kaspersky Security Center Cloud コンソールが機能しているモードによって異なります。

管理対象デバイス上のサードパーティアプリケーションをアップデートしたり、サードパーティアプリケーションの脆弱性を修正したりする場合、ユーザーの操作が必要になる場合があります。たとえば、サードパーティのアプリケーションが起動している場合、終了するように指示される場合があります。

脆弱性の修正タスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
3. Kaspersky Security Center Cloud コンソールを対象アプリケーションとするタスクから、［**脆弱性の修正**］タスク種別を選択します。
4. 作成中のタスク名を入力します。
   タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクを割り当てるデバイスを選択します。
6. ［**追加**］をクリックします。
   脆弱性のリストが表示されます。
7. 修正する脆弱性を選択し、［**OK**］をクリックします。
8. OS の再起動設定を指定します。
   - **デバイスを再起動しない**

操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

- **通知の繰り返し間隔（分）**

  このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

  既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

  このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

- **再起動するまでの時間（分）**

  ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

  既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了する**

  アプリケーションを実行すると、クライアントデバイスの再起動が妨げられる場合があります。たとえば、ドキュメント作成アプリケーションでドキュメントを編集しており、その内容が保存されていない場合、アプリケーションはデバイスの再起動を許可しません。

  このオプションをオンにすると、ブロックされたデバイス上のアプリケーションが、再起動の前に強制的に閉じられます。これにより、保存していなかった作業内容が失われる場合があります。

  このオプションをオフにすると、ブロックされたデバイスは再起動されません。このデバイス上のタスクのステータスでは、デバイスの再起動が必要であることが表示されます。ブロックされたデバイスでは、実行中のアプリケーションすべてをユーザーが手動で終了し、デバイスを再起動する必要があります。

  既定では、このオプションはオフです。

9. 次のようにアカウントの設定を指定します。

- **既定のアカウント**

  タスクを実行するアプリケーションと同じアカウントでタスクが実行されます。
  既定では、このオプションがオンです。

- **アカウントの指定**

  ［**アカウント**］と［**パスワード**］に、タスクを実行するアカウントの情報を入力します。アカウントには、当該タスクの実行に必要な権限が付与されている必要があります。

- **アカウント**

  タスクを実行するアカウント。

- **パスワード**

  タスクが実行されるアカウントのパスワード。

10. ［**タスク作成の終了**］ページで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

11. ［**終了**］をクリックします。
    タスクが作成され、タスクリストに表示されます。

12. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

13. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。

14. ［**保存**］をクリックします。

タスクが指定した設定で作成されます。

［アップデートのインストールと脆弱性の修正］タスクの作成

［*アップデートのインストールと脆弱性の修正*］タスクを利用できるかどうかは、Kaspersky Security Center Cloud コンソールのモードと現在のライセンスによって異なります。

［*アップデートのインストールと脆弱性の修正*］タスクは、管理対象デバイス上で Microsoft 製品やその他のサードパーティ製ソフトウェアの脆弱性をアップデートによって修正するために使用します。このタスクを使用することで、一定のルールに従って複数のアップデートをインストールしたり、複数の脆弱性を修正したりすることができます。

［*アップデートのインストールと脆弱性の修正*］タスクを使用してアップデートのインストールまたは脆弱性の修正を実行するには、次のうち 1 つの操作を実行します：

- アップデートのインストールウィザードまたは脆弱性修正ウィザードを実行します。
- ［*アップデートのインストールと脆弱性の修正*］タスクを作成します。
- 既存の［*アップデートのインストールと脆弱性の修正*］タスクにアップデートのインストールに関するルールを追加します。

ソフトウェアのアップデートのインストールタスクにはいくつかの制限があります。これらの制限は、Kaspersky Security Center Cloud コンソールで使用しているライセンスと、Kaspersky Security Center Cloud コンソールが機能しているモードによって異なります。

［アップデートのインストールと脆弱性の修正］タスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。

   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. Kaspersky Security Center Cloud コンソールを対象アプリケーションとするタスクから、［**アップデートのインストールと脆弱性の修正**］タスク種別を選択します。
4. 作成中のタスク名を入力します。タスク名は 100 文字以下で、特殊文字（"*<>?\:|）を含めることはできません。
5. タスクを割り当てるデバイスを選択します。
6. アップデートインストールのルールを指定してから、次の設定を指定します：

   - **デバイスの再起動時またはシャットダウン時にインストールを開始する**

     このオプションをオンにすると、デバイスの再起動時またはシャットダウン時にアップデートがインストールされます。オプションがオフの場合、アップデートのインストールはスケジュールに従って実行されます。

     アップデートのインストールによりデバイスのパフォーマンスに影響を与える可能性がある場合は、このオプションを使用します。

     既定では、このオプションはオフです。

   - **必要なシステムコンポーネントをインストールする**

     このオプションをオンにすると、アップデートのインストール前にインストールが必要な一般システムコンポーネントをすべて自動的にインストールします。インストールが必要な対象とは、たとえばオペレーティングシステムのアップデートなどです。

     このオプションをオフにすると、必須コンポーネントを手動でインストールすることが必要となる場合があります。

     既定では、このオプションはオフです。

   - **アップデート中に新しい製品のバージョンのインストールを許可する**

このオプションをオンにすると、製品の新しいバージョンをインストールするアップデートを許可できます。

このオプションをオフにすると、製品はアップグレードされません。製品の新しいバージョンは手動でインストールするか、別のタスクを通してインストールできます。この設定は、所属企業のインフラストラクチャでソフトウェアの新しいバージョンがサポートされていなかったり、アップグレードをテスト環境で確認したい場合に使用します。

既定では、このオプションはオンです。

製品をアップデートすることにより、クライアントデバイスにインストールされた対象製品に依存するアプリケーションが正しく動作しなくなることがあります。

- **デバイスにアップデートをダウンロードするがインストールしない**

このオプションをオンにすると、アップデートをデバイスにダウンロードしますが、自動ではインストールしません。ダウンロードされたアップデートを手動でインストールできます。

Microsoft 製品のアップデートは、システム Windows フォルダーにダウンロードされます。サードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートは、［**アップデートのダウンロード先**］で指定したフォルダーにダウンロードされます。

このオプションをオフにすると、アップデートはデバイスに自動的にインストールされません。

既定では、このオプションはオフです。

- **アップデートのダウンロード用フォルダー**

このフォルダーはサードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートのダウンロードに使用されます。

- **詳細な診断を有効にする**

このオプションをオンにすると、Kaspersky Security Center Cloud コンソールのリモート診断ユーティリティでネットワークエージェントによるトレースがオフになっていても、ネットワークエージェントがトレースを書き込みます。トレースは 2 つのファイルに交互に書き込まれます。2 つのファイルの合計サイズの上限は、［**詳細な診断ファイルの最大サイズ（MB）**］で指定した値となります。2 つのファイルの容量が上限に達したら、ネットワークエージェントは上書きを開始します。トレースが書き込まれたファイルは %WINDIR%\Temp フォルダーに保存されます。これらのファイルはリモート診断ユーティリティからアクセスでき、ダウンロードや削除を実行できます。

このオプションをオフにすると、ネットワークエージェントによるトレースの書き込みは Kaspersky Security Center Cloud コンソールのリモート診断ユーティリティの設定に従って実行されます。追加のトレースは書き込まれません。

タスクの作成時に、詳細な診断を有効にする必要はありません。一部のデバイスで任意のタスクの実行が失敗し、もう一度タスクを実行する時に追加情報を収集する必要があるなどの場合に、この機能を有効にできます。

既定では、このオプションはオフです。

- **詳細な診断ファイルの最大サイズ（MB）**

既定値は 100 MB で、1 MB から 2048 MB までの値を指定できます。お客様が送信した詳細な診断ファイルの情報量がトラブルシューティングを行う上で不十分だった場合、テクニカルサポートの担当者から既定値の変更を要求される場合があります。

7. OS の再起動設定：

- **デバイスを再起動しない**

  操作後に、クライアントデバイスは自動的には再起動されません。操作を完了するには、デバイスを再起動する必要があります（手動で、またはデバイスの管理タスクを使用して）。必要な再起動についての情報は、タスク履歴とデバイスのステータスに保存されます。このオプションは、継続的な稼働が不可欠なサーバーなどのデバイスで実行するタスクに適切です。

- **デバイスを再起動する**

  インストールの完了に再起動が必要な場合は常に、クライアントデバイスは自動的に再起動されます。このオプションは、定期的に稼働が一時停止（シャットダウンまたは再起動）するデバイスのタスクに有用です。

- **ユーザーに処理を確認する**

  手動で再起動を要求する再起動リマインダーがクライアントデバイスの画面に表示されます。このオプションで、いくつかの詳細設定を定義可能です：ユーザーに表示されるメッセージテキスト、メッセージの表示頻度、（ユーザーの確認なしに）再起動が強制実行されるまでの時間。このオプションは、ユーザーにとって最も好都合な時間を指定して再起動できることが要求されるワークステーションに最適です。

  既定では、このオプションがオンです。

- **通知の繰り返し間隔（分）**

  このオプションをオンにすると、オペレーティングシステムを再起動するように、ユーザーへのメッセージが指定された頻度で表示されます。

  既定では、このオプションはオンです。既定の間隔は 5 分です。1 分から 1,440 分までの値を指定できます。

  このオプションをオフにすると、確認メッセージは 1 回だけ表示されます。

- **再起動するまでの時間（分）**

  ユーザーへの確認メッセージを表示した後で、指定した時間が経過すると、強制的にオペレーティングシステムが再起動します。

  既定では、このオプションはオンです。既定の間隔は 30 分です。1 分から 1,440 分までの値を指定できます。

- **セッションがブロックされたアプリケーションを強制終了するまで待機する時間（分）**

  ユーザーのデバイスがロックされた場合にアプリケーションが強制終了されます（指定した非アクティブの時間が経過した後に自動で、または手動で）。

  このオプションを有効にすると、入力フィールドに指定した時間を過ぎた時に、ロックされたデバイスでアプリケーションが強制的に終了します。

  このオプションをオフにすると、ロックされたデバイスでアプリケーションは終了しません。

  既定では、このオプションはオフです。

8. ［**タスク作成の終了**］ページで［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、既定のタスク設定を編集できます。このオプションをオフにすると、既定の設定でタスクが作成されます。既定の設定からの変更は、後からいつでも実行できます。

9. ［**終了**］をクリックします。
   タスクが作成され、タスクリストに表示されます。

10. 作成したタスクの名前をクリックし、タスクのプロパティウィンドウを開きます。

11. タスクのプロパティウィンドウで、タスクの全般的な設定を指定します。

12. ［**保存**］をクリックします。
    タスクが指定した設定で作成されます。

タスクの結果に 0x80240033「Windows Update Agent error 80240033（「License terms could not be downloaded.」）」エラーが含まれている場合、Windows レジストリを使用してこの問題を解決することができます。

アップデートインストールのルールの追加

この機能を使用できるかどうかは、Kaspersky Security Center Cloud コンソールのモードと現在のライセンスによって異なります。

［*アップデートのインストールと脆弱性の修正*］タスクを使用してソフトウェアのアップデートをインストールする、またはソフトウェアの脆弱性を修正する場合は、アップデートインストールのルールを指定する必要があります。これらのルールにより、インストールするアップデートと修正する脆弱性が決定されます。

厳密な設定内容は、追加するルールがすべてのアップデート、Windows Update 更新プログラム、サードパーティ製品（カスペルスキーと Microsoft 以外の製造元が作成した製品）のアップデートのいずれを対象とするのかによって異なります。Windows Update 更新プログラムまたはサードパーティ製品のアップデートのいずれかを対象にルールを追加する場合は、アップデートをインストールする特定のアプリケーションとバージョンを選択できます。すべてのアップデートのルールを追加する場合は、インストールする特定のアップデートおよびアップデートをインストールすることで修正する脆弱性を選択できます。

次の方法で、アップデートのインストールのルールを追加できます：

- 新規の［アップデートのインストールと脆弱性の修正］タスクの作成中にルールを追加する。
- 既存の［*アップデートのインストールと脆弱性の修正*］タスクの［**Application Settings**］タブでルールを追加する。
- アップデートのインストールウィザードまたは脆弱性修正ウィザード。

すべてのアップデートを対象とするルールを追加するには：

1. ［**追加**］をクリックします。
   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

2. ［**ルール種別**］ページで、［**すべてのアップデートのルール**］を選択します。

3. ［**全般基準**］ウィンドウで、ドロップダウンリストを使用して次の設定を指定します。

- **インストールするアップデートの設定**

  クライアントデバイスにインストールする必要がある更新を選択します。

  - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
  - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
  - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。

- **次のレベル以上の深刻度の脆弱性を修正する**

  ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

  このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

  このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

  既定では、このオプションはオフです。

4. ［**アップデート**］ウィンドウで、インストールするアップデートを選択します：

- **すべての適用可能なアップデートをインストールする**

  ウィザードの［**全般基準**］ウィンドウで指定した基準に合致するソフトウェアアップデートをすべてインストールします。既定では、この項目が選択されます。

- **リストのアップデートのみをインストールする**

  手動で選択したリストのソフトウェアアップデートのみをインストールします。追加できるアップデートには、使用可能なすべてのソフトウェアアップデートが含まれます。

  特定のアップデートを選択する状況としてはたとえば、テスト環境でのインストールの確認、重要なアプリケーションのみのアップデート、特定のアプリケーションのみのアップデートなどが考えられます。

- **選択したアップデートのインストールに必要な以前のアップデートをすべて自動的にインストールする**

選択したアップデートのインストールに必要な場合に中間バージョンのインストールに同意する時は、このオプションをオンのままにします。

このオプションをオフにすると、選択したバージョンのアプリケーションのみがインストールされます。途中のバージョンのアプリケーションをインストールせずに、アプリケーションを目的のバージョンまで直接アップデートしたい場合は、このオプションをオフにします。以前のバージョンのアプリケーションをインストールせずに選択したアップデートをインストールできない場合は、アプリケーションのアップデートは失敗します。

たとえば、デバイスにアプリケーションのバージョン 3 がインストールされていて、バージョン 5 にアップデートしたいが、バージョン 5 はバージョン 4 経由のみでしかインストールできない状況を想定します。このオプションをオンにすると、先にバージョン 4 をインストールし、続いてバージョン 5 をインストールします。このオプションをオフにすると、アプリケーションのアップデートは失敗します。

既定では、このオプションはオンです。

5. ［**脆弱性**］ウィンドウで、選択したアップデートのインストールで修正する脆弱性を選択します：

   - **他の基準に一致するすべての脆弱性を修正する**

     ウィザードの［**全般基準**］ウィンドウで指定した基準に合致する脆弱性をすべて修正します。既定では、この項目が選択されます。

   - **リストの脆弱性のみを修正する**

     手動で選択したリストの脆弱性のみをインストールします。追加できるアップデートには、検知されたすべての脆弱性が含まれます。

     特定の脆弱性を選択する状況としてはたとえば、テスト環境での脆弱性の修正の確認、重要なアプリケーションのみでの脆弱性の修正、特定のアプリケーションのみでの脆弱性の修正などが考えられます。

6. ［**名前**］ページで、追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**設定**］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが追加され、新規タスクウィザードまたはタスクのプロパティに表示されます。

Windows Update 更新プログラムを対象とする新しいルールを追加するには：

1. ［**追加**］をクリックします。

   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

2. ［**ルール種別**］ページで、［**Windows Update のルール**］を選択します。

3. ［**全般基準**］ウィンドウで、次の設定を指定します：

   - **インストールするアップデートの設定**

クライアントデバイスにインストールする必要がある更新を選択します。

- **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
- **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
- **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。

- **次のレベル以上の深刻度の脆弱性を修正する**

ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

既定では、このオプションはオフです。

- **次のレベル以上の MSRC 深刻度の脆弱性を修正する**

ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

このオプションをオンにすると、MSRC（Microsoft Security Response Center）が設定する重要度レベルが、リストで選択した値（**低**、**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

既定では、このオプションはオフです。

4. ［**アプリケーション**］ウィンドウで、アップデートをインストールするアプリケーションとアプリケーションのバージョンを選択します。既定では、すべてのアプリケーションがオンです。

5. ［**アップデートのカテゴリ**］ウィンドウで、インストールするアップデートのカテゴリを選択します。これらのカテゴリは Microsoft Update カタログで使用されているのと同じカテゴリです。既定では、すべてのカテゴリがオンです。

6. ［**名前**］ページで、追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［**設定**］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが追加され、新規タスクウィザードまたはタスクのプロパティに表示されます。

サードパーティ製品のアップデートを対象とする新しいルールを追加するには：

1. ［**追加**］をクリックします。
   ルール作成ウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
2. ［**ルール種別**］ページで、［**サードパーティ製品のアップデートのルール**］を選択します。
3. ［**全般基準**］ウィンドウで、次の設定を指定します：

   - **インストールするアップデートの設定**

     クライアントデバイスにインストールする必要がある更新を選択します。
     - **承認されたアップデートのみをインストール**：承認されたアップデートのみをインストールします。
     - **（拒否されたもの以外の）すべてのアップデートをインストール**：承認ステータスが［*承認*］または［*未定義*］のアップデートをインストールします。
     - **（拒否されたものも含め）すべてのアップデートをインストール**：承認ステータスに依存せず、すべてのアップデートをインストールします。このオプションを使用する時は、よく検討してください。使用例としてはたとえば、拒否されたアップデートをテスト環境にインストールして確認してみる場合などがあります。

   - **次のレベル以上の深刻度の脆弱性を修正する**

     ソフトウェアのアップデートを適用することで、ソフトウェアのユーザーエクスペリエンスを損なってしまう場合があります。この場合、ソフトウェアの動作にとって重要なアップデートのみをインストールし、その他のアップデートのインストールは行わないようにすることができます。

     このオプションをオンにすると、カスペルスキーが設定する重要度レベルが、リストで選択した値（**中**、**高**、**緊急**のいずれか）と同じかそれより高い脆弱性のみが修正されます。選択した値より重要度レベルが低い脆弱性は修正されません。

     このオプションをオフにすると、重要度レベルに依存せず、アップデートはすべての脆弱性を修正します。

     既定では、このオプションはオフです。

4. ［**アプリケーション**］ウィンドウで、アップデートをインストールするアプリケーションとアプリケーションのバージョンを選択します。既定では、すべてのアプリケーションがオンです。
5. ［**名前**］ページで、追加するルールの名前を指定します。この名前は、作成したタスクのプロパティウィンドウを開くことで、後から［設定］セクションで変更できます。

ルール作成ウィザードを完了すると、新しいルールが追加され、新規タスクウィザードまたはタスクのプロパティに表示されます。

管理対象デバイスで検知されたすべてのソフトウェア脆弱性に関する情報の表示

管理対象デバイスでのソフトウェア脆弱性のスキャンが完了すると、管理対象デバイスで検知されたすべてのソフトウェア脆弱性を表示できます。

管理対象デバイスで検知されたすべてのソフトウェア脆弱性のリストを表示するには：

メインメニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアの脆弱性**］の順に移動します。

クライアントデバイスで検知されたソフトウェア脆弱性のリストが表示されます。

脆弱性レポートの生成と表示も実行できます。

ソフトウェア脆弱性のリストの表示では、フィルターを指定できます。ソフトウェア脆弱性のリストの右上にある**フィルター**アイコン（）をクリックして、フィルターを指定してください。ソフトウェア脆弱性のリストの上の［**設定済みのフィルター**］ドロップダウンリストから、いずれかの設定済みのフィルターを選択することもできます。

リスト内の任意の脆弱性に関する詳細情報を取得できます。

ソフトウェア脆弱性に関する情報を取得するには：

ソフトウェア脆弱性のリストで、脆弱性の名前のリンクをクリックします。

ソフトウェアの脆弱性のプロパティウィンドウが開きます。

指定した管理対象デバイスで検知されたソフトウェア脆弱性に関する情報の表示

指定した管理対象の Windows デバイスで検知されたソフトウェア脆弱性に関する情報を表示できます。

指定した管理対象デバイスで検知されたソフトウェア脆弱性のリストを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、検知されたソフトウェア脆弱性を表示するデバイスの名前のリンクをクリックします。
   選択したデバイスのプロパティウィンドウが表示されます。
3. 選択したデバイスのプロパティウィンドウで、［**詳細**］タブを選択します。
4. 左側のペインで、［**ソフトウェアの脆弱性**］セクションを選択します。
   修正可能なソフトウェア脆弱性のみを表示するには、［**修正可能な脆弱性のみ表示**］をオンにします。

選択した管理対象デバイスで検知された脆弱性のリストが表示されます。

選択したソフトウェア脆弱性のプロパティを表示するには：

ソフトウェア脆弱性のリストで、脆弱性の名前のリンクをクリックします。

選択したソフトウェア脆弱性のプロパティウィンドウが表示されます。

管理対象デバイス上の脆弱性に関する統計情報の表示

管理対象デバイス上でのそれぞれのソフトウェア脆弱性に関する統計情報を表示できます。統計情報は図表として表示されます。図表には、次のステータスごとに該当するデバイス数が表示されます：

- *無視：<デバイス数>*：脆弱性のプロパティでその脆弱性を無視するように手動で設定した場合に、このステータスが割り当てられます。
- *修正済み：<デバイス数>*：脆弱性を修正するためのタスクが正常に完了した場合に、このステータスが割り当てられます。
- *修正をスケジュール済み：<デバイス数>*：脆弱性を修正するためのタスクを作成済みだが、タスクがまだ実行されていない場合に、このステータスが割り当てられます。
- *パッチが適用済み：<デバイス数>*：脆弱性の修正をするためのソフトウェアのアップデートを手動で選択したが、そのソフトウェアのアップデートでは脆弱性が修正されていない場合に、このステータスが割り当てられます。
- *修正が必要：<デバイス数>*：脆弱性の修正が管理対象デバイスの一部でのみ行われ、それ以外の管理対象デバイスでは修正が必要になっている場合に、このステータスが割り当てられます。

管理対象デバイス上の脆弱性に関する統計情報を表示するには：

1. メイン メニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアの脆弱性**］の順に移動します。
   管理対象デバイスで検知されたソフトウェア脆弱性のリストが表示されます。
2. 目的の脆弱性に隣接するチェックボックスをオンにします。
3. ［**デバイスの脆弱性の統計**］をクリックします。

脆弱性のステータスを示した図表が表示されます。それぞれのステータスをクリックすると、選択したステータスの脆弱性が存在するデバイスのリストが表示されます。

ソフトウェア脆弱性のリストのファイルへのエクスポート

表示されている脆弱性のリストを CSV ファイルまたは TXT ファイルにエクスポートできます。エクスポートしたファイルは、情報セキュリティ部門に共有したり、統計情報を取得するために保存するなどの用途に使用できます。

管理対象デバイスで検知されたすべてのソフトウェア脆弱性のリストをファイルにエクスポートするには：

1. メイン メニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアの脆弱性**］の順に移動します。
   管理対象デバイスで検知されたソフトウェア脆弱性のリストが表示されます。
2. エクスポートするファイルの形式に応じて、［**TXT へエクスポート**］または［**CSV へエクスポート**］をクリックします。

操作に使用しているデバイスに、ソフトウェア脆弱性のリストをエクスポートしたファイルがダウンロードされます。

選択した管理対象デバイスで検知されたソフトウェア脆弱性のリストをファイルにエクスポートするには：

1. 選択した管理対象デバイスで検知されたソフトウェア脆弱性のリストを表示します。
2. エクスポートするソフトウェア脆弱性項目を選択します。

   選択した管理対象デバイスで検知されたソフトウェア脆弱性のリストをそのままエクスポートする場合は、この手順をスキップします。

   ただし、選択した管理対象デバイスで検知されたソフトウェア脆弱性のリストをそのままエクスポートする場合でも、エクスポートできるのはウィンドウで現在表示されている脆弱性項目のみです。
3. エクスポートするファイルの形式に応じて、［**TXT へエクスポート**］または［**CSV へエクスポート**］をクリックします。

操作に使用しているデバイスに、選択した管理対象デバイスで検知されたソフトウェア脆弱性のリストをエクスポートしたファイルがダウンロードされます。

検知されたソフトウェアの脆弱性への非対応の判断

必要に応じて、検知されたソフトウェア脆弱性を無視することもできます。ソフトウェア脆弱性に対応しない理由として、次が考えられます：

- 管理者として、該当するソフトウェアの脆弱性が組織内で緊急なものではないと判断した場合。
- 脆弱性の修正を適用すると、該当するソフトウェアでデータの破損などが生じる可能性があることが判明した場合。
- 管理者として、管理対象デバイスを保護する別の対策を使用しているため、ソフトウェア脆弱性が組織ネットワークにとって危険ではないと判断した場合。

すべてのデバイス上または選択した特定のデバイス上で、ソフトウェア脆弱性を無視できます。

すべての管理対象デバイスで、特定のソフトウェア脆弱性に対応せずに無視するには：

1. メイン メニューで、［**操作**］→［**パッチの管理**］→［**ソフトウェアの脆弱性**］の順に移動します。

   管理対象デバイスで検知されたソフトウェア脆弱性のリストが表示されます。
2. ソフトウェア脆弱性のリストで、対応せずに無視する脆弱性の名前のリンクをクリックします。

   ソフトウェア脆弱性のプロパティウィンドウが開きます。
3. ［**全般**］タブで、［**脆弱性を無視**］をオンにします。
4. ［**保存**］をクリックします。

   ソフトウェア脆弱性のプロパティウィンドウが閉じます。

すべての管理対象デバイスで、対象のソフトウェア脆弱性が無視されます。

選択した管理対象デバイスで、特定のソフトウェア脆弱性に対応せずに無視するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。

   管理対象デバイスのリストが表示されます。

2. 管理対象デバイスのリストで、特定のソフトウェア脆弱性を無視するデバイスの名前のリンクをクリックします。

   デバイスのプロパティウィンドウが表示されます。

3. デバイスのプロパティウィンドウで［**詳細**］タブを選択します。

4. 左側のペインで、［**ソフトウェアの脆弱性**］セクションを選択します。

   デバイスで検知された脆弱性のリストが表示されます。

5. ソフトウェア脆弱性のリストで、選択しているデバイス上で対応せずに無視する脆弱性を選択します。

   ソフトウェア脆弱性のプロパティウィンドウが開きます。

6. ソフトウェア脆弱性のプロパティウィンドウの［**全般**］タブで、［**脆弱性を無視**］をオンにします。

7. ［**保存**］をクリックします。

   ソフトウェア脆弱性のプロパティウィンドウが閉じます。

8. デバイスのプロパティウィンドウを閉じます。

選択したデバイスで、対象のソフトウェア脆弱性が無視されます。

無視することを選択したソフトウェアの脆弱性は、［*脆弱性の修正*］タスクまたは［*アップデートのインストールと脆弱性の修正*］タスクが完了しても修正されません。脆弱性のリストで、無視することを選択した脆弱性をフィルターを使用して表示から除外することができます。

対応済みの脆弱性に関する情報を保管する期間

管理対象デバイス上ですでに対応済みの脆弱性に関する情報をデータベースに保管する期間を設定するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. 表示されたページで、［**イベントリポジトリ**］タブに移動します。

3. 対応済みの脆弱性に関する情報をデータベースに保管する期間を指定します。

   既定の保管する期間は、試用モードで 7 日間、製品モードで 60 日間です。上限は、試用モードで 14 日間、製品モードで 365 日間です。

4. ［**保存**］をクリックします。

脆弱性に関する情報をデータベースに保管する期間が指定した日数に制限されます。

クライアントデバイス上で実行されるアプリケーションの管理

このセクションでは、クライアントデバイス上で実行されるアプリケーションの管理と関連する Kaspersky Security Center Cloud コンソールの機能について説明します。

シナリオ：アプリケーションの管理

クライアントデバイス上でのアプリケーションの起動を管理できます。管理対象デバイス上でのアプリケーションの起動を許可またはブロックできます。この用途には、アプリケーションコントロール機能を使用します。Windows または Linux デバイスにインストールされているアプリケーションのみを管理できます。

Linux ベースのオペレーティングシステムの場合、Application Control コンポーネントは Kaspersky Endpoint Security 11.2 for Linux 以降から使用できます。

必須条件

- 組織内に Kaspersky Security Center Cloud コンソールが導入されている。
- Kaspersky Endpoint Security for Windows または Kaspersky Endpoint Security for Linux のポリシーが作成され、有効になっている。

実行するステップ

アプリケーションコントロールのユーザーシナリオは次のステップに分かれています：

1. **クライアントデバイスにインストールされているアプリケーションのリストの作成と表示**

   このステップでは、管理対象デバイスにどのようなアプリケーションがインストールされているかを把握できます。アプリケーションのリストを確認しながら、所属組織のセキュリティポリシーに応じて、どのアプリケーションの使用を許可してどのアプリケーションの使用を禁止するかを判断してください。組織の情報セキュリティポリシーに関連した制限が必要になる場合もあります。管理対象デバイスにどのようなアプリケーションがインストールされているかを、既に正確に把握できている場合は、このステップをスキップできます。

   実行手順の説明：クライアントデバイスにインストールされているアプリケーションのリストの取得と表示

2. **クライアントデバイス上の実行ファイルのリストの作成と表示**

   このステップでは、管理対象デバイスでどのような実行ファイルが検知されたかを把握できます。実行ファイルのリストを表示して、許可対象の実行ファイルと禁止対象の実行ファイルのリストと照合してください。組織の情報セキュリティポリシーに関連した制限が実行ファイルに対して必要になる場合もあります。管理対象デバイスにどのような実行ファイルが存在するかを、既に正確に把握できている場合は、このステップをスキップできます。

   実行手順の説明：クライアントデバイスにインストールされている実行ファイルのリストの取得と表示

3. **組織内で使用されているアプリケーションのアプリケーションカテゴリの作成**

   管理対象デバイスに保管されているアプリケーションと実行ファイルのリストを分析します。分析結果に基づいて、アプリケーションカテゴリを作成します。組織内で標準的に使用されているアプリケーションで構成される「作業アプリケーション」カテゴリを作成すると有用です。様々なセキュリティグループが仕事で異なるアプリケーションセットを使用している場合は、セキュリティグループごとに別個のアプリケーションカテゴリを作成できます。

   アプリケーションカテゴリを作成する基準によって、作成できるアプリケーションカテゴリの種別は 2 つに分かれます。

   実行手順の説明：コンテンツが手動で追加されるアプリケーションカテゴリの作成、選択したデバイスの実行ファイルを含むアプリケーションカテゴリの作成

4. **Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定**

   上述したステップで作成したアプリケーションカテゴリを使用して、Kaspersky Endpoint Security for Windows ポリシー内でアプリケーションコントロール機能を設定します。

   実行手順の説明：Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定

5. **アプリケーションコントロール機能のテストモードでの有効化**

   アプリケーションコントロールルールが業務で必要なアプリケーションをブロックしないことを確認するため、新規ルールの作成後にテストを有効にして動作を検証することを推奨します。テストモードで実行している場合、Kaspersky Endpoint Security for Windows は、アプリケーションコントロールルールで起動が禁止されているアプリケーションをブロックせず、その起動について管理サーバーに通知します。

   アプリケーションコントロールルールのテストでは、次の手順の実施を推奨します：

   - 必要に応じたテスト期間を指定する。必要なテスト期間は数日から 2 カ月ほどまで、ルールに応じて異なります。
   - アプリケーションコントロールの動作テストによって記録されたイベントを分析する。

   実行手順の説明：Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定。これらの手順に従って、設定プロセスでテストモードを有効にします。

6. **アプリケーションコントロール機能におけるアプリケーションカテゴリの設定の変更**

   必要に応じて、アプリケーションコントロール設定に変更を行います。テスト結果に応じて、アプリケーションコントロール機能のイベントに関連していた実行ファイルを「手動でコンテンツを追加するカテゴリ」に追加できます。

   実行手順の説明：イベントに関連する実行ファイルのアプリケーションカテゴリへの追加

7. **アプリケーションコントロールルールの実運用での適用**

   アプリケーションコントロールルールのテストとアプリケーションカテゴリの設定が完了したら、実際にアプリケーションコントロールルールを適用できます。

   実行手順の説明：Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定。これらの手順に従って、設定プロセスでテストモードを無効にします。

8. **アプリケーションコントロールの設定の検証**

   以下を確認します：

   - アプリケーションカテゴリのリストが空ではない。アプリケーションカテゴリのリストを表示し、設定したカテゴリが含まれていることを確認します。
   - アプリケーションカテゴリを使用してアプリケーションコントロールが作成されている。Kaspersky Endpoint Security for Windows ポリシーの設定を表示して、［**アプリケーション設定**］→［**セキュリティコントロール**］→［**アプリケーションコントロール**］でアプリケーションコントロールが設定されていることを確認します。
   - アプリケーションコントロールルールが実運用で適用されている。Kaspersky Endpoint Security for Windows でモードを確認し、［**アプリケーション設定**］→［**セキュリティコントロール**］→［**アプリケーションコントロール**］の順に移動して、［**テストモード**］が無効になっていることを確認します。

結果

すべての手順を完了すると、管理対象デバイスでのアプリケーションの起動コントロールが実現します。ユーザーは、組織で許可されているアプリケーションのみを実行でき、禁止されているアプリケーションは実行できなくなります。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ

アプリケーションコントロールの概要

アプリケーションコントロールは、アプリケーションを起動しようとするユーザーの試みを監視し、アプリケーションコントロールルールによってアプリケーションの起動を制御します。

アプリケーションコントロール機能は、カスペルスキー製品の Kaspersky Endpoint Security for Windows と Kaspersky Endpoint Security for Linux（バージョン 11.2 以降）で使用できます。このセクションでは、Kaspersky Endpoint Security でのアプリケーションコントロール機能の設定方法について説明します。

パラメータがいずれのアプリケーションコントロールルールとも一致していないアプリケーションの起動は、アプリケーションコントロール機能の動作モードに応じて次のように制御されます：

- *拒否リスト*：ブロックルールで指定しているアプリケーション以外のすべてのアプリケーションの起動を許可するには、このモードを使用します。既定では*拒否リスト*モードが選択されます。
- *許可リスト*。許可ルールで指定しているアプリケーション以外のすべてのアプリケーションの起動をブロックするには、このモードを使用します。

アプリケーションコントロールルールは、アプリケーションカテゴリを通じて実装されます。どのようなアプリケーションをカテゴリに含めるかの基準を指定してアプリケーションカテゴリを作成できます。Kaspersky Security Center Cloud コンソールでは、2 つのアプリケーションカテゴリの種別を使用できます：

- 手動でコンテンツを追加するカテゴリ：ファイルのメタデータ、ハッシュコード、証明書、KL カテゴリ、ファイルパスなど、実行ファイルをカテゴリに含める条件を指定します。
- 選択したデバイスの実行ファイルを含むカテゴリ：デバイスを指定して、デバイス上に存在する実行ファイルを自動的にカテゴリに含めます。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ

クライアントデバイスにインストールされているアプリケーションのリストの取得と表示

Kaspersky Security Center Cloud コンソールは、Linux または Windows を実行している管理対象クライアントデバイスにインストールされているすべてのソフトウェアのインベントリを作成します。

ネットワークエージェントが、デバイスにインストールされているアプリケーションのリストを作成し、管理サーバーに送信します。ネットワークエージェントがアプリケーションリストを更新するには約 10 ～ 15 分かかります。

Windows ベースのクライアントデバイスの場合、ネットワークエージェントは、インストールされているアプリケーションに関する大部分の情報を Windows レジストリから受け取ります。Linux ベースのクライアントデバイスの場合、パッケージマネージャーはインストールされているアプリケーションに関する情報をネットワークエージェントに提供します。

管理対象デバイスにインストールされているアプリケーションのリストを表示するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。

   このページでは、管理対象デバイスにインストールされているアプリケーションが表形式で表示されます。アプリケーションを選択して、製造元名、バージョン番号、実行ファイルのリスト、該当するアプリケーションがインストールされているデバイスのリスト、適用可能なソフトウェアアップデートのリスト、検知されたソフトウェア脆弱性のリストなど、様々なプロパティを表示します。

2. インストールされたアプリケーションの表のデータは、次のようにしてグループ化およびフィルタリングできます：

   - 表の右上隅にある設定アイコン（ ）をクリックします。

     呼び出された［**列の設定**］メニューで、表に表示する列を選択します。アプリケーションがインストールされたクライアントデバイスのオペレーティングシステムの種別を表示するには、［**OS の種別**］列を選択します。

   - 表の右上隅にあるフィルターアイコン（ ）をクリックして、呼び出されたメニューでフィルター条件を指定して適用します。

     インストールされているアプリケーションをフィルタリングした表が表示されます。

特定の管理対象デバイスにインストールされているアプリケーションのリストを表示するには：

メインメニューで、［**デバイス**］→［**管理対象デバイス**］→［**<デバイス名>**］→［**詳細**］→［**アプリケーションレジストリ**］の順に移動します。このメニューで、アプリケーションのリストを CSV ファイルまたは TXT ファイルにエクスポートできます。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ

クライアントデバイスにインストールされている実行ファイルのリストの取得と表示

管理対象デバイス上にインストールされた実行ファイルのリストを取得できます。実行ファイルのインベントリを実行するには、インベントリタスクを作成する必要があります。

実行ファイルのインベントリ機能は、次のアプリケーションで使用できます：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux（バージョン 11.2 以降）

インストールされているアプリケーションに関する情報を取得しながらデータベースの負荷を軽減できます。これを行うには、ソフトウェアの標準セットがインストールされている参照デバイスでインベントリタスクを実行することをお勧めします。

クライアントデバイス上の実行ファイルのインベントリタスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。ウィザードの指示に従ってください。
3. ［**新規タスク**］ページの［**アプリケーション**］ドロップダウンリストで、クライアントデバイスのオペレーティングシステムの種別に応じて、Kaspersky Endpoint Security for Windows または Kaspersky Endpoint Security for Linux を選択します。
4. ［**タスク種別**］ドロップダウンリストから［**インベントリ**］を選択します。
5. ［**タスク作成の終了**］ページで、［**終了**］をクリックします。

   新規タスクウィザードの終了後、指定した設定で［**インベントリ**］タスクが作成されます。必要に応じて、作成したタスクの設定を編集できます。作成したタスクはタスクリストに表示されます。

インベントリタスクの詳細については、次のヘルプを参照してください：

- Kaspersky Endpoint Security for Windows のヘルプ
- Kaspersky Endpoint Security for Linux のヘルプ

［**インベントリ**］タスクの実行が完了すると、管理対象デバイス上にインストールされた実行ファイルのリストが作成され、このリストを表示できるようになります。

インベントリでは、MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR、HTML ファイル形式の実行ファイルが検出されます。

クライアントデバイス上に保管された実行ファイルのリストを表示するには：

メインメニューで、［**操作**］→［**サードパーティ製品**］→［**実行ファイル**］の順に選択します。

クライアントデバイス上にインストールされた実行ファイルのリストが表示されます。

管理対象デバイスからカスペルスキーへ実行ファイルを送信し、潜在的な脅威をチェックすることができます。

管理対象デバイスの実行ファイルをカスペルスキーに送るには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**実行ファイル**］の順に移動します。
2. カスペルスキーに送る実行ファイルのリンクをクリックします。

3. 表示されたウィンドウで、［**デバイス**］セクションに移動し、実行ファイルの送信元の管理対象デバイスのチェックボックスをオンにします。

   実行ファイルを送信する前に、［**管理サーバーから切断しない**］を選択して管理対象デバイスが管理サーバーに直接接続されていることを確認してください。［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

4. ［**カスペルスキーに送信**］をクリックします。

選択した実行ファイルがダウンロードされ、カスペルスキーに送信されます。

コンテンツが手動で追加されるアプリケーションカテゴリの作成

組織内で起動を許可またはブロックする実行ファイルのテンプレートとしての条件を、単独でまたは組み合わせて指定できます。一定の条件に一致する実行ファイルをまとめて管理するために、アプリケーションカテゴリを作成してアプリケーションコントロールの設定で使用できます。

コンテンツが手動で追加されるアプリケーションカテゴリを作成するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションカテゴリ**］の順に移動します。

   アプリケーションカテゴリのリストが表示されます。

2. ［**追加**］をクリックします。

   新規カテゴリウィザードが起動します。ウィザードの指示に従ってください。

3. ウィザードの［**カテゴリの作成方法の選択**］ページで、［**手動でコンテンツを追加するカテゴリ：実行ファイルのデータを手動でカテゴリに追加します**］を選択します。

4. ウィザードの［**条件**］ページで［**追加**］をクリックして、作成中のカテゴリに含めるファイルの条件を追加します。

5. ［**条件の基準**］ページで、カテゴリを作成するルールの種別をリストから選択します：

   - **KL カテゴリから選択**

     このオプションをオンにすると、カスペルスキー製品のカテゴリを、アプリケーションカテゴリにアプリケーションを追加する条件として指定できます。指定したカスペルスキー製品カテゴリのアプリケーションが、アプリケーションカテゴリに追加されます。

   - **リポジトリから証明書を選択**

     このオプションをオンにすると、保管領域の証明書を指定できます。指定された証明書に従って署名された実行ファイルが、アプリケーションカテゴリに追加されます。

   - **アプリケーションのパスを指定（マスクをサポート）**

     このオプションをオンにすると、クライアントデバイス上のフォルダーのパスを指定できます。そのフォルダーに含まれる実行ファイルが、アプリケーションカテゴリに追加されます。

- **リムーバブルドライブ**

  このオプションをオンにすると、アプリケーションを実行するメディアの種別（任意のドライブまたはリムーバブルドライブ）を指定できます。指定した種別のドライブ上で実行されたアプリケーションが、アプリケーションカテゴリに追加されます。

- **ハッシュ、メタデータ、証明書のいずれか**：

  - **実行ファイルリストから選択**

    このオプションをオンにすると、クライアントデバイス上の実行ファイルのリストを使用して、アプリケーションを選択してカテゴリに追加できます。

  - **アプリケーションレジストリから選択**

    このオプションをオンにすると、アプリケーションレジストリが表示されます。アプリケーションをレジストリから選択し、次のようなファイルのメタデータを指定できます：

    - ファイル名。
    - ファイルバージョン。バージョンの正確な数字を指定することも、「次より多い：5.0」のような条件を指定することもできます。
    - アプリケーション名。
    - アプリケーションのバージョン。バージョンの正確な数字を指定することも、「次より多い：5.0」のような条件を指定することもできます。
    - 製造元。

  - **手動で指定**

このオプションをオンにした場合、ファイルのハッシュ、メタデータ、証明書のいずれかを、アプリケーションカテゴリにアプリケーションを追加する条件として指定する必要があります。

ファイルのハッシュ

ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、このカテゴリ内のファイルに、Kaspersky Security Center Cloud コンソールによるハッシュ値計算のアルゴリズムを選択する必要があります。計算されたハッシュ値に関する情報は、管理サーバーのデータベースに保存されます。ハッシュ値の保存でデータベースのサイズが大幅に増えることはありません。

暗号学的ハッシュ関数 SHA-256 はアルゴリズムに脆弱性が発見されておらず、現在最も信頼できる暗号化機能とみなされています。SHA-256 計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降でサポートされています。ハッシュ関数 MD5 の計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のすべてのバージョンでサポートされます。

カテゴリ内のファイルに、Kaspersky Security Center Cloud コンソールによるハッシュ値計算のオプションを選択します：

- ネットワークにインストールされているセキュリティ製品のすべてのインスタンスが Kaspersky Endpoint Security 10 Service Pack 2 for Windows またはそれ以降のバージョンである場合は、［**SHA-256**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンで、実行ファイルの SHA-256 ハッシュ値の基準に従って作成したカテゴリは追加しないでください。セキュリティ製品の動作に不具合が生じることがあります。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 MD5 を使用することができます。

- ネットワークに Kaspersky Endpoint Security 10 Service Pack 2 for Windows より以前のバージョンの製品がインストールされている場合は、［**MD5 ハッシュ**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョン向けの実行ファイルの MD5 チェックサムの基準に従って作成したカテゴリは追加できません。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 SHA-256 を使用できます。

- ネットワークにある別々の端末で Kaspersky Endpoint Security 10 の以前のバージョンと以降のバージョンと両方が使用されている場合は、［**SHA-256**］と［**MD5 ハッシュ**］の両方をオンにしてください。

メタデータ

このオプションをオンにすると、ファイル名、バージョン、製造元などのファイルのメタデータを指定できます。メタデータが管理サーバーに送信されます。同じメタデータを含む実行ファイルがアプリケーションカテゴリに追加されます。

証明書

このオプションをオンにすると、保管領域の証明書を指定できます。指定された証明書に従って署名された実行ファイルが、アプリケーションカテゴリに追加されます。

- **ファイル、MSI パッケージ、アーカイブフォルダーから選択**

このオプションをオンにすると、MSI インストーラーファイルを、アプリケーションカテゴリにアプリケーションを追加する条件として指定できます。アプリケーションのインストーラーのメタデータが管理サーバーに送信されます。インストーラーのメタデータが指定の MSI インストーラーと同じアプリケーションが、アプリケーションカテゴリに追加されます。

選択した基準が、条件のリストに追加されます。

アプリケーションカテゴリの作成基準は、個数の制限なく必要な数だけ追加できます。

6. ウィザードの［**除外**］ページで［**追加**］をクリックして、作成中のカテゴリから除外するファイルの条件を追加します。

7. ［**条件の基準**］ページで、カテゴリ作成用のルールの種別を選択したときと同様に、リストからルールの種別を選択します。

ウィザードを最後まで完了すると、アプリケーションカテゴリが作成されます。新しいルールがアプリケーションカテゴリのリストに表示されます。アプリケーションコントロールを設定時に作成したアプリケーションカテゴリを使用できます。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ

選択したデバイスの実行ファイルを含むアプリケーションカテゴリの作成

選択したデバイス上に存在する実行ファイルを、許可またはブロックする実行ファイルのテンプレートとして使用できます。選択したデバイス上に存在する実行ファイルを基準に、アプリケーションカテゴリを作成してアプリケーションコントロールの設定で使用できます。

選択したデバイスの実行ファイルを含むアプリケーションカテゴリを作成するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションカテゴリ**］の順に選択します。

   アプリケーションカテゴリのリストが表示されます。

2. ［**追加**］をクリックします。

   新規カテゴリウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ウィザードの［**カテゴリの作成方法の選択**］ページで、カテゴリ名を指定して［**選択したデバイスの実行ファイルを含むカテゴリ：デバイスの実行ファイルが自動的に処理され、メトリックがカテゴリに追加されます**］をオンにします。

4. ［**追加**］をクリックします。

5. 表示されるウィンドウで、アプリケーションカテゴリの作成に実行ファイルを使用するデバイスを選択します。

6. 次の設定を指定します：

   - **ハッシュ値計算アルゴリズム**

ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、このカテゴリ内のファイルに、Kaspersky Security Center Cloud コンソールによるハッシュ値計算のアルゴリズムを選択する必要があります。計算されたハッシュ値に関する情報は、管理サーバーのデータベースに保存されます。ハッシュ値の保存でデータベースのサイズが大幅に増えることはありません。

暗号学的ハッシュ関数 SHA-256 はアルゴリズムに脆弱性が発見されておらず、現在最も信頼できる暗号化機能とみなされています。SHA-256 計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降でサポートされています。ハッシュ関数 MD5 の計算は、Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のすべてのバージョンでサポートされます。

カテゴリ内のファイルに、Kaspersky Security Center Cloud コンソールによるハッシュ値計算のオプションを選択します：

- ネットワークにインストールされているセキュリティ製品のすべてのインスタンスが Kaspersky Endpoint Security 10 Service Pack 2 for Windows またはそれ以降のバージョンである場合は、［**SHA-256**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンで、実行ファイルの SHA-256 ハッシュ値の基準に従って作成したカテゴリは追加しないでください。セキュリティ製品の動作に不具合が生じることがあります。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 MD5 を使用することができます。

- ネットワークに Kaspersky Endpoint Security 10 Service Pack 2 for Windows より以前のバージョンの製品がインストールされている場合は、［**MD5 ハッシュ**］をオンにしてください。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョン向けの実行ファイルの MD5 チェックサムの基準に従って作成したカテゴリは追加できません。そのような場合は、対象カテゴリのファイルに対して暗号学的ハッシュ関数 SHA-256 を使用できます。

ネットワークにある別々の端末で Kaspersky Endpoint Security 10 の以前のバージョンと以降のバージョンと両方が使用されている場合は、［**SHA-256**］と［**MD5 ハッシュ**］の両方をオンにしてください。

既定では、［**このカテゴリのファイルの SHA-256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）**］が選択されています。

［**このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）**］は既定ではオフです。

- **データを管理サーバーのリポジトリと同期**

指定したフォルダーでの変更内容を管理サーバーに定期的にチェックさせる場合は、このオプションを使用します。

既定では、このオプションはオフです。

このオプションをオンにする場合、指定したフォルダーでの変更内容をチェックする間隔（時間単位）を指定します。既定の間隔は 24 時間です。

- **ファイル種別**

このセクションでは、アプリケーションカテゴリを作成するのに使用するファイルの種別を指定できます。

すべてのファイル：カテゴリの作成時にすべてのファイルが使用されます。既定では、このオプションがオンです。

アプリケーションカテゴリ以外のファイルのみ：カテゴリの作成時に、アプリケーションカテゴリ以外のファイルのみが使用されます。

- **フォルダー**

このセクションでは、選択したデバイス上で、アプリケーションカテゴリを作成するのに使用するファイルが含まれているフォルダーを指定できます。

すべてのフォルダー：カテゴリの作成時にすべてのフォルダーのファイルが使用されます。既定では、このオプションがオンです。

指定フォルダー：カテゴリの作成時に指定したフォルダーのファイルのみが使用されます。このオプションをオンにする場合、フォルダーのパスを指定する必要があります。

ウィザードを最後まで完了すると、アプリケーションカテゴリが作成されます。新しいルールがアプリケーションカテゴリのリストに表示されます。アプリケーションコントロールを設定時に作成したアプリケーションカテゴリを使用できます。

アプリケーションカテゴリのリストの表示

設定済みのアプリケーションカテゴリのリストと各アプリケーションカテゴリの設定を表示できます。

アプリケーションカテゴリのリストを表示するには：

メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションカテゴリ**］の順に選択します。

アプリケーションカテゴリのリストが表示されます。

アプリケーションカテゴリのプロパティを表示するには、

アプリケーションカテゴリの名前をクリックします。

アプリケーションカテゴリのプロパティウィンドウが表示されます。プロパティはいくつかのタブにグループ化されています。

Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロール機能の設定

アプリケーションカテゴリの作成が完了すると、Kaspersky Endpoint Security for Windows ポリシーでのアプリケーションコントロールの設定時にこれらのカテゴリを使用できます。

Kaspersky Endpoint Security for Windows ポリシーでアプリケーションコントロール機能を設定するには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
   ポリシーのリストが表示されます。
2. **Kaspersky Endpoint Security for Windows** のポリシーをクリックします。
   ポリシーの設定ウィンドウが表示されます。

3. ［**アプリケーション設定**］→［**セキュリティコントロール**］→［**アプリケーションコントロール**］の順に移動します。

   ［**アプリケーションコントロール**］ウィンドウでアプリケーションコントロール設定が表示されます。

4. ［**アプリケーションコントロール**］は既定でオンになっています。［**アプリケーションコントロールは無効です**］スイッチを切り替えて、オプションをオフにします。

5. ［**Application Control Settings**］設定で、動作モードを有効にしてアプリケーションコントロールルールを適用し、Kaspersky Endpoint Security for Windows がアプリケーションの起動をブロックできるようにします。

   アプリケーションコントロールルールをテストする場合は、［**Application Control Settings**］セクションでテストモードを有効にします。テストモードでは、Kaspersky Endpoint Security for Windows はアプリケーションの起動をブロックしませんが、適用されたルールに関する情報をレポートに記録します。［**レポートの表示**］をクリックすると、この情報を表示できます。

6. Kaspersky Endpoint Security for Windows で、ユーザーがアプリケーションを起動したときの DLL モジュールの読み込みを監視する場合は、［**DLL モジュールの読み込みを管理**］をオンにします。

   モジュールに関する情報とモジュールを読み込んだアプリケーションに関する情報がレポートに保存されます。

   Kaspersky Endpoint Security for Windows は、［**DLL モジュールの読み込みを管理**］がオンになった後に読み込まれた DLL モジュールとドライバーのみを監視します。Kaspersky Endpoint Security for Windows の起動前に読み込まれていた DLL モジュールとドライバーも含めてすべての DLL モジュールとドライバーを監視する場合、［**DLL モジュールの読み込みを管理**］をオンにした後にコンピューターを再起動してください。

7. （省略可能な手順）［**メッセージのテンプレート**］セクションで、アプリケーションの起動がブロックされたときに表示されるメッセージのテンプレートとお手元に送信されるメッセージのテンプレートを編集できます。

8. ［**アプリケーションコントロールモード**］設定で、［**拒否リスト**］モードまたは［**許可リスト**］モードを選択します。

   既定では、［**拒否リスト**］モードが選択されています。

9. ［**ルールリストの設定**］をクリックします。

   ［**拒否リストと許可リスト**］ウィンドウで、アプリケーションカテゴリを追加できます。既定では、［**拒否リスト**］モードをオンにするとは［**拒否リスト**］タブが選択され、［**許可リスト**］モードをオンにするとは［**許可リスト**］タブが選択されます。

10. ［**拒否リストと許可リスト**］ウィンドウで［**追加**］をクリックします。

    ［**アプリケーションコントロールルール**］ウィンドウが表示されます。

11. ［**カテゴリを選択してください**］をクリックします。

    ［**アプリケーションカテゴリ**］ウィンドウが開きます。

12. 作成済みのアプリケーションカテゴリを追加します。

    ［**編集**］をクリックすると、作成済みのカテゴリの設定を編集できます。

    新しいカテゴリを作成するには、［**追加**］をクリックします。

    リストからカテゴリを削除するには、［**削除**］をクリックします。

13. アプリケーションカテゴリのリストの編集が完了したら、［**OK**］をクリックします。

    ［**アプリケーションカテゴリ**］ウィンドウが閉じます。

14. ［**アプリケーションコントロール**ルール］ウィンドウの［**オブジェクトとその権限**］セクションで、アプリケーションコントロールルールを適用するユーザーとユーザーのグループのリストを作成します。

15. ［**OK**］をクリックして、設定を保存し［**アプリケーションコントロールルール**］ウィンドウを閉じます。

16. ［**OK**］をクリックして、設定を保存し［**拒否リストと許可リスト**］ウィンドウを閉じます。

17. ［**OK**］をクリックし、設定を保存して［**アプリケーションコントロール**］ウィンドウを閉じます。

18. Kaspersky Endpoint Security for Windows ポリシー設定のウィンドウを閉じます。

アプリケーションコントロールの設定が適用されます。ポリシーのクライアントデバイスへの適用が完了すると、実行ファイルの起動が管理されるようになります。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ

イベントに関連する実行ファイルのアプリケーションカテゴリへの追加

Kaspersky Endpoint Security for Windows のポリシーでアプリケーションコントロールの設定を完了させると、イベントのリストに次のイベントが表示されます：

- **アプリケーションの起動が禁止されました**（*緊急*イベント）：このイベントは、アプリケーションコントロールの設定で、実際にルールを適用するように指定した場合に表示されます。
- **アプリケーションの起動がテストモードでブロックされています**（*情報*イベント）：このイベントは、アプリケーションコントロールの設定で、ルールをテストするように指定した場合に表示されます。
- **アプリケーションの起動禁止に関する管理者へのメッセージ**（*警告*イベント）。このイベントは、アプリケーションコントロールの設定で実際にルールを適用するように指定しており、起動時にブロックされたアプリケーションへのアクセスをユーザーが要求した場合に表示されます。

アプリケーションコントロールの動作に関するイベントを表示するために、イベントの抽出を作成しておくことを推奨します。

アプリケーションコントロールイベントの対象となった実行ファイルを、既存のアプリケーションカテゴリや新規に作成するアプリケーションカテゴリに追加できます。実行ファイルは、手動でコンテンツを追加するタイプのアプリケーションカテゴリにのみ追加できます。

アプリケーションコントロールイベントの対象となった実行ファイルをアプリケーションカテゴリに追加するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
   イベントの抽出のリストが表示されます。

2. アプリケーションコントロールに関するイベントを表示するためのイベントの抽出を選択し、イベントの抽出を実行します。
   アプリケーションコントロールに関するイベントを表示するためのイベントの抽出をまだ作成していない場合は、代わりに「**最近のイベント**」などの事前定義済みのイベントの抽出を選択して実行することもできます。

イベントのリストが表示されます。

3. 対象となった実行ファイルをアプリケーションカテゴリに追加するイベントを選択し、［**カテゴリへ割り当て**］をクリックします。

   新規カテゴリウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

4. ウィザードのウィンドウで、関連する設定を指定します：

   - ［**イベントに関係する実行ファイルへの処理**］セクションで、次のいずれかのオプションをオンにします：

     - **新規アプリケーションカテゴリへ追加**

       イベントに関連する実行ファイルを元に新しいアプリケーションカテゴリを作成する場合は、このオプションをオンにします。

       既定では、このオプションがオンです。

       このオプションを選択する場合は、新しいカテゴリ名を指定してください。

     - **アプリケーションカテゴリへ追加**

       イベントに関連する実行ファイルを既存のアプリケーションカテゴリに追加する場合は、このオプションをオンにします。

       既定では、このオプションはオフです。

       このオプションを選択する場合は、実行ファイルの追加先として、手動でコンテンツを追加するタイプのアプリケーションカテゴリを選択してください。

   - ［**ルールの種別**］セクションで、次のいずれかを選択します：

     - **除外しない場合のルール**
     - **除外に追加する場合のルール**

   - ［**条件として使用する情報**］セクションで、次のいずれかのオプションをオンにします：

     - **証明書の詳細情報（証明書がないファイルの場合 SHA-256 ハッシュ）**

       ファイルが証明書によって署名されていることがあります。複数のファイルが同じ証明書で署名されていることがあります。たとえば、同じアプリケーションの異なるバージョンが同じ証明書で署名されていたり、同じ開発元の様々なアプリケーションが同じ証明書で署名されていたりすることがあります。証明書を選択した場合、アプリケーションの複数のバージョンまたは同じ開発元の複数のアプリケーションが同じカテゴリに属す場合があります。

       それぞれのファイルには固有の SHA-256 ハッシュ関数があります。SHA-256 ハッシュ関数を選択した場合、1つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

       実行ファイルの証明書の詳細（または証明書がないファイルの SHA-256 ハッシュ機能）をカテゴリルールに追加する場合は、このオプションを選択します。

       既定では、このオプションがオンです。

     - **証明書の詳細情報（証明書のないファイルはスキップ）**

ファイルが証明書によって署名されていることがあります。複数のファイルが同じ証明書で署名されていることがあります。たとえば、同じアプリケーションの異なるバージョンが同じ証明書で署名されていたり、同じ開発元の様々なアプリケーションが同じ証明書で署名されていたりすることがあります。証明書を選択した場合、アプリケーションの複数のバージョンまたは同じ開発元の複数のアプリケーションが同じカテゴリに属す場合があります。

実行ファイルの証明書の詳細をカテゴリルールに追加する場合は、このオプションを選択します。実行ファイルに証明書がない場合、そのファイルはスキップされます。このファイルに関する情報は、カテゴリに追加されません。

- **SHA-256 のみ（ハッシュのないファイルはスキップ）**

  それぞれのファイルには固有の SHA-256 ハッシュ関数があります。SHA-256 ハッシュ関数を選択した場合、1つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

  実行ファイルの SHA-256 ハッシュ機能の詳細だけを追加する場合、このオプションを選択します。

- **MD5 のみ（非推奨、Kaspersky Endpoint Security 10 Service Pack 1 の場合のみ）**

  それぞれのファイルには固有の MD5 ハッシュ関数があります。MD5 ハッシュ関数を選択した場合、1つのファイル（たとえばアプリケーションの特定のバージョン）のみがカテゴリに属します。

  実行ファイルの MD5 ハッシュ機能の詳細だけを追加する場合、このオプションを選択します。Kaspersky Endpoint Security 10 Service Pack 1 for Windows およびそれ以前のすべてのバージョンで、MD5 ハッシュ機能の計算がサポートされています。

5. ［**OK**］をクリックします。

ウィザードが完了すると、アプリケーションコントロールのイベントに関連付けられていた実行ファイルが、既存のアプリケーションカテゴリまたは新規に作成したアプリケーションカテゴリに追加されます。変更または新規に作成したアプリケーションカテゴリの設定を表示できます。

Application Control の詳細については、次のヘルプトピックを参照してください：

- Kaspersky Endpoint Security for Windows のオンラインヘルプ
- Kaspersky Endpoint Security for Linux のオンラインヘルプ

定義データベースからのサードパーティ製品のインストールパッケージの作成

Kaspersky Security Center Web コンソールでは、インストールパッケージを使用してサードパーティ製品のリモートインストールを実行できます。このようなサードパーティ製品は、専用の定義データベースに格納されています。

定義データベースから作成されたサードパーティ製品のインストールパッケージを作成することは、脆弱性とパッチ管理ライセンスの下でのみ行うことができます。

定義データベースからサードパーティ製品のインストールパッケージを作成するには：

1. メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動します。
2. ［**追加**］をクリックします。
3. 開いた新規パッケージウィザードページで、［**カスペルスキーのデータベースからアプリケーションを選択してインストールパッケージを作成する**］をオンにして、［**次へ**］をクリックします。
4. 開いたアプリケーションのリストで、関連するアプリケーションを選択し、［**次へ**］をクリックします。
5. ドロップダウンリストから関連するローカリゼーション言語を選択し、［**次へ**］をクリックします。

   このステップは、アプリケーションに複数の言語オプションが用意されている場合にのみ表示されます。

6. インストールについて使用許諾契約書に同意するよう求められたら、開いた［**使用許諾契約書**］ページで、リンクをクリックして製造元の Web サイトで使用許諾契約書を読み、［**この使用許諾契約書の内容をすべて確認し、理解した上で条項に同意する**］をオンにします。
7. 開いた［**新規インストールパッケージの名前**］ページの［**パッケージ名**］にインストールパッケージの名前を入力し、［**次へ**］をクリックします。

新しく作成されたインストールパッケージが管理サーバーにアップロードされるまで待ちます。パッケージの作成プロセスが成功したことを通知するメッセージが新規パッケージウィザードに表示されたら、［**終了**］をクリックします。

新しく作成されたインストールパッケージがインストールパッケージのリストに表示されます。このパッケージは、*アプリケーションのリモートインストール*タスクを作成または再設定する際に選択できます。

定義データベースからのサードパーティ製品のインストールパッケージの設定に関する表示と変更

以前に定義データベースに一覧表示されているサードパーティ製品のインストールパッケージを作成している場合は、後でこれらのパッケージの設定を表示および変更できます。

定義データベースから作成されたサードパーティ製品のインストールパッケージの設定を変更することは、脆弱性とパッチ管理ライセンスの下でのみ行うことができます。

定義データベースからサードパーティ製品のインストールパッケージの設定を表示および変更するには：

1. メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**インストールパッケージ**］の順に移動します。
2. 表示されたインストールパッケージのリストで、関連するパッケージの名前をクリックします。
3. 開いたプロパティページで、必要に応じて設定を変更します。
4. ［**保存**］をクリックします。

変更した設定が保存されます。

定義データベースからのサードパーティ製品のインストールパッケージの設定

サードパーティ製品のインストールパッケージの設定は、次のタブにグループ化されています：

既定で表示されるのは以下の一覧に表示されている設定の一部のみであるため、［**フィルター**］をクリックしてリストから関連する列名を選択することで、対応する列を追加できます。

- ［**全般**］タブ：
  - 手動で編集できるインストールパッケージの名前を含む入力フィールド
  - **アプリケーション**

    インストールパッケージが作成されるサードパーティ製品の名前。
  - **バージョン**

    インストールパッケージが作成されるサードパーティ製品のバージョン番号。
  - **サイズ**

    サードパーティのインストールパッケージのサイズ（キロバイト単位）。
  - **作成日時**

    サードパーティのインストールパッケージが作成された日時。
  - **パス**

    サードパーティのインストールパッケージが保存されているネットワークフォルダーのパス。
- ［**インストール手続き**］タブ：
  - **必要なシステムコンポーネントをインストールする**

    このオプションをオンにすると、アップデートのインストール前にインストールが必要な一般システムコンポーネントをすべて自動的にインストールします。インストールが必要な対象としては、オペレーティングシステムのアップデートなどが考えられます。

    このオプションをオフにすると、必須コンポーネントを手動でインストールすることが必要となる場合があります。

    既定では、このオプションはオフです。
  - アップデートのプロパティを表示し、次の列を含む表：

- **名前**

  アップデートの名前。

- **説明**

  アップデートの説明。

- **ソース**

  アップデート元、つまり、Microsoft または別のサードパーティ開発元のいずれによってリリースされたものであるか。

- **種別**

  アップデートの種別、つまり、対象とするのがドライバーまたはアプリケーションのいずれであるか。

- **カテゴリ**

  Microsoft のアップデート（緊急更新プログラム、定義更新プログラム、ドライバー、機能パック、セキュリティ更新プログラム、サービスパック、ツール、更新プログラムロールアップ、更新プログラム、またはアップグレード）に対して表示される Windows Server Update Services（WSUS）カテゴリ。

- **MSRC による重要度**

  Microsoft Security Response Center（MSRC）によって定義されたアップデートの重要度。

- **重要度**

  カスペルスキーによって定義されたアップデートの重要度。

- **パッチ重要度レベル**

  カスペルスキー製品を対象とする場合のパッチの重要度。

- **記事**

  アップデートについて説明するナレッジベースの記事の識別子（ID）。

- **セキュリティ情報**

  アップデートについて説明するセキュリティ情報の ID。

- **新しいバージョンのインストール未割り当て**

  アップデートのステータスが「インストール用に未割り当て」であるかどうかを表示します。

- **インストール予定**

  アップデートのステータスが「インストール予定」であるかどうかを表示します。

- **インストール中**

  アップデートのステータスが「インストール中」であるかどうかを表示します。

- **インストール済み**

  アップデートのステータスが「インストール済み」であるかどうかを表示します。

- **失敗**

  アップデートのステータスが「失敗」であるかどうかを表示します。

- **再起動が必要です**

  アップデートのステータスが「再起動が必要」であるかどうかを表示します。

- **登録日**

  アップデートが登録された日時を表示します。

- **対話モードでのインストール**

  アップデートのインストール中にユーザーとの対話が必要であるかどうかを表示します。

- **取り消し**

  アップデートが取り消された日時を表示します。

- **アップデート承認の状況**

  アップデートのインストールが承認済みであるかどうかを表示します。

- **リビジョン**

  アップデートの現在のリビジョン番号を表示します。

- **アップデート ID**

  アップデートの ID を表示します。

- **アプリケーションのバージョン**

  アプリケーションのアップデート後のバージョン番号を表示します。

- **より古い**

該当するアップデートを置換できる他のアップデートを表示します。

- **より新しい**

  このアップデートで置換できる他のアップデートを表示します。

- **使用許諾契約書の条項に同意する必要があります**

  アップデート時に使用許諾契約書（EULA）への同意が必要であるかどうかを表示します。

- **詳細 URL**

  アップデートの製造元の名前を表示します。

- **アプリケーションファミリー**

  アップデートが属するアプリケーションファミリーの名前を表示します。

- **アプリケーション**

  アップデートが属するアプリケーションの名前を表示します。

- **ローカリゼーション言語**

  アップデートの言語を表示します。

- **新しいバージョンのインストール未割り当て**

  アップデートのステータスが「新しいバージョンのインストール用に未割り当て」であるかどうかを表示します。

- **必須アップデートのインストールが必要**

  アップデートのステータスが「必須コンポーネントのインストールが必要」であるかどうかを表示します。

- **ダウンロード方法**

  アップデートのダウンロード方法を表示します。

- **パッチ**

  アップデートがパッチであるかどうかを表示します。

- **未インストール**

  アップデートのステータスが「未インストール」であるかどうかを表示します。

- ［**設定**］タブには、インストール中にコマンドラインパラメータとして使用される、インストールパッケージの設定とその名前、説明、および値が表示されます。パッケージにそのような設定が用意されていない場合は、対応するメッセージが表示されます。これらの設定の値を変更できます。

- ［**変更履歴**］タブにはインストールパッケージのリビジョンが表示され、次の列が含まれます：

  - **リビジョン**

    インストールパッケージのリビジョン番号を表示します。

  - **時間**

    リビジョンが作成された時刻を表示します。

  - **ユーザー**

    リビジョンが作成されたユーザーアカウントの名前を表示します。

  - **処理**

    リビジョン内のインストールパッケージで実行された処理を一覧表示します。

  - **説明**

    リビジョンに追加されたテキストの説明を表示します。

アプリケーションタグ

このセクションでは、サードパーティ製品を対象としたアプリケーションタグの概要と、アプリケーションタグの作成、編集、製品への割り当てを行う方法を説明しています。

アプリケーションタグの概要

Kaspersky Security Center Cloud コンソールでは、サードパーティ製品（カスペルスキー以外の製造元が作成した製品）にタグを付与することができます。タグとは、アプリケーションに割り当てるラベルで、アプリケーションのグループ化と検索に使用できます。アプリケーションに割り当てたタグは、デバイスの抽出の条件として使用できます。

たとえば、「ブラウザー」というタグを作成し、すべてのブラウザー（Microsoft Internet Explorer、Google Chrome、Mozilla Firefox など）に割り当てるなどの使い方ができます。

アプリケーションタグの作成

アプリケーションタグを作成するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションタグ**］の順に選択します。
2. ［**追加**］をクリックします。
   新規タグの入力ウィンドウが表示されます。
3. タグの名前を入力します。
4. ［**OK**］をクリックして変更内容を保存します。

アプリケーションタグのリストに新しいタグが表示されます。

アプリケーションタグの名前変更

アプリケーションタグの名前を変更するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションタグ**］の順に選択します。
2. 名前を変更するタグの横のチェックボックスをオンにし、［**編集**］をクリックします。
   タグのプロパティウィンドウが表示されます。
3. タグの名前を変更します。
4. ［**OK**］をクリックして変更内容を保存します。

アプリケーションタグのリストに更新したタグが表示されます。

アプリケーションへのタグの割り当て

アプリケーションにタグを割り当てるには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。
2. タグを割り当てるアプリケーションの名前をクリックします。
3. ［**タグ**］タブを選択します。
   タブには管理サーバー上のすべてのアプリケーションタグが表示されます。選択したアプリケーションに割り当てられているタグでは、［**タグの割り当て**］列のチェックボックスがオンになっています。
4. 新たに割り当てるタグの［**タグの割り当て**］列のチェックボックスをオンにします。
5. ［**保存**］をクリックして変更内容を保存します。

アプリケーションにタグが割り当てられます。

アプリケーションに割り当てたタグの削除

アプリケーションからタグを削除するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションレジストリ**］の順に選択します。
2. タグを削除するアプリケーションの名前をクリックします。
3. ［**タグ**］タブを選択します。

   タブには管理サーバー上のすべてのアプリケーションタグが表示されます。選択したアプリケーションに割り当てられているタグでは、［**タグの割り当て**］列のチェックボックスがオンになっています。
4. 削除するタグの［**タグの割り当て**］列のチェックボックスをオフにします。
5. ［**保存**］をクリックして変更内容を保存します。

アプリケーションからタグが解除されます。

解除されたアプリケーションタグ自身は削除されません。必要に応じて、手動で削除できます。

アプリケーションタグの削除

アプリケーションタグを削除するには：

1. メインメニューで、［**操作**］→［**サードパーティ製品**］→［**アプリケーションタグ**］の順に選択します。
2. リストから削除するアプリケーションタグを選択します。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**OK**］をクリックします。

アプリケーションタグが削除されます。削除されたタグが割り当てられていたすべてのアプリケーションから、このタグが自動的に削除されます。

管理サーバーの設定

このセクションでは、Kaspersky Security Center 管理サーバーの設定手順とプロパティについて説明しています。

管理サーバーの階層の作成：セカンダリ管理サーバーの追加

オンプレミスで実行されている管理サーバーを、セカンダリ管理サーバーとして機能するように設定し、ネットワークに「プライマリ」と「セカンダリ」の階層を構築できます。カスペルスキーのインフラストラクチャに含まれる管理サーバーの場合、ネットワーク上のプライマリ管理サーバーとセカンダリ管理サーバーはどちらもセカンダリサーバーです。Windows ベースまたは Linux ベースの管理サーバーを追加できます。

接続可能なセカンダリ管理サーバーを追加するには：

1. 追加するセカンダリ管理サーバーに Kaspersky Security Center Web コンソールがインストールされていることを確認します。

2. 追加するセカンダリ管理サーバーで管理サーバー証明書をダウンロードして保存し、セカンダリ管理サーバー追加ウィザードウィザードのステップでプライマリ管理サーバーに追加できるようにします。

3. 追加するセカンダリ管理サーバーで、Kaspersky Security Center Web コンソールから次の操作を実行します（または、追加するセカンダリ管理サーバーの管理者にこれらの操作を実行するよう依頼できます）：

   a. メインメニューで、目的のセカンダリ管理サーバーの名前の横にある設定アイコン（）をクリックします。

   b. 表示されるプロパティページで、［**全般**］タブの［**管理サーバーの階層**］セクションに移動します。

   c. ［**この管理サーバーをセカンダリ管理サーバーとして使用する**］をオンにします。

   d. プライマリ管理サーバーの種別として［**Cloud Console**］を選択します。

   セカンダリ管理サーバーとプライマリ管理サーバー間で接続を確立するための設定のフィールドが使用可能になります。

   e. ［**HDS サーバーアドレス（Cloud コンソールのプライマリ管理サーバー）**］と［**HDS サーバーポート**］に、Kaspersky Security Center Cloud コンソールのプライマリ管理サーバーのアドレスとポートを入力します。

   HDS サーバーアドレスと HDS サーバーポートは、Kaspersky Security Center Cloud コンソール管理サーバーのプロパティウィンドウの、［**全般**］タブの［**管理サーバーの階層**］セクションで確認できます。このデータをコピーして、セカンダリ管理サーバーのウィンドウのフィールドに貼り付けることができます。

   f. ［**プライマリ管理サーバーの証明書を指定する**］をクリックして、証明書を選択します。

   この証明書は、Kaspersky Security Center Cloud コンソール管理サーバーのプロパティウィンドウの、［**全般**］タブの［**管理サーバーの階層**］セクションで、［**管理サーバー証明書の表示**］をクリックしてダウンロードできます。

   g. ［**Hosted Discovery Service の証明書を指定する**］をクリックして、証明書を選択します。

   この証明書は、Kaspersky Security Center Cloud コンソール管理サーバーのプロパティウィンドウの、［**全般**］タブの［**管理サーバーの階層**］セクションで、［**HDS ルート認証局証明書**］をクリックしてダウンロードできます。

h. プロキシサーバーを使用して Kaspersky Security Center Cloud コンソール管理サーバー（構築した階層のプライマリサーバー）に接続している場合は、これを指定してプロキシサーバーの資格情報を入力します。

i. セカンダリ管理サーバーが非武装地帯（DMZ）にある場合は、［**プライマリ管理サーバーを DMZ 内のセカンダリ管理サーバーに接続する**］をオンにします。

j. ［**保存**］をクリックして変更を保存し、ウィンドウを閉じます。

4. メインメニューで、目的のプライマリ管理サーバーの名前の横にある設定アイコン（  ）をクリックします。

5. 表示されたプロパティページで、［**管理サーバー**］タブをクリックします。

6. セカンダリ管理サーバーを追加する管理グループの名前の横にあるチェックボックスをオンにします。

7. メニューヘッダーから［**セカンダリ管理サーバーの接続**］を選択します。
セカンダリ管理サーバー追加ウィザードが起動します。

8. ウィザードの最初のページで、次のフィールドに値を入力します：

- **セカンダリ管理サーバーの表示名**

  階層で表示する、セカンダリ管理サーバーの名前。必要に応じて、IP アドレスを名前として入力するか、「グループ 1 のセカンダリサーバー」などの名前を使用できます。

- **セカンダリ管理サーバーアドレス（任意）**

  セカンダリ管理サーバーの IP アドレスまたはドメイン名を指定します。

9. プロキシサーバーを使用して Kaspersky Security Center Cloud コンソール管理サーバー（プライマリサーバーとして指定するサーバー）に接続している場合は、これを指定してプロキシサーバーの資格情報を入力します。

10. ウィザードの以降の指示に従います。

ウィザードが完了すると、プライマリとセカンダリの階層が構築されます。ポート 13000 経由で、セカンダリ管理サーバーからプライマリ管理サーバーへの接続が開始されます。プライマリ管理サーバーからのタスクとポリシーが受信および適用されます。プライマリ管理サーバー上の追加先の管理グループにセカンダリ管理サーバーが表示されます。

管理グループの作成

最初は、管理グループの階層には**管理対象デバイス**グループと呼ばれる管理グループが 1 つだけ含まれています。**管理対象デバイス**グループにはデバイスやサブグループを追加できます。

管理グループを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。

2. 階層で、新しい管理グループを含める管理グループを選択します。

3. ［**追加**］をクリックします。

4. 表示されたウィンドウで、グループの名前を入力し、［**追加**］をクリックします。

   指定した名前の新しい管理グループが管理グループの階層に表示されます。

Active Directory またはドメインネットワークの構成に基づいて管理グループの階層を作成することが可能です。テキストファイルからグループの構成を作成することも可能です。

管理グループの構造を作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。

2. ［**インポート**］をクリックします。

   新規管理グループ構造作成ウィザードが開始します。ウィザードの指示に従ってください。

削除されたデバイスに関するイベントの保存期間の設定

Kaspersky Security Center Cloud コンソールでは、イベントのリポジトリにイベントが保存されます。イベントのリポジトリに保存するイベントの数は設定できません。

管理サーバーのプロパティウィンドウの［**イベントリポジトリ**］セクションで、削除されたデバイスに関するイベントの保存期間を設定できます。最長の保存期間は 1000 日です。

削除されたデバイスに関するイベントの保存日数を設定するには：

1. メインメニューで、Kaspersky Security Center Cloud コンソール管理サーバーの横にある設定アイコン（ ）をクリックします。

   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**イベントリポジトリ**］セクションを選択します。

3. ［**デバイスの削除後にイベントを保管する**］をオンにします。

4. ［**保存期間（日）**］編集ボックスで、削除されたデバイスに関するイベントの保存日数を指定します。

   指定した値によって、削除されたデバイスに関するイベントの保存日数が制限されます。

さらに、任意のタスクの設定を変更して、タスクの進行状況に関連するイベントを保存したり、タスクの実行結果のみを保存したりできます。それにより、データベース内のイベントの数を削減することで、データベース内のイベントの分析を伴う操作の実行速度を向上し、多数のイベントによって重要なイベントが上書きされる可能性を低下させることができます。

イベントに関するメールの集計

運用中、Kaspersky Security Center Cloud コンソールと管理対象のカスペルスキー製品はイベントを生成します。イベントにはそれぞれ種別と重要度（*緊急*、*機能エラー*、*警告*、*情報*）という属性があります。イベントが発生した条件に応じて、Kaspersky Security Center Cloud コンソールは同じ種別のイベントに異なる重要度を割り当てることができます。

Kaspersky Security Center Cloud コンソールは、イベントに関する通知をメールで自動的に送信します。Kaspersky Security Center Cloud コンソールが送信するのは、［**管理サーバーのプロパティ**］ウィンドウの［**イベントの設定**］タブのリストに表示されているイベントに関する通知です。すべてのイベント種別に対して共通の通知設定が使用されます。

送信する必要があるメールの数を制限するため、Kaspersky Security Center Cloud コンソールは、特定の期間に同じ重要度のイベントを集計します。期間の値はカスペルスキーの担当者が管理します。その結果、受信者は「<数字> 個の<重要度>（およびそれ以下のレベル）のイベントが発生しました」というテンプレートで集計されたメールメッセージを受信します。

オンプレミスで実行されているセカンダリ管理サーバーを Kaspersky Security Center Cloud コンソールで管理する場合の制限事項

Kaspersky Security Center Cloud コンソールの対応するオプションを使用して、オンプレミスで実行されているセカンダリ管理サーバーに切り替えると、セカンダリ管理サーバーの管理における特定の制限が製品によって適用されます。ユーザーは、Kaspersky Security Center Cloud コンソールの操作に関連する次の設定を使用できなくなります：

- ネットワークエージェントと管理サーバーのポリシーの設定で、［**イベントの設定**］と［**アプリケーション設定**］タブを使用できなくなります。新しいポリシーは作成できません。
- ネットワークエージェントと管理サーバーのタスクの設定で、［**イベントの設定**］と［**アプリケーション設定**］タブを使用できなくなります。新しいタスクは作成できません。
- ネットワークエージェントと管理サーバーの管理、およびセカンダリ管理サーバーのプロパティウィンドウを使用できなくなります。
- クイックスタートウィザードを使用できなくなります。
- ネットワークエージェントと管理サーバーのイベントに関するストレージと通知の設定を変更できなくなります。
- ［**現在入手可能な製品バージョン**］を使用できなくなります。
- ［**インストールパッケージ**］セクションを使用できなくなります。

セカンダリ管理サーバーのリストの表示

セカンダリ管理サーバー（仮想管理サーバーを含む）のリストを表示するには：

メインメニューで、設定アイコン（）の横にある管理サーバーの名前をクリックします。

セカンダリ管理サーバー（仮想管理サーバーを含む）のドロップダウンリストが表示されます。

表示されている管理サーバーの名前をクリックすると、そのサーバーに移動できます。

管理サーバーの階層の削除

管理サーバーの階層構造が不要になった場合は、管理サーバーを階層構造から離脱させることができます。

管理サーバーの階層を削除するには：

1. メインメニューで、プライマリ管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
2. 表示されたページで、［**管理サーバー**］タブに移動します。
3. セカンダリ管理サーバーを削除する管理グループで、目的のセカンダリ管理サーバーを選択します。
4. メニューヘッダーから［**削除**］を選択します。
5. 表示されるウィンドウで、［**OK**］をクリックし、セカンダリ管理サーバーを削除する処理を確定させます。

プライマリ管理サーバーとして動作していた管理サーバーと、セカンダリ理サーバーとして動作していた管理サーバーは、互いに独立して動作するようになります。これにより、階層構造が解消されます。

インターフェイスの設定

Kaspersky Security Center Cloud コンソールのインターフェイスを設定して、使用している機能に応じてセクションとインターフェイス要素を表示または非表示にすることができます。

現在使用している機能に基づいて Kaspersky Security Center Cloud コンソールのインターフェイスを設定するには：

1. メインメニューで、アカウント設定に移動して、［**インターフェイスのオプション**］を選択します。
2. 表示される［**インターフェイスのオプション**］ウィンドウで、次のオプションをオンまたはオフにします：

   - **データ暗号化と保護機能の表示**

     このオプションを使用して、インターフェイスで［**操作**］→［**データ暗号化と保護機能**］セクションを表示または非表示にできます。Kaspersky Security Center Cloud コンソールは、現在のユーザーアカウント用にのみ、このオプションの値を保存します。他のユーザーは異なる値を設定できます。

   - **MDR 機能を表示**

     このオプションを使用して、インターフェイスで［**監視とレポート**］→［**インシデント**］セクションを表示または非表示にできます。Kaspersky Security Center Cloud コンソールは、現在のユーザーアカウント用にのみ、このオプションの値を保存します。他のユーザーは異なる値を設定できます。

3. Kaspersky Security Center Cloud コンソールの［ポリシーの導入結果］で表示するデバイスの数を設定します。

4. ［**保存**］をクリックします。

コンソールのインターフェイス設定は、ユーザーの好みに応じて設定できます。

仮想管理サーバーの管理

このセクションでは、仮想管理サーバーを管理する次の操作について説明します：

- 仮想管理サーバーの作成
- 仮想管理サーバーの有効化および無効化
- 仮想管理サーバーの管理者を割り当てる
- クライアントデバイスの管理サーバーの変更
- 仮想管理サーバーの削除

仮想管理サーバーの作成

仮想管理サーバーを作成して、管理グループに追加できます。

仮想管理サーバーを作成して追加するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
2. 表示されるウィンドウで、［**管理サーバー**］タブに移動します。
3. 仮想管理サーバーを追加する管理グループを選択します。
4. メニューのリストから［**新しい仮想管理サーバー**］を選択します。
5. 表示されるウィンドウで、［**仮想管理サーバー名**］を指定します。
6. ［**保存**］をクリックします。

新しい仮想管理サーバーが作成され、［**管理サーバー**］タブで表示されていた管理グループに追加されます。

仮想管理サーバーの有効化および無効化

新しい仮想管理サーバーを作成すると、既定で有効になります。いつでも無効にしたり、再び有効にできます。仮想管理サーバーの無効化または有効化は、物理管理サーバーをオフまたはオンに切り替えることと同じです。

仮想管理サーバーを有効または無効にするには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
2. 表示されるウィンドウで、［**管理サーバー**］タブに移動します。

3. 有効または無効にする仮想管理サーバーを選択します。

4. メニューヘッダーで［**仮想管理サーバーの有効化または無効化**］を選択します。

以前の状態に応じて、仮想管理サーバーの状態が有効または無効に変更されます。管理サーバー名の横にアップデートされた状態が表示されます。

仮想管理サーバーへの管理者の割り当て

組織内で仮想管理サーバーを使用する場合、仮想管理サーバーごとに専任の管理者を割り当てることができます。たとえば、仮想管理サーバーを作成して組織の個別のオフィスや部門を管理する場合や、MSP プロバイダーで仮想管理サーバーを介してテナントを管理する場合に便利です。

仮想管理サーバーを作成すると、プライマリ管理サーバーのユーザーリストとすべてのユーザー権限が継承されます。ユーザーがプライマリサーバーへのアクセス権を持っている場合、このユーザーは仮想サーバーへのアクセス権も持っています。作成後、サーバーへのアクセス権を個別に構成します。仮想管理サーバーのみに管理者を割り当てる場合は、管理者がプライマリ管理サーバーのプロパティで**アクセス権**リストに含まれていないことを確認してください。

仮想管理サーバーへの管理者アクセス権を付与することにより、仮想管理サーバーの管理者を割り当てます。次のいずれかの方法で、必要なアクセス権を付与できます：

- 管理者のアクセス権を手動で設定する
- 管理者に1つ以上のユーザーロールを割り当てる

管理者を割り当てる時は、単一の仮想管理サーバーへのアクセス権を付与するようにしてください。複数の仮想管理サーバーへのアクセス権を持つ管理者は、Kaspersky Security Center Cloud コンソールにサインインできません。

仮想管理サーバーの管理者は、プライマリ管理サーバーにサインインするのと同じ方法で Kaspersky Security Center Cloud コンソールにサインインします。Kaspersky Security Center Cloud コンソールは管理者を認証し、管理者がアクセス権を持つ仮想管理サーバーを開きます。管理者は、管理サーバーを切り替えることはできません。

必須条件

開始する前に、次の条件が満たされていることを確認してください：

- 仮想管理サーバーが削除されている。
- プライマリ管理サーバーで、仮想管理サーバーに割り当てる管理者のアカウントを作成した。
- 作成された仮想サーバー管理者のアカウントは、プライマリかセカンダリかを問わず、どのサーバーのプロパティの**アクセス権**リストにも含まれません。
- ［**一般的な機能**］→［**ユーザーのアクセス許可**］機能領域の**オブジェクト ACL の変更**権限を持っている。

アクセス権の手動設定

仮想管理サーバーの管理者を割り当てるには：

1. メインメニューで、必要な仮想管理サーバーに切り替えます：

   a. シェブロンアイコン（  ）が現在の管理サーバー名の右側に表示されます。

   b. 必要な管理サーバーを選択します。

2. メインメニューで、管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

3. ［**アクセス権**］タブで、［**追加**］をクリックします。
   プライマリ管理サーバーと現在の仮想管理サーバーのユーザーの統合リストが表示されます。

4. ユーザーのリストから、仮想管理サーバーに割り当てる管理者のアカウントを選択し、［**OK**］をクリックします。
   選択したユーザーが［**アクセス権**］タブのユーザーリストに追加されます。

5. 追加されたアカウントの横にあるチェックボックスをオンにし、［**アクセス権**］をクリックします。

6. 仮想管理サーバーで管理者が持つ権限を設定します。
   認証が成功するためには、管理者には少なくとも次の権限が必要です：

   - **読み取り**権限（［**一般的な機能**］→［**基本機能**］の機能領域）
   - **読み取り**権限（［**一般的な機能**］→［**仮想管理サーバー**］の機能領域）

変更されたユーザー権限が管理者アカウントに保存されます。

ユーザーロールの割り当てによるアクセス権の設定

あるいは、ユーザーロールを介して仮想管理サーバー管理者にアクセス権を付与することもできます。たとえば、同じ仮想管理サーバーに複数の管理者を割り当てる場合に便利です。この場合、複数の管理者に同じユーザー権限を構成する代わりに、管理者のアカウントに同じ1つ以上のユーザーロールを割り当てることができます。

ユーザーロールを割り当てて仮想管理サーバーの管理者を割り当てるには：

1. プライマリ管理サーバーで、新しいユーザーロールを作成し、管理者が仮想管理サーバーで持つ必要があるすべてのアクセス権を指定します。たとえば、様々な機能領域へのアクセスを分離する場合は、複数のロールを作成できます。

2. メインメニューで、必要な仮想管理サーバーに切り替えます：

   a. シェブロンアイコン（  ）が現在の管理サーバー名の右側に表示されます。

   b. 必要な管理サーバーを選択します。

3. 新しいロールまたは複数のロールを管理者アカウントに割り当てます。

新しいロールが管理者アカウントに割り当てられます。

オブジェクトレベルでのアクセス権の設定

機能領域レベルでのアクセス権の割り当てに加えて、仮想管理サーバー上の特定のオブジェクト（特定の管理グループやタスクなど）へのアクセスを設定できます。これを行うには、仮想管理サーバーに切り替えてから、オブジェクトのプロパティでアクセス権を設定します。

仮想管理サーバーの削除

仮想管理サーバーを削除すると、管理サーバーで作成したすべてのオブジェクト（ポリシーとタスクを含む）も削除されます。仮想管理サーバーで管理されていた管理グループの管理対象デバイスは、管理グループから削除されます。Kaspersky Security Center Cloud コンソールの管理下にデバイスを戻すには、ネットワークポーリングを実行して、検出されたデバイスを未割り当てデバイスグループから管理グループに移動します。

仮想管理サーバーを削除するには：

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。
2. 表示されるウィンドウで、［**管理サーバー**］タブに移動します。
3. 削除する仮想管理サーバーを選択します。
4. メニューヘッダーから［**削除**］を選択します。

   仮想管理サーバーが削除されます。

監視とレポート

このセクションでは Kaspersky Security Center Cloud コンソールの監視機能とレポート機能について説明します。これらの機能を使用して、インフラストラクチャの状況、保護ステータス、統計情報を確認できます。

Kaspersky Security Center Cloud コンソールの導入後または運用中に、必要に応じて監視とレポートの機能の設定を最適な状態に編集できます。

シナリオ：監視とレポート

このセクションでは、Kaspersky Security Center Cloud コンソールの監視機能とレポート機能を設定する手順を説明しています。

必須条件

組織のネットワークへの Kaspersky Security Center Cloud コンソールの導入後、監視を開始し、動作状況のレポートを生成できます。

実行するステップ

組織のネットワークにおける監視とレポートの設定は、以下の手順で進みます：

1. **デバイスのステータスの切り替えの設定**

   特定の条件に応じたデバイスのステータスの設定方法を確認します。各種設定を変更することで、重要度レベルが「緊急」または「警告」のイベントの数を変えることができます。デバイスのステータスの切り替えを設定する時には、次の点に注意してください：

   - 新しい設定が組織の情報セキュリティポリシーと矛盾しない。
   - 組織のネットワークにおける重要なセキュリティイベントに迅速に対応できる。

2. **クライアントデバイスで発生したイベントに関する通知の設定**

   実行手順の説明：クライアントデバイス上のイベントのメール通知の設定

3. **ウイルスアウトブレイクイベントについてのセキュリティネットワーク対応の変更**

   対象となるしきい値は管理サーバーのプロパティで変更できます。このイベントが発生した時に有効になるより基準の厳しいポリシーを作成したり、イベント発生時に実行されるタスクを作成できます。

4. **組織のネットワークのセキュリティステータスの確認**

   実行手順の説明：

   - 「**保護ステータス**」ウィジェットを確認する
   - **保護ステータスレポート**を生成し確認する
   - **エラーに関するレポート**を生成し確認する

5. **保護されていないクライアントデバイスの検出**

   実行手順の説明：

- **［新しいデバイス］**ウィジェットを確認する
- **製品導入レポート**を生成し確認する

6. **クライアントデバイスの保護状態の確認**

   実行手順の説明：

   - **［保護ステータス］**および**［脅威の統計］**カテゴリからレポートを生成して確認する
   - **緊急**についてのイベントの抽出を開始して確認する

7. **ライセンス情報の確認**

   実行手順の説明：

   - **［ライセンス使用状況］**ウィジェットをダッシュボードに追加して確認する
   - **ライセンス使用レポート**を生成し確認する

結果

これらの手順が完了すると、組織のネットワークの保護に関する情報を確認できるようになり、今後のセキュリティ対策の計画や脅威への対応に役立てることができます。

監視機能とレポート機能の種別の概要

組織ネットワーク上のセキュリティ関連のイベントに関する情報は管理サーバーデータベースに保存されます。イベントの情報に基づいて、Kaspersky Security Center Cloud コンソールでは、組織ネットワークを対象とした次の種別の監視機能とレポート機能を利用できます。

- ダッシュボード
- レポート
- イベントの抽出

ダッシュボード

ダッシュボードでは、組織ネットワーク内でのセキュリティトレンドをグラフや表などを通して視覚的に把握し、監視できます。

レポート

レポート機能を使用することで、組織ネットワークのセキュリティに関する詳細な数値データを取得し、これらの情報をファイルに保存したり、メールで送信したり、印刷することができます。

イベントの抽出

イベントの抽出は、管理サーバーのデータベース内に保存されているイベントを一定の条件を指定して抽出し、画面上に表示できる機能です。これらのイベントは、次のカテゴリに従ってグループ化されます：

- 重要度：**緊急イベント**、**機能エラー**、**警告**、**情報イベント**
- 発生時期：**最近のイベント**
- 種別：**ユーザー要求**、**監査イベント**

また、Kaspersky Security Center Cloud コンソールのインターフェイスで編集可能な設定を使用して、ユーザー定義のイベントの抽出を作成し表示できます。

ダッシュボードとウィジェット

このセクションでは、ダッシュボードとダッシュボードで利用できるウィジェットについて説明します。このセクションでは、ウィジェットを管理する方法と、ウィジェットの設定について説明します。

ダッシュボードの使用

ダッシュボードでは、組織ネットワーク内でのセキュリティトレンドをグラフや表などを通して視覚的に把握し、監視できます。

Kaspersky Security Center Cloud コンソールの［**監視とレポート**］セクションで、［**ダッシュボード**］をクリックすると、ダッシュボードが表示されます。

ダッシュボードでは、カスタマイズ可能なウィジェットを利用できます。円グラフや表、棒グラフ、リストなどの各種形式で表示できる様々なウィジェットを選択できます。ウィジェットに表示される情報は自動的に更新されます。更新には1～2分かかります。更新の間隔はウィジェットごとに異なります。設定メニューを使用して、任意のタイミングで手動でウィジェットを更新できます。

既定では、ウィジェットには管理サーバーのデータベースに保存されているイベントの情報が含まれています。

Kaspersky Security Center Cloud コンソールには、次のカテゴリのウィジェットが既定のウィジェットのセットとして指定されています：

- **保護ステータス**
- **製品の導入**
- **アップデート**
- **脅威の統計**
- **その他**

一部のウィジェットのテキスト情報にはリンクが含まれている場合があります。リンクをクリックすると詳細情報を確認できます。

ダッシュボードの設定では、必要に応じて、ウィジェットの追加、非表示への変更、サイズや表示の変更、移動、設定の変更を行うことができます。

ダッシュボードへのウィジェットの追加

ダッシュボードにウィジェットを追加するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. ［**Web ウィジェットを追加または復元**］をクリックします。
3. 使用可能なウィジェットのリストから、ダッシュボードに追加するウィジェットを選択します。

   ウィジェットはカテゴリ別にグループ化されています。カテゴリに含まれるウィジェットのリストを表示するには、カテゴリ名の横にあるアイコン（›）をクリックします。
4. ［**追加**］をクリックします。

選択したウィジェットがダッシュボードの一番下に追加されます。

追加したウィジェットの表示と設定を変更できます。

ダッシュボードでウィジェットを非表示にする操作

ダッシュボードで表示中のウィジェットを非表示にするには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 非表示にするウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. ［**Web ウィジェットを非表示にする**］を選択します。
4. ［**警告**］ウィンドウが表示されたら、［**OK**］をクリックします。

選択したウィジェットが表示されなくなります。いつでも、このウィジェットをもう一度ダッシュボードに追加できます。

ダッシュボードでのウィジェットの移動

ダッシュボードでウィジェットを移動するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 移動するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. ［**移動**］を選択します。
4. ウィジェットを移動する場所をクリックします。選択できるのは別のウィジェットの表示位置のみです。

選択したウィジェットの表示位置が入れ替わります。

ウィジェットのサイズと表示形式の変更

グラフを表示するウィジェットでは、グラフの形式（棒グラフまたは折れ線グラフ）を変更できます。一部のウィジェットではウィジェットのサイズを「コンパクト」「中サイズ」「最大」に変更できます。

ウィジェットの表示形式を変更するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 編集するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. 次のいずれかの手順を実行します：
   - ウィジェットを棒グラフとして表示するには、［**グラフの種別：棒**］をオンにします。
   - ウィジェットを折れ線グラフとして表示するには、［**グラフの種別：折れ線**］をオンにします。
   - ウィジェットの表示領域を変更するには、次の値のうちの1つを選択してください：
     - **コンパクト**
     - **コンパクト（棒グラフのみ）**
     - **中サイズ（円グラフ）**
     - **中サイズ（棒グラフ）**
     - **最大**

選択したウィジェットの表示形式が変更されます。

ウィジェットの設定の変更

ウィジェットの設定を変更するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 変更するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. ［**設定を表示する**］を選択します。
4. ウィジェットの設定ウィンドウが表示されるので、必要に応じてウィジェットの設定を変更します。
5. ［**保存**］をクリックして変更内容を保存します。

選択したウィジェットの設定が変更されます。

どのような設定項目が存在するかは、ウィジェットごとに異なります。一般的な設定項目としてはたとえば次のような設定があります：

- **Web ウィジェットの範囲**（管理グループやデバイスの抽出など、ウィジェットが情報を表示する対象オブジェクトの範囲）。
- **タスクの選択**（ウィジェットが情報を表示する対象タスクの範囲）。
- **時間**（［開始日から終了日まで］、［開始日から現在まで］、［今日から指定した日数だけ過去にさかのぼった範囲を対象］のいずれかの形式で指定できる、ウィジェットが情報を表示する対象期間）。
- **ステータスを「緊急」にする条件**および**ステータスを「警告」にする条件**（ステータス信号の色を決定するルール）。

ウィジェットの設定を変更した後、ウィジェット上のデータを手動で更新できます。

ウィジェットのデータを更新するには：

1. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
2. 移動するウィジェットに隣接する設定アイコン（⚙）をクリックします。
3. ［**更新**］を選択します。

ウィジェットのデータが更新されました。

ダッシュボードのみモードについて

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

ユーザーがダッシュボードのみモードで作業する場合、次の制限事項が適用されます：

- ユーザーにはメインメニューは表示されません。そのためネットワーク保護の設定などを変更することはできません。
- ユーザーはウィジェットに対して表示もしくは非表示にするなどの操作を行うことはできません。そのため、オブジェクトの計算ルールや時間間隔の指定など、ユーザーに必要なすべてのウィジェットをダッシュボードに表示できるように設定する必要があります。

自分自身にダッシュボードのみモードを割り当てることはできません。このモードで作業したい時は、システム管理者、マネージドサービスプロバイダー（MSP）、または［**一般的な機能：ユーザー権限**］機能領域の**オブジェクト ACL の変更**権限を持つユーザーに問い合わせてください。

ダッシュボードのみモードの設定

ダッシュボードのみモードの設定を始める前に、次の要件を満たしていることを確認してください：

- ［**一般的な機能：ユーザー権限**］機能領域の**オブジェクト ACL の変更**権限を持っている。この権限を持っていない場合、モードの設定用タブは表示されません。

- ［**一般的な機能:：基本機能**］の機能領域の**読み取り**権限を持っている。

ネットワークで管理サーバーの階層が配置されている場合、ダッシュボードのみモードを設定するには［**ユーザーとロール**］→［**ユーザーとグループ**］セクションの［**ユーザー**］タブでユーザーアカウントが使用できるサーバーに移動します。プライマリサーバーまたは物理セカンダリサーバーを選択できます。仮想サーバーでモードを調整することはできません。

ダッシュボードのみモードを設定するには：

1. メインメニューで、［**ユーザーとロール**］→［**ユーザーとグループ**］の順に移動し、［**ユーザー**］タブを選択します。
2. ダッシュボードのウィジェットを調整するユーザーアカウント名をクリックします。
3. アカウント設定ウィンドウが表示されたら、［**ダッシュボード**］を選択します。

   表示されたタブに、ユーザーに表示されるものと同じダッシュボードが表示されます。
4. ［**ダッシュボードのみモードでコンソールを表示**］オプションがオンになっている場合は切り替えスイッチをオフにします。

   このオプションがオンになっていると、自身もダッシュボードを変更することができません。このオプションをオフにした後、ウィジェットを管理できるようになります。
5. ダッシュボードの表示を設定します。カスタマイズ可能なアカウントを持つユーザー向けに、［**ダッシュボード**］タブで事前設定されたウィジェットのセットが使用可能です。ユーザーはウィジェットのサイズや設定を変更したり、ダッシュボードからウィジェットを追加したり削除したりすることはできません。そのため、ユーザーに対してネットワーク保護の統計が表示されるようにウィジェットを調整します。［**監視とレポート**］→［**ダッシュボード**］セクションで行うのと同様の操作を［**ダッシュボード**］タブで実行します：
   - ダッシュボードに新しいウィジェットを追加します。
   - ユーザーに必要ないウィジェットを非表示にします。
   - 必要な順番にウィジェットを移動します。
   - ウィジェットの表示方法やサイズを変更します。
   - ウィジェットの設定を変更します。
6. ［**ダッシュボードのみモードでコンソールを表示**］オプションの切り替えスイッチをオンにします。

   その後、ユーザーはダッシュボードのみを使用できるようになります。ユーザーは統計情報を監視できますが、ネットワーク保護の設定やダッシュボードの表示を変更することはできません。ユーザーとお客様ご自身にも同じダッシュボードが表示され、お客様もダッシュボードを変更することはできません。

   このオプションをオフにしておくと、ユーザーにはメインメニューが表示され、ユーザーは Kaspersky Security Center Cloud コンソールでセキュリティ設定やウィジェットの変更を含む、様々な操作を実行することができます。
7. ダッシュボードのみモードの設定を完了したら、［**保存**］をクリックします。この後、準備したダッシュボードがユーザーに表示されます。
8. ユーザーが、サポートされるカスペルスキー製品の統計を表示するアクセス権を必要とする場合は、ユーザーの権限を設定します。設定すると、カスペルスキー製品のデータがユーザーのこれらのアプリケーションのウィジェットに表示されるようになります。

ユーザーはカスタマイズされたアカウントで Kaspersky Security Center Cloud コンソールにログインし、ダッシュボードのみモードでネットワーク保護の統計を監視できるようになりました。

レポート

このセクションでは、レポートの使用、カスタムレポートテンプレートの管理、レポートテンプレートを使用した新規レポートの作成、レポートの配信タスクの作成について説明します。

レポートの使用

レポート機能を使用することで、組織ネットワークのセキュリティに関する詳細な数値データを取得し、これらの情報をファイルに保存したり、メールで送信したり、印刷することができます。

Kaspersky Security Center Cloud コンソールの［**監視とレポート**］セクションで、［**レポート**］をクリックすると、レポートが表示されます。

既定では、レポートには過去 30 日の情報が含まれます。

Kaspersky Security Center Cloud コンソールには、次のカテゴリのレポートが既定のウィジェットのセットとして指定されています：

- **保護ステータス**
- **製品の導入**
- **アップデート**
- **脅威の統計**
- **その他**

カスタムレポートテンプレートの作成、レポートテンプレートの編集、レポートテンプレートの削除を行うことができます。

既存のテンプレートに基づくレポートの作成、ファイルへのレポートのエクスポート、レポートの配信タスクの作成を行うことができます。

レポートテンプレートの作成

レポートテンプレートを作成するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。

レポートサブセクションのレポートテンプレートのリスト

2. ［**追加**］をクリックします。

   新規レポートテンプレートウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。

3. ウィザードの最初のページで、レポート名の入力とレポート種別の選択を行います。

新規レポートテンプレートウィザード。レポートテンプレートの名前と種類の指定

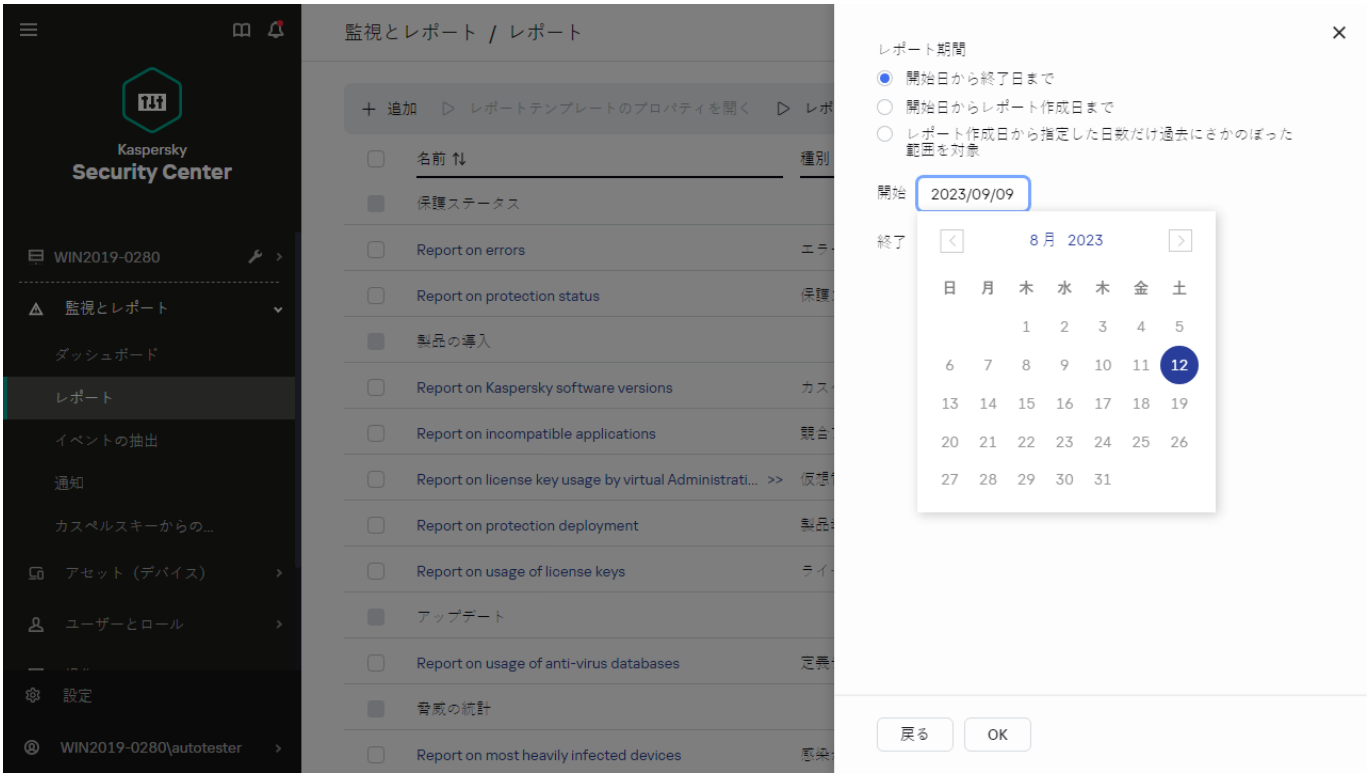
4. ウィザードの［**範囲**］ウィンドウで、このレポートテンプレートに基づいたレポートでデータの表示対象にするクライアントデバイスを指定します（管理グループ、デバイスの抽出、指定したデバイス、ネットワーク内のすべてのデバイス）。

新規レポートテンプレートウィザード。レポートテンプレートの範囲の指定

5. ウィザードの［**レポート期間**］ウィンドウで、レポートの対象期間を指定します。次の値を設定できます：

   - 指定した 2 つの日付の間の期間
   - 指定日からレポート作成日までの期間
   - レポート作成日から指定した日数だけ過去にさかのぼった期間

   一部のレポートではこのページが表示されない場合もあります。



新規レポートテンプレートウィザード。レポート期間の指定

6. ［**OK**］をクリックしてウィザードを終了します。

7. 次のいずれかの手順を実行します：

- ［**保存して実行**］をクリックすると、新しいレポートテンプレートを保存して、テンプレートに基づくレポートを実行できます。
  レポートテンプレートが保存されます。レポートが生成されます。

- ［**保存**］をクリックすると、新しいレポートテンプレートを保存できます。
  レポートテンプレートが保存されます。

新しいテンプレートを使用して、レポートの作成と表示ができます。

レポートテンプレートのプロパティの表示と編集

レポートテンプレートについて、レポートテンプレートの名前やレポートに表示されるフィールドなどの基本的なプロパティを表示し、編集できます。

レポートテンプレートのプロパティを表示したり編集するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。

2. プロパティの表示と編集を行うレポートテンプレートに隣接するチェックボックスを選択します。
   あるいは、まずレポートを生成して、次に［**編集**］をクリックします。

3. ［**レポートテンプレートのプロパティを開く**］をクリックします。
   ［**レポート「<レポート名>」の編集**］ウィンドウの［**全般**］タブが表示されます。

4. レポートテンプレートのプロパティを編集します。

- ［**全般**］タブ：

  - レポートテンプレート名

  - **表示する項目数の上限**

このオプションをオンにすると、詳細なレポートデータの表に表示されるエントリ数に、指定した上限値が設定されます。このオプションは、レポートをファイルにエクスポートする時にレポートに含めることができるイベントの最大数には影響しません。

レポートのエントリは、レポートテンプレートの［**フィールド**］→［**詳細フィールド**］セクションで指定したルールに従って並べ替えられ、合致するエントリのうち表示順が上のエントリだけが維持されます。詳細レポートのタイトルには、レポートテンプレートで設定したその他の条件に合致するエントリの合計数と表示されている数が表示されます。

このオプションをオフにすると、詳細なレポートデータの表にはすべての使用可能なエントリが表示されますこのオプションをオフにすることは推奨されません。表示されるレポートエントリの数を制限することにより、DBMS（データベース管理システム）の負荷を減らし、レポートの生成とエクスポートの所要時間を削減できます。一部のレポートではエントリ数が多すぎる場合があります。このような場合、すべてのエントリに目を通し分析することは困難です。また、こうしたレポートの生成中にデバイスのメモリ不足が発生し、レポート自体を表示できない可能性もあります。

既定では、このオプションはオンです。既定値は 1000 です。

Kaspersky Security Center Cloud コンソールのインターフェイスで表示できるエントリの最大数は 2500 個です。これを超える数のイベントを表示する必要がある場合は、レポートのエクスポート機能を使用します。

- **グループ**

  レポートの作成対象にするクライアントデバイスを変更するには、［**設定**］をクリックします。一部のレポートの種別では、このボタンを使用できない場合があります。実際の設定は、レポートテンプレートの作成時に指定した設定によって異なります。

- **時間**

  レポートの対象期間を変更するには、［**設定**］をクリックします。一部のレポートの種別では、このボタンを使用できない場合があります。次の値を設定できます：

  - 指定した 2 つの日付の間の期間
  - 指定日からレポート作成日までの期間
  - レポート作成日から指定した日数だけ過去にさかのぼった期間

- **セカンダリまたは仮想管理サーバーのデータを含める**

  このオプションをオンにすると、レポートテンプレートを作成する管理サーバーに属するセカンダリ管理サーバーおよび仮想管理サーバーからの情報をレポートに含めます。

  現在の管理サーバーのデータのみを表示する場合は、このオプションをオフにします。

  既定では、このオプションはオンです。

- **ネスト数の上限**

  対象の管理サーバーに属するセカンダリ管理サーバーおよび仮想管理サーバーのうち、指定したネスト数以内のサーバーのデータをレポートに含めます。

  既定値は 1 です。ツリー内でより下位に位置するセカンダリ管理サーバーの情報を取得する必要がある場合、この値を変更することができます。

- **データの待機時間（分）**

レポートを生成する前に、レポートテンプレートを作成する管理サーバーは、セカンダリ管理サーバーからデータが送信されるのを、指定した分数だけ待機します。指定した時間が経過してもセカンダリ管理サーバーからデータを取得できなかった場合は、これらのデータを除外してレポートが実行されます。［**セカンダリ管理サーバーのデータをキャッシュする**］を有効にすると、実際のデータの代わりにキャッシュデータがレポートに表示されます。無効にすると、［**該当なし**］と表示されます。

既定値は 5 分です。

- **セカンダリ管理サーバーのデータをキャッシュする**

  セカンダリ管理サーバーからレポートテンプレートを作成する管理サーバーに定期的にデータが送信されます。送信されたデータはキャッシュに保存されます。

  レポートの生成時に現在の管理サーバーがセカンダリ管理サーバーからデータを取得できなかった場合、キャッシュから取得したデータがレポートに表示されます。データがキャッシュに送信された日付も合わせて表示されます。

  このオプションをオンにすると、最新のデータを取得できなかった場合でもセカンダリ管理サーバーの情報を表示できます。ただし、表示されるデータが最新のものではない場合があります。

  既定では、このオプションはオフです。

- **キャッシュの更新頻度（時間）**

  セカンダリ管理サーバーからレポートテンプレートを作成する管理サーバーに定期的にデータが送信されます。この期間は時間単位で指定できます。0 時間を指定すると、レポートの生成時にのみデータが送信されます。

  既定値は 0 です。

- **セカンダリ管理サーバーから詳細情報を転送する**

  生成されたレポートの詳細なレポートデータの表に、レポートテンプレートを作成する管理サーバーのセカンダリ管理サーバーから取得したデータを含めます。

  このオプションをオンにすると、レポートの生成にかかる時間が長くなり、管理サーバー間のトラフィックも増大します。ただし、1つのレポートですべてのデータを表示できるメリットもあります。

  このオプションをオンにする他に、先に詳細なレポートデータを分析してエラーが発生しているセカンダリ管理サーバーを特定した上で、エラーが発生している管理サーバーのみを対象にレポートを生成するという方法も活用できます。

  既定では、このオプションはオフです。

- ［**フィールド**］タブ

  レポートで表示されるフィールドを選択し、［**上へ**］と［**下へ**］を使用して、フィールドの順序を変更します。［**追加**］または［**編集**］をクリックすると、該当するフィールドに基づいて情報の並べ替えとフィルター処理を行えるかどうかを設定できます。

  ［**詳細フィールドのフィルター**］で、［**フィルターの変換**］をクリックすることでも拡張フィルタリング形式の使用を開始できます。この形式は、論理演算子「OR」を使用することで様々なフィールドに指定された条件を結合できます。ボタンをクリックした後、［**フィルターの変換**］パネルが右側に開きます。［**フィルターの変換**］をクリックして変換を確定します。［**詳細フィールド**］セクションで論理演算子「OR」を使用することで適用される条件付きの変換されたフィルターを定義できるようになります。

複雑なフィルタリング条件をサポートする形式にレポートを変換すると、以前の Kaspersky Security Center (11 より前のバージョン) でレポートを使用できなくなることがあります。また、このような互換性のないバージョンの製品を実行しているセカンダリの管理サーバーからのデータは、変換されたレポートに含めることができません。

5. ［**保存**］をクリックして変更内容を保存します。

6. ［**レポート <レポート名> の編集**］ウィンドウを閉じます。

レポートテンプレートのリストに更新したレポートテンプレートが表示されます。

レポートのファイルへのエクスポート

1 つまたは複数のレポートを XML、HTML、または 1 つの PDF として保存できます。Kaspersky Security Center Cloud コンソールでは、最大 10 件のレポートを指定した形式のファイルに同時にエクスポートできます。

レポートをファイルにエクスポートするには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。

2. エクスポートするレポートを選択します。
   10 件を超えるレポートを選択すると、［**レポートのエクスポート**］がオフになります。

3. ［**レポートのエクスポート**］をクリックします。

4. 開いたウィンドウで、次のエクスポートパラメータを指定します：

   - **ファイル名**。
     エクスポートするレポートを 1 つ選択する場合は、レポートファイル名を指定します。
     複数のレポートを選択した場合、レポートファイル名は、選択したレポートテンプレートの名前と一致します。

   - **エントリの最大数**。
     レポートファイルに含まれるエントリの最大数を指定します。既定値は 10,000 です。

   - **ファイル形式**。
     レポートのファイル形式（XML、HTML、PDF）を選択します。複数のレポートをエクスポートする場合、選択したすべてのレポートが指定された形式で個別のファイルとして保存されます。

5. ［**レポートのエクスポート**］をクリックします。

レポートは、指定した形式でファイルに保存されます。

レポートの生成と表示

レポートを作成および表示するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. レポートの作成に使用するレポートテンプレートの名前をクリックします。

   選択したテンプレートを使用してレポートが作成され、表示されます。

レポートデータは英語でのみ表示され、他のローカライズは使用できません。

レポートには次のデータが表示されます：

- ［**サマリー**］タブ：
  - レポート名とレポート種別、概要説明、レポート期間、レポートが作成されたデバイスグループに関する情報。
  - 代表的なレポートのデータを示している図表。
  - 計算されたレポートの指標を含む表。
- **[詳細]**タブで、詳細レポートデータの表が表示されます。

レポート配信タスクの作成

選択したレポートを配信するタスクを作成できます。

レポート配信タスクを作成するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］に移動します。
2. レポート配信タスクを作成するレポートテンプレートに隣接するチェックボックスをオンにします（後の手順でも選択できるため、省略可能です）。
3. ［**レポート配信タスクの新規作成**］をクリックします。
4. 新規タスクウィザードが起動します。［**次へ**］をクリックしながらウィザードに沿って手順を進めます。
5. ウィザードの最初のページで、タスク名を入力します：既定の名前は「**レポートの配信（<タスクの連番>）**」です。
6. ウィザードのタスク設定のページで、次の設定を指定します：
   a. タスクでレポートを配信するレポートテンプレート。ステップ 2 で選択済みの場合は、このステップを省略できます。
   b. レポート形式（HTML、XLS、PDF）。
   c. レポートをメールで送信するかどうかと、送信する場合のメール通知設定。
7. タスク作成後に、続けてタスクのその他の設定を編集する場合、ウィザードの［**タスク作成の終了**］ページで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。

8. タスクを作成しウィザードを終了するには、［**作成**］をクリックします。

   レポート配信タスクが作成されます。［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにした場合、タスク設定ウィンドウが表示されます。

レポートテンプレートの削除

レポートのテンプレートを削除するには：

1. メインメニューで、［**監視とレポート**］→［**レポート**］の順に選択します。
2. 削除するレポートテンプレートの隣にあるチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで、［**OK**］をクリックして処理を確定します。

選択したレポートテンプレートが削除されます。これらのレポートテンプレートがレポートの配信タスクに含まれていた場合、タスクからも該当するレポートテンプレートが削除されます。

イベントとイベントの抽出

このセクションでは、イベントとイベントの抽出、Kaspersky Security Center Cloud コンソールコンポーネントで発生するイベントの種別、頻出イベントのブロック管理について説明します。

Kaspersky Security Center Cloud コンソールのイベントについて

Kaspersky Security Center Cloud コンソールでは、管理サーバーと管理対象デバイスにインストールされた他のカスペルスキー製品の動作中に発生したイベントの情報を受信できます。イベントに関する情報は管理サーバーデータベースに保存されます。この情報は外部 SIEM システムにエクスポートできます。イベント情報を外部 SIEM システムにエクスポートすると、SIEM システムの管理者は、管理対象デバイスまたはデバイスのグループで発生したセキュリティシステムイベントに迅速に対処できます。

種別ごとのイベント

Kaspersky Security Center Cloud コンソールには、次のイベント種別があります：

- 一般イベント：管理対象となるカスペルスキー製品すべてで共通して発生するイベントです。一般イベントの例としては「ウイルスアウトブレイク」があります。一般イベントでは、構文と形式が厳密に定義されています。一般イベントは、レポートやダッシュボードなどで使用されます。
- 管理対象のカスペルスキー製品それぞれに固有のイベント：管理対象となるカスペルスキーの各製品には、独自のイベントのセットがあります。

ソース別イベント

製品によって生成されるイベントの完全なリストは、アプリケーションポリシーの［**イベントの設定**］タブで確認できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示できます。

イベントは、次の製品で生成される可能性があります：

- Kaspersky Security Center Cloud コンソールのコンポーネント：
  - 管理サーバー
  - ネットワークエージェント
- 管理対象のカスペルスキー製品

  管理対象のカスペルスキー製品によって生成されるイベントの詳細は、該当する製品のドキュメントを参照してください。

重要度別イベント

各イベントには固有の重要度があります。発生した状況に応じて、イベントには様々な重要度が割り当てることができます。イベントの重要度には次の 4 つがあります：

- *緊急イベント*は、データの損失、誤動作、または重大なエラーを招きかねない重大な問題が発生したことを示すイベントです。
- *機能エラー*は、アプリケーションの動作中または手順の実行中に重大な問題、エラー、または誤動作の発生を示すイベントです。
- *警告*は、必ずしも重大ではなくても、将来問題が発生する可能性があることを示すイベントです。こうしたイベントの発生後、データや機能を失わずにアプリケーションを復元できるのであれば、ほとんどのイベントは警告を意味します。
- *情報*イベントは、操作が適切に完了したこと、アプリケーションが適切に動作していること、手順が完了したことを伝えるために発生するイベントです。

各イベントには保管期間が定義されており、保管期間中、ユーザーは Kaspersky Security Center Cloud コンソールでイベントを表示または変更することができます。一部のイベントは既定により、管理サーバーデータベースに保管されません。保管期間がゼロと定義されているためです。管理サーバーデータベースに 1 日以上保管されるイベントだけを外部システムにエクスポートできます。

Kaspersky Security Center Cloud コンソールのコンポーネントのイベント

Kaspersky Security Center Cloud コンソールの各コンポーネントには、独自のイベント種別のセットがあります。このセクションでは、Kaspersky Security Center Cloud コンソール管理サーバーとネットワークエージェントで発生するイベントの種別について説明します。カスペルスキー製品で発生する可能性のあるイベントの種別は、このセクションの説明には含まれていません。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

イベント種別のデータ構造の説明

イベント種別ごとに、表示名、識別子（ID）、英字コード、内容の説明、既定の保管期間を記載しています。

- **イベント種別の表示名**：イベントを設定してそれが発生すると、この列のテキストが Kaspersky Security Center Cloud コンソールで表示されます。
- **イベント種別の ID**：イベント解析用のサードパーティ製品を使用してイベントを処理すると、この列の数字コードが使用されます。
- **イベント種別**（英字コード）：このコードは、Kaspersky Security Center Cloud コンソールのデータベースのパブリックビューを使用したイベントの参照時および処理時に使用されます。
- **説明**：この列では、イベントが発生する状況と可能な対応が説明されています。
- **既定の保管期間**：この列には、イベントが管理サーバーデータベースに保管され、管理サーバーのイベントリストに表示される日数が記載されています。この期間が過ぎると、イベントが削除されます。イベントの保管期間の値が「0」の場合、これらのイベントについては検知のみが行われ、管理サーバーのイベントリストへの表示は行われません。

管理サーバーのイベント

このセクションには、管理サーバーに関するイベントの情報が記載されています。

管理サーバーの緊急イベント

次の表は、重要度が「**緊急**」に分類される Kaspersky Security Center Cloud コンソール管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

管理サーバーの緊急イベント

イベント種別の表示名	イベント種別の ID	イベント種別	説明	既定の保管期間
ライセンス数の上限を超えました	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	1 日に 1 回、Kaspersky Security Center Cloud コンソールはライセンスの上限の超過が発生していないかどうかを確認します。	180 日間

			この種別のイベントは、クライアントデバイスにインストールされているカスペルスキー製品で、ライセンスの上限の超過を管理サーバーが検出しており、単一のライセンスに紐付けられていて現在使用中のライセンス単位数がそのライセンスで本来許可されている合計ライセンス単位数の 110% を超えている場合に記録されます。 このイベントが発生した場合でも、クライアントデバイスの保護は継続されます。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストを確認します。使用されていないデバイスを削除します。 • 製品を使用できるデバイス数の上限が増えるように、ライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。 Kaspersky Security Center Cloud コンソールでは、ライセンス数の上限の超過時にイベントを生成するルールを指定できます。	
ウイルスアウトブレイク	26（ファイル脅威対策の場合）	GNRL_EV_VIRUS_OUTBREAK	この種別のイベントは、短期間のうちに複数の管理対象デバイスで検知された悪意のあるオブジェクトの数がしきい値を超えた場合に記録されます。 このイベントには、次の方法で対応できます： • 対象となるしきい値を管理サーバーのプロパティで編集します。 • このイベントの発生時に有効になるより基準の厳しいポリシーを作成したり、イベント発生時に実行されるタスクを作成します。	180 日間
ウイルスアウトブレイク	27（メール脅威対策の場合）	GNRL_EV_VIRUS_OUTBREAK	この種別のイベントは、短期間のうちに複数の管理対象デバイスで検知された悪意のあるオブジェクトの数がしきい値を超えた場合に記録されます。 このイベントには、次の方法で対応できます：	180 日間

			• 対象となるしきい値を管理サーバーのプロパティで編集します。 • このイベントの発生時に有効になるより基準の厳しいポリシーを作成したり、イベント発生時に実行されるタスクを作成します。	
ウイルスアウトブレイク	28（ファイアウォールの場合）	GNRL_EV_VIRUS_OUTBREAK	この種別のイベントは、短期間のうちに複数の管理対象デバイスで検知された悪意のあるオブジェクトの数がしきい値を超えた場合に記録されます。 このイベントには、次の方法で対応できます： • 対象となるしきい値を管理サーバーのプロパティで編集します。 • このイベントの発生時に有効になるより基準の厳しいポリシーを作成したり、イベント発生時に実行されるタスクを作成します。	180日間
デバイスが管理対象外になりました	4111	KLSRV_HOST_OUT_CONTROL	この種別のイベントは、デバイスはネットワーク上で可視だが管理サーバーに接続していない状態が指定期間を越えて継続すると記録されます。 デバイス上でネットワークエージェントの正常な動作を妨げている要素を特定します。原因としては、ネットワークの問題や、ネットワークエージェントがデバイスから削除された状況などが考えられます。	180日間
デバイスのステータスが「緊急」です	4113	KLSRV_HOST_STATUS_CRITICAL	この種別のイベントは、管理対象デバイスに「*緊急*」ステータスが割り当てられると記録されます。デバイスのステータスが「*緊急*」に切り替わる条件を設定できます。	180日間
機能が制限されています	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	この種別のイベントは、Kaspersky Security Center Cloudコンソールの動作モードが変更されて基本機能のみが使用可能になり、脆弱性とパッチ管理機能およびモバイルデバイス管理機能が使用できない時に記録されます。	180日間

			イベントが発生する理由と対応は次の通りです： • ライセンスの有効期限が終了している：Kaspersky Security Center Cloud コンソールの全機能を使用できるモードで必要なライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。 • ライセンスの上限で指定された台数を超過して管理サーバーでデバイスを管理している：管理サーバーの管理グループから別の管理サーバーの管理グループにデバイスを移動します（移動先の管理サーバーのライセンスの上限内で）。	
ライセンスの有効期間がまもなく終了します	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	この種別のイベントは、製品版ライセンスの有効期限が近づいている時に発生します。 1日に1回、Kaspersky Security Center はライセンス有効期間の終了日が近づいているかどうかを確認します。この種別のイベントは、ライセンスの有効期限まで残り 30 日、15 日、5 日および1日となった時に発生します。この日数は変更できません。管理サーバーがライセンスの有効期限より前に指定された日にオフになった場合は翌日までイベントは発生しません。 製品版ライセンスの有効期間が終了した場合は、Kaspersky Security Center Cloud コンソールは基本機能のみを提供します。 このイベントには、次の方法で対応できます： • 予備のライセンスが管理サーバーに追加されていることを確認します。 • 定額制サービスをご利用の場合は、必ず更新してください。支払い期日までに決済された場合、無制限の定額制サービスは自動的に更新されます。	180 日間
証明書の	4132	KLSRV_CERTIFICATE_EXPIRED	近日中に情報を追加する予定です。	180 日間

有効期間が終了しています				
カスペルスキー製品モジュールのアップデートが取り消されました	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	この種別のイベントは、カスペルスキーのテクニカルスペシャリストにより、より新しいバージョンの製品にアップデートする必要があるなどの理由でシームレスアップデートの利用が拒否された場合（アップデートのステータスとして「*取り消し*」が表示）に記録されます。このイベントは、Kaspersky Security Center Cloud コンソールのパッチを対象としており、管理対象のカスペルスキー製品モジュールとの関連はありません。イベントでは、シームレスアップデートがインストールされなかった理由に関する情報が提供されます。	180 日間
監査：SIEM へエクスポートできませんでした	5130	KLAUD_EV_SIEM_EXPORT_ERROR	このタイプのイベントは、SIEM システムとの接続エラーが原因で SIEM システムへのイベントのエクスポートが失敗した場合に発生します。	180 日間

管理サーバーの機能エラーイベント

次の表は、重要度が「**機能エラー**」に分類される Kaspersky Security Center Cloud コンソール管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

管理サーバーの機能エラーイベント

イベント種別の表示名	イベント種別の ID	イベント種別	説明	既定の保管期間
インストール数の上限を超えたライセンス認証済みアプリケー	4126	KLSRV_INVLICPROD_EXCEDED	この種別のイベントは、管理サーバーによって 1 時間ごとに生成されます。この種別のイベントは、Kaspersky Security Center Cloud コンソールでサードパーティ製品を	180 日間

ションググループがあります			管理していて、サードパーティ製品のライセンスで設定された上限を超えると記録されます。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストを確認します。該当するサードパーティ製品が使用されていないデバイスからサードパーティ製品を削除します。 • 製品を使用できるデバイス数の上限が増えるように、サードパーティ製品のライセンスを追加します。 ライセンス認証済みアプリケーショングループ機能を使用することで、サードパーティ製品のライセンスを管理できます。ライセンス認証済みアプリケーショングループには、管理者が設定した基準を満たすサードパーティ製品が含まれます。	

管理サーバーの警告イベント

次の表は、重要度が「**警告**」に分類される Kaspersky Security Center Cloud コンソール管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

管理サーバーの警告イベント

イベント種別の表示名	イベント種別の ID	イベント種別	説明	既定の保管期間
ライセンス数の上限を超えました	4098	KLSRV_EV_LICENSE_CHECK_100_110	1 日に 1 回、Kaspersky Security Center Cloud コンソールはライセンスの上限の超過が発生していないかどうかを確認します。	90 日間

			この種別のイベントは、クライアントデバイスにインストールされているカスペルスキー製品でライセンスの上限の超過が発生していることを管理サーバーが検知し、なおかつ単一のライセンスに紐付けられていて現在使用中のライセンス単位数がそのライセンスで本来許可されている合計ライセンス単位数の 100% から 110% の範囲内の場合に記録されます。 このイベントが発生した場合でも、クライアントデバイスの保護は継続されます。 このイベントには、次の方法で対応できます： • 管理対象デバイスのリストを確認します。使用されていないデバイスを削除します。 • 製品を使用できるデバイス数の上限が増えるように、ライセンスを追加します（有効なアクティベーションコードまたはライセンス情報ファイルを管理サーバーに追加）。Kaspersky Security Center Cloud コンソールでは、ライセンス数の上限の超過時にイベントを生成するルールを指定できます。	
デバイスがネットワーク上で長期間アクティブになっていません	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	近日中に情報を追加する予定です。	90 日間
デバイスの名前が競合しています	4102	KLSRV_EVENT_HOSTS_CONFLICT	近日中に情報を追加する予定です。	90 日間
デバイスのステータスが「警告」です	4114	KLSRV_HOST_STATUS_WARNING	この種別のイベントは、管理対象デバイスに「*警告*」ステータスが割り当てられると記録されます。デバイスのステータスが「*警告*」に切り替わる条件を設定できます。	90 日間

インストール数が上限に近づいているライセンス認証済みアプリケーショングループがあります	4127	KLSRV_INVLICPROD_FILLED	近日中に情報を追加する予定です。	90日間
証明書が要求されました	4133	KLSRV_CERTIFICATE_REQUESTED	近日中に情報を追加する予定です。	90日間
証明書が削除されました	4134	KLSRV_CERTIFICATE_REMOVED	近日中に情報を追加する予定です。	90日間
APNs 証明書の有効期間が終了しています	4135	KLSRV_APN_CERTIFICATE_EXPIRED	近日中に情報を追加する予定です。	90日間
APNs 証明書の有効期間がまもなく終了します	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	近日中に情報を追加する予定です。	90日間
モバイルデバイスに FCM メッセージを送信できませんでした	4138	KLSRV_GCM_DEVICE_ERROR	近日中に情報を追加する予定です。	90日間
FCM メッセージを FCM サーバーに送信している時に HTTP エラーが発生しました	4139	KLSRV_GCM_HTTP_ERROR	近日中に情報を追加する予定です。	90日間
FCM メッセージを FCM サーバーに送信できませんでした	4140	KLSRV_GCM_GENERAL_ERROR	近日中に情報を追加する予定です。	90日間
セカンダリ管理サーバーとの接続が中断されました	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	近日中に情報を追加する予定です。	90日間
プライマリ管理サーバーとの接続が中断されました	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	近日中に情報を追加する予定です。	90日間
KSN プロキシサーバー	7719	KSNPROXY_STARTED_CON_CHK_FAILED	近日中に情報を追加する予定です。	90日間

が起動しました。KSN可用性をチェックできませんでした				
カスペルスキー製品モジュールの新しいアップデートが登録されました	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	近日中に情報を追加する予定です。	90日間
データベースのイベントの上限数を超えました。イベントの削除が開始されました	4145	KLSRV_EVP_DB_TRUNCATING	この種別のイベントは、管理サーバーのデータベース容量が上限に達して、データベース内の古いイベントの削除が開始された時に記録されます。 このイベントには、次の方法で対応できます： • 管理サーバーデータベースに記録するイベント数の上限を変更してください。 • 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください。	90日間
データベースのイベントの上限数を超えました。このイベントは削除されました	4146	KLSRV_EVP_DB_TRUNCATED	この種別のイベントは、管理サーバーのデータベース容量が上限に達して、データベース内の古いイベントが削除された時に記録されます。 このイベントには、次の方法で対応できます： • 管理サーバーデータベースに保管できるイベント数の上限を変更してください。 • 管理サーバーデータベースへの保存対象に含めるイベント種別を減らしてください。	90日間
ライセンスの有効期間がまもなく終了します	4128	KLSRV_INVLICPROD_EXPIRED_SOON	近日中に情報を追加する予定です。	90日間
監査：SIEM	5120	KLAUD_EV_SIEM_TEST_FAILED	このタイプのイベントは、	90

サーバーへの接続テストが失敗しました			SIEM サーバーへの自動接続テストが失敗した時に発生します。	日間

管理サーバーの情報イベント

次の表は、重要度が「**情報**」に分類される Kaspersky Security Center Cloud コンソール管理サーバーのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。管理サーバーの場合、管理サーバーのプロパティでもイベントリストを表示または設定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

管理サーバーの情報イベント

イベント種別の表示名	イベント種別の ID	イベント種別	既定の保管期間
ライセンス使用率が 90% を超えています	4097	KLSRV_EV_LICENSE_CHECK_90	30 日間
新しいデバイスが検出されました	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 日間
デバイスがルールに従って自動的に移動されました	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 日間
デバイスがグループから削除されました：ネットワーク上で長期間アクティブになっていません	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 日間
インストール数が上限に近づいている（95% を超える数を使用済み）ライセンス認証済みアプリケーショングループがあります	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 日間
カスペルスキーへ分析のために送付するファイルが見つかりました	4131	KLSRV_APS_FILE_APPEARED	30 日間
このモバイルデバイス上で FCM 送信者 ID が変更されました	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 日間
指定のフォルダーにアップデートがコピーされました	4122	KLSRV_UPD_REPL_OK	30 日間
セカンダリ管理サーバーとの接続が確立されました	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 日間
プライマリ管理サーバーとの接続が確立されました	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 日間
定義データベースがアップデートされました （Kaspersky Security Center Cloud コンソールでは、セカンダリ管理サーバーでのみ、このイベント種別を使用できます。）	4144	KLSRV_UPD_BASES_UPDATED	30 日間

KSN プロキシサーバーが起動しました。KSN 可用性チェックが完了しました	7718	KSNPROXY_STARTED_CON_CHK_OK	30 日間
KSN プロキシが停止しました	7720	KSNPROXY_STOPPED	30 日間
監査：管理サーバーとの接続が確立されました	4147	KLAUD_EV_SERVERCONNECT	30 日間
監査：オブジェクトが変更されました	4148	KLAUD_EV_OBJECTMODIFY	30 日間
監査：オブジェクトのステータスが変更されました	4150	KLAUD_EV_TASK_STATE_CHANGED	30 日間
監査：グループ設定が変更されました	4149	KLAUD_EV_ADMGROUP_CHANGED	30 日間
監査：管理サーバーから暗号化キーがインポートまたはエクスポートされました	5100	KLAUD_EV_DPEKEYSEXPORT	30 日間
監査：SIEM サーバーへの接続テストが成功しました	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 日間

ネットワークエージェントのイベント

このセクションには、ネットワークエージェントに関するイベントの情報が記載されています。

ネットワークエージェントの機能エラーイベント

次の表は、重要度が「**機能エラー**」に分類される Kaspersky Security Center ネットワークエージェントのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

ネットワークエージェントの機能エラーイベント

イベント種別の表示名	イベント種別の ID	イベント種別	説明	既定の保管期間
アップデートのインストールエラー	7702	KLNAG_EV_PATCH_INSTALL_ERROR	この種別のイベントは、Kaspersky Security Center Cloud コンソールコンポーネントの自動アップデートおよびパッチ適用に失敗した時に記録されます。このイベントは、管理対象のカスペルスキー製品のアップデートとの関連はありません。	30 日間

			イベントの説明を確認します。管理サーバーで Windows 関連の問題がこのイベントの原因となっている可能性があります。イベントの説明で Windows の設定に関する問題が言及されている場合、その問題を解決してください。	
サードパーティ製品のアップデートをインストールできませんでした	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	この種別のイベントは、脆弱性とパッチ管理とモバイルデバイス管理を使用していて、サードパーティ製品のアップデートに失敗した時に記録されます。 サードパーティ製品へのリンクが有効かどうかを確認します。イベントの説明を確認します。	30 日間
Windows Update 更新プログラムをインストールできませんでした	7717	KLNAG_EV_WUA_INSTALL_ERROR	この種別のイベントは、Windows の更新プログラムの適用に失敗した時に記録されます。ネットワークエージェントポリシーで Windows アップデートの設定を行ってください。 イベントの説明を確認します。該当するエラーに関する説明がマイクロソフト サポート技術情報で提供されていないかを検索してください。問題の解決が困難な場合は、マイクロソフトのテクニカルサポートにお問い合わせください。	30 日間

ネットワークエージェントの警告イベント

次の表は、重要度が「**警告**」に分類される Kaspersky Security Center のネットワークエージェントのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

ネットワークエージェントの警告イベント

イベント種別の表示名	イベント種別の ID	イベント種別	既定の保管期間
ソフトウェアモジュールのアップデートのインストール中に警告が発生しました	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 日間
サードパーティ製品のアップデートの	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30

インストールが警告を出力して完了しました			日間
サードパーティ製品のアップデートのインストールが延期されました	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 日間
セキュリティ問題が発生しました	549	GNRL_EV_APP_INCIDENT_OCCURED	30 日間
KSN プロキシサーバーが起動しました。KSN 可用性をチェックできませんでした	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 日間

ネットワークエージェントの情報イベント

次の表は、重要度が「**情報**」に分類される Kaspersky Security Center のネットワークエージェントのイベントを示します。

アプリケーションによって生成されるイベントごとに、製品ポリシーの［**イベントの設定**］タブで通知とストレージの設定を指定できます。すべてのイベントの通知設定を一度に設定する場合は、管理サーバーのプロパティで全般通知設定を設定してください。

ネットワークエージェントの情報イベント

イベント種別の表示名	イベント種別の ID	イベント種別	既定の保管期間
ソフトウェアモジュールのアップデートがインストールされました	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 日間
ソフトウェアモジュールのアップデートのインストールを開始しました	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 日間
アプリケーションがインストールされました	7703	KLNAG_EV_INV_APP_INSTALLED	30 日間
アプリケーションがアンインストールされました	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 日間
監視対象アプリケーションがインストールされました	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 日間
監視対象アプリケーションがアンインストールされました	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 日間
サードパーティ製品がインストールされました	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 日間
新しいデバイスが追加されました	7708	KLNAG_EV_DEVICE_ARRIVAL	30 日間
デバイスが削除されました	7709	KLNAG_EV_DEVICE_REMOVE	30 日間
デバイスが検出されました	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 日間
デバイスが認証されました	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30

			日間
Windows デスクトップ共有：ファイルが読み取られました	7712	KLUSRLOG_EV_FILE_READ	30 日間
Windows デスクトップ共有：ファイルが変更されました	7713	KLUSRLOG_EV_FILE_MODIFIED	30 日間
Windows デスクトップ共有：アプリケーションが起動しました	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 日間
Windows デスクトップ共有：開始しました	7715	KLUSRLOG_EV_WDS_BEGIN	30 日間
Windows デスクトップ共有：停止しました	7716	KLUSRLOG_EV_WDS_END	30 日間
サードパーティ製品のアップデートがインストールされました	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 日間
サードパーティ製品のアップデートのインストールを開始しました	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 日間
KSN プロキシサーバーが起動しました。KSN 可用性チェックが完了しました	7719	KSNPROXY_STARTED_CON_CHK_OK	30 日間
KSN プロキシが停止しました	7720	KSNPROXY_STOPPED	30 日間

イベントの抽出の使用

イベントの抽出は、管理サーバーのデータベース内に保存されているイベントを一定の条件を指定して抽出し、画面上に表示できる機能です。これらのイベントは、次のカテゴリに従ってグループ化されます：

- 重要度：**緊急イベント**、**機能エラー**、**警告**、**情報イベント**
- 発生時期：**最近のイベント**
- 種別：**ユーザー要求**、**監査イベント**

また、Kaspersky Security Center Cloud コンソールのインターフェイスで編集可能な設定を使用して、ユーザー定義のイベントの抽出を作成し表示できます。

Kaspersky Security Center Cloud コンソールの［**監視とレポート**］セクションで、［**イベントの抽出**］をクリックすると、イベントの抽出が表示されます。

既定では、イベントの抽出には過去 7 日の情報が含まれます。

Kaspersky Security Center Cloud コンソールには、事前定義された次の既定のイベントの抽出のセットが用意されています：

- 重要度別のイベント：
  - **緊急イベント**

- **機能エラー**
- **警告**
- **情報メッセージ**

- **ユーザー要求**（管理対象製品のイベント）
- **最近のイベント**（過去1週間を対象）
- **監査イベント**

  Kaspersky Security Center Cloud コンソールでは、ワークスペース内のサービスの動作に関連する監査イベントが表示されます。これらのイベントは、カスペルスキーの担当者の操作により調整されます。たとえば、管理サーバーポートの変更、管理サーバーデータベースのバックアップ、ユーザーアカウントの作成、変更、削除がこれらのイベントに含まれます。

ユーザー定義の抽出を追加で作成し設定できます。ユーザー定義の抽出では、イベントが発生したデバイスの属性（デバイス名、IP アドレスの範囲、管理グループ）、イベントの種別と重要度、製品名とコンポーネント名、および対象期間によってイベントをフィルターできます。検索対象に、タスクの実行結果を含めることもできます。また、1つ以上の単語を入力して検索する、シンプルな検索フィールドも使用できます。この場合、入力した単語のいずれかが、いずれかの属性（イベント名、説明、コンポーネント名など）に含まれるイベントがすべて一致対象として表示されます。

事前定義の抽出とユーザー定義の抽出の両方で、表示するイベント数と検索対象にするレコード数を制限できます。両方のオプションの値が、Kaspersky Security Center Cloud コンソールでイベントの抽出が表示されるまでの所要時間に影響します。データベースのサイズが大きいほど、プロセスの所要時間が長くなります。

次のことができます：

- イベントの抽出のプロパティの編集
- イベントの抽出の生成
- イベントの抽出の詳細の表示
- イベントの抽出の削除
- 管理サーバーのデータベースからのイベントの削除

イベントの抽出の作成

イベントの抽出を作成するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に移動します。
2. ［**追加**］をクリックします。
3. ［**新規のイベントの抽出**］ウィンドウで、新しいイベントの抽出の設定を指定します。必要に応じて、ウィンドウの各セクションでこの操作を行います。
4. ［**保存**］をクリックして変更内容を保存します。

確認ウィンドウが開きます。

5. イベントの抽出の結果を表示するには、［**抽出の結果に移動**］をオンにしたままにします。

6. ［**保存**］を選択して、イベントの抽出の作成を確定させます。

［**抽出の結果に移動**］をオンにしたままの場合、イベントの抽出結果が表示されます。オフにした場合、新しいイベントの抽出が追加されたイベントの抽出のリストが表示されます。

イベントの抽出の編集

イベントの抽出を編集するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。

2. 編集するイベントの抽出に隣接するチェックボックスをオンにします。

3. ［**プロパティ**］をクリックします。
イベントの抽出の設定ウィンドウが表示されます。

4. イベントの抽出のプロパティを編集します。

> 製品導入時から利用できる定義済みのイベントの抽出では、［**全般**］タブ（抽出の名前以外）、［**時間**］タブ、［**アクセス権**］タブのプロパティのみを編集できます。

ユーザー定義の抽出では、すべてのプロパティを編集できます。

5. ［**保存**］をクリックして変更内容を保存します。

編集したイベントの抽出がリストに表示されます。

イベントの抽出のリストの表示

イベントの抽出を表示するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。

2. 開始するイベントの抽出に隣接するチェックボックスをオンにします。

3. 次のいずれかの手順を実行します：

- イベントの抽出結果の表示で並べ替えを設定したい場合は、次の操作を実行します：

  a. ［**並べ替えを再設定して実行**］をクリックします。

  b. ［**イベントの抽出の並べ替えの再設定**］ウィンドウが表示されるので、並べ替えの設定を指定します。

c. 抽出名をクリックします。

- 管理サーバーでの並べ替え順序を変更せずにイベントのリストを表示する場合は、抽出名をクリックします。

イベントの抽出結果が表示されます。

イベントの抽出のエクスポート

Kaspersky Security Center Cloud コンソールを使用すると、イベントの抽出とその設定を KLO ファイルに保存できます。この KLO ファイルを使用して、Kaspersky Security Center Windows と Kaspersky Security Center Linux の両方に保存したイベントの抽出をインポートできます。

エクスポートできるのは、ユーザー定義のイベントの抽出のみであることに注意してください。既定の Kaspersky Security Center Cloud コンソールセットからのイベントの抽出（事前定義された抽出）は、ファイルに保存できません。

イベントの抽出をエクスポートするには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
2. エクスポートするイベントの抽出に隣接するチェックボックスをオンにします。

   複数のイベントの抽出を同時にエクスポートすることはできません。複数の抽出を選択すると、［**エクスポート**］が無効になります。
3. ［**エクスポート**］をクリックします。
4. 開いた［**名前を付けて保存**］ウィンドウで、イベントの抽出ファイル名とパスを指定し、［**保存**］をクリックします。

   ［**名前を付けて保存**］ウィンドウは、Google Chrome、Microsoft Edge、または Opera を使用している場合にのみ表示されます。別のブラウザーを使用する場合、イベントの抽出ファイルは自動的に［**Downloads**］フォルダーに保存されます。

イベントの抽出のインポート

Kaspersky Security Center Cloud コンソールを使用すると、KLO ファイルからイベントの抽出をインポートできます。KLO ファイルには、エクスポートされたイベントの抽出とその設定が含まれています。

イベントの抽出をインポートするには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
2. ［**インポート**］をクリックし、インポートするイベントの抽出ファイルを選択します。
3. 表示されたウィンドウで、KLO ファイルのパスを指定し、［**開く**］をクリックします。選択できるイベントの抽出イベントの抽出ファイルは1つだけです。

   イベントの抽出処理が開始されます。

インポート結果の通知が表示されます。イベントの抽出が正常にインポートされた場合は、［**インポートの詳細を表示**］をクリックしてイベントの抽出のプロパティを表示できます。

インポートが成功すると、イベントの抽出が抽出リストに表示されます。イベントの抽出の設定もインポートされます。

新しくインポートされたイベントの抽出と同じ名前のイベントの抽出が既に存在している場合、インポートされたイベントの抽出の名前に、たとえば **(1)**、**(2)** のようなインデックス「**(<次の連番>)**」が付きます。

イベントの詳細の表示

イベントの詳細を表示するには：

1. イベントの抽出を開始します。
2. 目的のイベントの時刻をクリックします。
   ［**イベントのプロパティ**］ウィンドウが開きます。
3. 表示されたウィンドウでは、次の操作を実行できます：
   - 選択したイベントの情報の表示
   - イベントの抽出結果の 1 つ前または 1 つ後のイベントへの移動
   - イベントが発生したデバイスの情報への移動
   - イベントが発生したデバイスが属する管理グループへの移動
   - （タスクに関係しているイベントの場合）該当タスクへの移動

イベントのファイルへのエクスポート

イベントをファイルにエクスポートするには：

1. イベントの抽出を開始します。
2. 目的のイベントに隣接するチェックボックスをオンにします。
3. ［**ファイルへのエクスポート**］をクリックします。

   選択したイベントがファイルにエクスポートされます。

イベントに含まれるオブジェクトの履歴の表示

リビジョン管理をサポートするオブジェクトの作成イベントまたは変更イベントからは、オブジェクトの履歴画面に移動することができます。

イベントからオブジェクトの履歴を表示するには：

1. イベントの抽出を開始します。
2. 目的のイベントに隣接するチェックボックスをオンにします。
3. ［**変更履歴**］をクリックします。

   オブジェクトの変更履歴が表示されます。

タスクおよびポリシーのイベントに関する情報の記録

このセクションでは、Kaspersky Security Center Cloud コンソールのデータベースに保存されているタスクとポリシーのイベント数を最小限に抑える方法に関する推奨事項について説明します。既定では、デバイス 1000 台ごとにイベントが 100,000 個あります。この制限を超えると、新しいイベントで古いイベントが上書きされます。その結果、重要なイベントが消える可能性があります。また、「**データベースのイベントの上限数を超えました。このイベントは削除されました**」という名前の管理サーバー警告イベントが発生する可能性があります。このような場合、このセクションの指示に従うことを推奨します。

その結果、イベントの分析に関連するシナリオの実施速度が向上します。また、これらの推奨事項は、緊急イベントが多数のイベントによって上書きされるリスクを軽減するのに役立ちます。

既定では、各タスクおよびポリシーのプロパティによって、タスクの実行およびポリシーの適用に関するすべてのイベントが保存されます。ただし、タスクが頻繁に（たとえば、1 週間に 2 回以上）実行される場合、イベントの数が多くなりすぎてデータベースの容量を超えてしまうことがあります。この場合、タスクの設定で 2 つのオプションのうち 1 つを選択することを推奨します：

- **タスクの進捗に関連したイベントを保存**：この場合、Kaspersky Security Center Cloud コンソールは、タスクの開始、進捗、完了（成功、警告、エラー）に関する情報のみを、タスクが実行される各デバイスから受信します。
- **タスク実行結果のみ保存**：この場合、Kaspersky Security Center Cloud コンソールは、タスクの完了（成功、警告、エラー）に関する情報のみを、タスクが実行される各デバイスから受信します。

ポリシーが多くのデバイス（たとえば 10,000 台以上）に対して定義されている場合も、イベントの数が多すぎてデータベースの容量を超えてしまうことがあります。この場合、ポリシーの設定で緊急イベントのみを選択し、その記録を有効にすることを推奨します。その他のイベントは記録を無効にします。

また、タスクまたはポリシーに関連するイベントの保存期間を短くすることもできます。既定の期間は、タスクに関連するイベントは 7 日、ポリシーに関連するイベントは 30 日です。イベントの保存期間を変更する際は、組織で運用している業務手順と、システム管理者がイベントを分析するのにかかる時間を考慮してください。

グループタスクの中間ステータスの変更に関するイベントとポリシーの適用に関するイベントが、Kaspersky Security Center Cloud コンソールデータベース内の全イベントの大部分を占めている場合は、イベントストレージの設定を変更することが推奨されます。

イベントの削除

イベントを削除するには：

1. イベントの抽出を開始します。
2. 目的のイベントの横にあるチェックボックスをオンにします。
3. ［**削除**］をクリックします。

   選択したイベントは削除され、このイベントは復元できません。

イベントの抽出の削除

削除できるのはユーザー定義のイベントの抽出のみです。製品組み込みで定義済みのイベントの抽出は削除できません。

イベントの抽出を削除するには：

1. メインメニューで、［**監視とレポート**］→［**イベントの抽出**］の順に選択します。
2. 削除するイベントの抽出に隣接するチェックボックスをオンにします。
3. ［**削除**］をクリックします。
4. 表示されたウィンドウで［**OK**］をクリックします。

   イベントの抽出が削除されます。

通知とデバイスのステータス

このセクションでは、通知の表示、通知の配信の設定、デバイスのステータスの使用、デバイスのステータス変更を有効にする方法について説明します。

通知について

Kaspersky Security Center Cloud コンソールでは、必要に応じて、重要だと考えられる任意のイベントに対して通知の送信を設定し、組織ネットワークの監視に役立てることができます。任意のイベントにメールでの通知を設定できます。

メールで通知を受け取った場合、イベント内容を確認して必要な対応を決定できます。組織のネットワークに応じて適切な対応を行ってください。

デバイスのステータスの切り替えの設定

デバイスに「*緊急*」または「*警告*」ステータスを割り当てる条件を変更できます。

デバイスのステータスの「緊急」への切り替えを有効にするには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. グループのリストが開いたら、デバイスのステータスの切り替えを設定するグループ名をクリックします。
3. プロパティウィンドウが開いたら、［**デバイスのステータス**］タブを選択します。
4. 左側のペインで、［**緊急**］を選択します。
5. 右側のペインの［**指定されている場合は「緊急」に設定**］セクションで、デバイスに［*緊急*］ステータスを割り当てる条件をオンにします。

   親ポリシーでロック状態になっていない設定のみ変更できます。

6. リスト内の条件の横にあるラジオボタンをオンにします。
7. リストの左上にある［**編集**］をクリックします。
8. 選択した条件に対して適切な値を設定します。
   すべての条件に値を設定できるわけではありません。
9. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*緊急*」ステータスが割り当てられます。

デバイスのステータスの「警告」への切り替えを有効にするには：

1. メインメニューで、［**アセット（デバイス）**］→［**グループ階層構造**］の順に選択します。
2. グループのリストが開いたら、デバイスのステータスの切り替えを設定するグループ名をクリックします。
3. プロパティウィンドウが開いたら、［**デバイスのステータス**］タブを選択します。
4. 左側のペインで、［**警告**］を選択します。
5. 右側のペインの［**指定されている場合は「警告」に設定**］セクションで、デバイスに［*警告*］ステータスを割り当てる条件をオンにします。

   親ポリシーでロック状態になっていない設定のみ変更できます。

6. リスト内の条件の横にあるラジオボタンをオンにします。
7. リストの左上にある［**編集**］をクリックします。
8. 選択した条件に対して適切な値を設定します。
   すべての条件に値を設定できるわけではありません。

9. ［**OK**］をクリックします。

指定した条件が満たされると、管理対象デバイスには「*警告*」ステータスが割り当てられます。

通知の設定

Kaspersky Security Center Cloud コンソールで発生するイベントに関するメール通知を設定できます。

Kaspersky Security Center Cloud コンソールで発生したイベントの通知の配信を設定するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
管理サーバーのプロパティウィンドウの［**全般**］タブが表示されます。
2. ［**通知**］セクションをクリックして、右側のペインでメール通知の設定を定義します：
受信者（メールアドレス）
Kaspersky Security Center Cloud コンソールが通知を送信するメールアドレス。このフィールドでは、複数のアドレスをセミコロンで区切って指定することができます。
指定できるメールアドレスは 24 個以下です。
3. ［**テストメッセージの送信**］をクリックすると、通知が正しく設定されているか確認することができます。指定したメールアドレスにテスト通知が送信されます。
4. ［**OK**］をクリックして、管理サーバーのプロパティウィンドウを閉じます。

保存した通知の配信設定は、Kaspersky Security Center Cloud コンソールで発生するすべてのイベントに適用されます。

管理サーバーの設定、ポリシーの設定、またはアプリケーションの設定で、［**イベントの設定**］で指定された設定を特定のイベントについて上書きできます。

カスペルスキーからの通知

このセクションでは、カスペルスキーからの通知の使用、設定、無効にする方法について説明します。

カスペルスキーからの通知について

カスペルスキーからの通知（［**監視とレポート**］→［**カスペルスキーからの通知**］）には、Kaspersky Security Center Cloud コンソールと、管理対象デバイスにインストールされている管理対象アプリケーションに関連する情報が提供されます。このセクションの情報は、古い通知を削除し、新しい情報を追加することで定期的にアップデートされます。

Kaspersky Security Center Cloud コンソールは、現在接続されている管理サーバーおよび管理サーバーの管理対象デバイスにインストールされているカスペルスキー製品に関連する、カスペルスキーからの通知のみ表示します。プライマリ、セカンダリ、または仮想サーバーなど管理サーバーの種別に関係なく個別に通知が表示されます。

複数の管理者が Kaspersky Security Center Cloud コンソールを使用し、異なるインターフェイスの言語を設定している場合、Kaspersky Security Center Cloud コンソールには管理者が使用している各言語でカスペルスキーからの通知が表示されます。インターフェイスの言語を変更し、コンソールからサインアウトして再びサインインすると、選択した言語のカスペルスキーの通知が自動的にセクションに追加されます。

通知には次の種別の情報が含まれます：

- セキュリティ関連告知

  お客様のネットワーク内にインストールされたカスペルスキー製品を最新かつ機能の制限がない状態に保つためのセキュリティ関連告知通知には、カスペルスキー製品の重要なアップデート、既知の脆弱性に対する修正、カスペルスキー製品の問題を修正する方法に関する情報が含まれることがあります。セキュリティ関連告知は既定で有効になっています。通知が必要ない場合は、この機能を無効にできます。

  > Kaspersky Security Center Cloud コンソールの試用モードでは、セキュリティ関連告知を無効にできません。

  お客様のネットワーク保護の設定に対応した情報を表示するために、Kaspersky Security Center Cloud コンソールはデータをカスペルスキーのクラウドサーバーに送信し、ネットワーク内にインストールされたカスペルスキー製品に関連する通知のみを受け取ります。サーバーに送信できるデータセットについては、会社のワークスペースの作成時に同意する Kaspersky Security Center Cloud コンソールの使用許諾契約書で説明されています。

- マーケティング関連告知

  マーケティング関連告知には、カスペルスキー製品に関するお得な情報やキャンペーン、カスペルスキーからのニュースなどが含まれます。マーケティング関連の告知は既定で無効になっています。この種類の告知は Kaspersky Security Network (KSN) を有効にした場合のみ受け取ります。KSN を無効にすることでマーケティング関連告知を無効にできます。

  お客様のネットワークのデバイスの保護や日々の作業に役立つ可能性のある情報のみを表示するため、Kaspersky Security Center Cloud コンソールはカスペルスキーのクラウドサーバーにデータを送信し、適切な通知を受け取ります。サーバーに送信される可能性のあるデータセットは、KSN に関する声明の処理されるデータに関する項で説明されています。

新しい情報は、重要度に基づいて次のカテゴリに分類されます：

1. 緊急の情報
2. 重要なニュース
3. 警告
4. 情報

カスペルスキーからの通知セクションに新しい情報が表示された際に、Kaspersky Security Center Cloud コンソールには通知の重要度のレベルに応じた通知ラベルが表示されます。ラベルをクリックして、［カスペルスキーからの通知］セクションで通知を表示できます。

カスペルスキーからの通知を無効にする

カスペルスキーからの通知（［**監視とレポート**］→［**カスペルスキーからの通知**］）には、Kaspersky Security Center Cloud コンソールのバージョンと、管理対象デバイスにインストールされている管理対象アプリケーションに関連する情報が提供されます。通知が必要ない場合は、この機能を無効にできます。

カスペルスキーからの通知には、セキュリティに関するものとマーケティングに関するものの 2 種類の情報があります。これらのお知らせは、種類ごとに無効にできます。

Kaspersky Security Center Cloud コンソールの試用モードでは、セキュリティ関連告知を無効にできません。

セキュリティ関連告知を無効にするには：

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**カスペルスキーからの通知**］を選択します。
3. ［**セキュリティ関連告知が［無効］です**］にします。
4. ［**保存**］をクリックします。
   カスペルスキーからの通知が無効になります。

マーケティング関連の告知は既定で無効になっています。マーケティング関連の告知は Kaspersky Security Network (KSN) を有効にした場合のみ受け取ります。KSN を無効にすることでこの種類のお知らせは無効にできます。

マーケティング関連の告知を無効にするには：

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**KSN 設定**］セクションを選択します。
3. ［**Kaspersky Security Network への参加に同意する**］を無効にします。
4. ［**保存**］をクリックします。
   マーケティング関連の告知が無効になります。

ライセンスの有効期限に関する警告の受信

Kaspersky Endpoint Security for Business Select ライセンスを管理サーバーに追加するには：

1. メインメニューで、管理サーバーの名前の横にある設定アイコン（）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。
2. ［**全般**］タブで、［**ライセンス**］セクションを選択します。
3. ［**選択**］をクリックします。
4. 表示されたウィンドウで、ライセンスを選択して［**OK**］をクリックします。

または、ライセンスが表示されない場合は、［**新しいライセンスを追加**］をクリックしてアクティベーションコードを使用できます。

ライセンスが管理サーバーのリポジトリに追加されます。これにより、ライセンスの有効期間が終了する1日前に緊急イベント［*ライセンスの有効期間がまもなく終了します*］、ライセンスの有効期間の終了後に緊急イベント［*機能が制限されています*］が管理サーバーで生成されます。必要に応じて、通知配信を設定できます。

Kaspersky Endpoint Security for Business Select ライセンスを管理サーバーのリポジトリに追加すると、1台のデバイスでライセンスが使用されていると判断されます。

Cloud Discovery

Kaspersky Security Center Cloud コンソールは、Windows を実行している管理対象デバイスでのクラウドサービスの使用を監視し、不要と思われるクラウドサービスへのアクセスをブロックできます。Cloud Discovery は、ブラウザーやデスクトップアプリケーションからこれらのサービスにアクセスしようとするユーザーの試行を追跡します。また、暗号化されていない接続（HTTP プロトコルなどを使用）経由でクラウドサービスにアクセスしようとするユーザーの試行も追跡します。この機能は、シャドー IT によるクラウドサービスの使用を検知して停止するのに役立ちます。

Cloud Discovery 機能は、Kaspersky NEXT ライセンスのいずれかを購入している場合にのみ使用できます。詳細については、ライセンスと各ライセンスの最小デバイス数を参照してください。

Cloud Discovery 機能を有効化し、機能を有効にするセキュリティポリシーまたはプロファイルを選択できます。各セキュリティポリシーまたはプロファイルで個別に機能を有効化または無効化することもできます。ユーザーにアクセスさせたくないクラウドサービスへのアクセスをブロックできます。

クラウドサービスへのアクセスをブロックできるようにするには、次の条件を満たしている必要があります。

- Kaspersky Endpoint Security 11.2 for Windows 以降を使用している。以前のバージョンのセキュリティ製品では、クラウドサービスの使用を監視することしかできませんでした。
- 不要なクラウドサービスへのアクセスをブロックする機能を提供する Kaspersky NEXT ライセンスの 1 つを購入済みである。

Cloud Discovery ウィジェットと Cloud Discovery レポートには、クラウドサービスへのアクセスの成功およびブロックされた試行に関する情報が表示されます。ウィジェットには、各クラウドサービスのリスクレベルも表示されます。Kaspersky Security Center Cloud コンソールは、機能が有効になっているセキュリティポリシーまたはプロファイルによってのみ保護されているすべての管理対象デバイスから、クラウドサービスの使用に関する情報を取得します。

ウィジェットを使用して Cloud Discovery を有効にする

Cloud Discovery 機能を使用すると、この機能が有効になっているセキュリティポリシーによってのみ保護されているすべての管理対象デバイスから、クラウドサービスの使用に関する情報を取得できます。Cloud Discovery は、Kaspersky Endpoint Security for Windows ポリシーに対してのみ有効化または無効化できます。

Cloud Discovery 機能を有効にする方法は 2 つあります。

- Cloud Discovery ウィジェットを使用する。
- Kaspersky Endpoint Security for Windows のプロパティを使用する。

  Kaspersky Endpoint Security for Windows のポリシーのプロパティで Cloud Discovery 機能を有効にする方法について詳しくは、Kaspersky Endpoint Security for Windows のヘルプの Cloud Discovery のセクションを参照してください。

Cloud Discovery 機能は、Kaspersky Endpoint Security for Windows のポリシーのパラメータでのみ無効にできることにご注意ください。

Cloud Discovery を有効にするには、［**一般機能：基本機能**］機能領域で**書き込み**権限が必要です。

Cloud Discovery ウィジェットを使用して Cloud Discovery 機能を有効にするには：

1. Kaspersky Security Center Cloud コンソールに移動します。
2. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
3. **Cloud Discovery** ウィジェットで、［**有効にする**］をクリックします。
4. 開いた［**Cloud Discovery を有効にする**］ウィンドウで、機能を有効にするセキュリティポリシーを選択し、［**有効にする**］をクリックします。
   次のポリシー設定が自動的に有効になります：**Web ページと連携するため Web トラフィック内にスクリプトを埋め込む**、**Web セッションの監視**、**暗号化された接続のスキャン**。

Cloud Discovery 機能が有効になり、ウィジェットがダッシュボードに追加されます。

Cloud Discovery ウィジェットをダッシュボードに追加する

Cloud Discovery ウィジェットをダッシュボードに追加して、管理対象デバイス上のクラウドサービスの使用を監視できます。

Cloud Discovery ウィジェットをダッシュボードに追加できるようにするには、**一般機能：基本機能**機能領域で**書き込み**権限を持っている必要があります。

Cloud Discovery ウィジェットをダッシュボードに追加するには：

1. Kaspersky Security Center Cloud コンソールに移動します。
2. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
3. ダッシュボードで、［**Web ウィジェットを追加または復元**］をクリックします。
4. 使用可能なウィジェットのリストで、山形アイコン（›）［**その他**］カテゴリの横にあります。
5. **Cloud Discovery** ウィジェットを選択し、［**追加**］をクリックします。
   Cloud Discovery 機能が無効になっている場合は、「ウィジェットを使用して Cloud Discovery を有効にする」セクションの手順に従ってください。

選択したウィジェットはダッシュボードの一番下に追加されます。

クラウドサービスの使用情報を確認する

クラウドサービスへのアクセスの試行に関する情報を示す**クラウド検出**ウィジェットを表示できます。ウィジェットには、各クラウドサービスのリスクレベルも表示されます。Kaspersky Security Center Cloud コンソールは、この機能が有効になっているセキュリティポリシーによってのみ保護されているすべての管理対象デバイスから、クラウドサービスの使用に関する情報を取得します。

表示する前に、次のことを確認してください：

- Cloud Discovery ウィジェットがダッシュボードに追加されている。
- Cloud Discovery 機能が有効になっている。
- **読み取り**権限が、［**一般的な機能：基本機能**］の機能領域で許可されている。

Cloud Discovery ウィジェットを表示するには：

1. Kaspersky Security Center Cloud コンソールに移動します。
2. メインメニューで、［**監視とレポート**］→［**ダッシュボード**］に移動します。
   Cloud Discovery ウィジェットがダッシュボードに表示されます。
3. **Cloud Discovery** ウィジェットの左側で、クラウドサービスのカテゴリを選択します。
   ウィジェットの右側のテーブルには、選択したカテゴリから、ユーザーが最も頻繁にアクセスを試行するサービスが最大 5 つ表示されます。成功した試行とブロックされた試行の両方がカウントされます。
4. ウィジェットの右側で、特定のサービスを選択します。
   以下の表には、サービスへのアクセスを最も頻繁に試行するデバイスが最大 10 個表示されます。

ウィジェットには、要求された情報が表示されます。

表示されたウィジェットでは、次の操作を実行できます：

- ［**監視とレポート**］→［**レポート**］セクションに進み、Cloud Discovery レポートを表示します。
- 選択したクラウドサービスへのアクセスをブロックまたは許可します。

Cloud Discovery 機能は、Kaspersky NEXT ライセンスのいずれかを購入している場合にのみ使用できます。詳細については、ライセンスと各ライセンスの最小デバイス数を参照してください。

クラウドサービスのリスクレベル

Cloud Discovery は、クラウドサービスごとにリスクレベルを提供します。リスクレベルは、組織のセキュリティ要件に適合しないサービスを判断するのに役立ちます。たとえば、特定のサービスへのアクセスをブロックするかどうかを決定する時に、リスクレベルを考慮することができます。

リスクレベルは推定指標であり、クラウドサービスの品質やサービス提供元に関しては言及していません。リスクレベルは、カスペルスキーのエキスパートによる推奨事項でしかありません。

クラウドサービスのリスクレベルは、Cloud Discovery ウィジェット、および監視対象のすべてのクラウドサービスのリストに表示されます。

不要なクラウドサービスへのアクセスをブロックする

ユーザーにアクセスさせたくないクラウドサービスへのアクセスをブロックできます。以前にブロックされたクラウドサービスへのアクセスを許可することもできます。

他の考慮事項の中でも、特定のサービスへのアクセスをブロックするかどうかを決定する際に、リスクレベルを考慮に入れることを推奨します。

セキュリティポリシーまたはプロファイルのクラウドサービスへのアクセスをブロックまたは許可できます。

不要なクラウドサービスへのアクセスをブロックする方法は 2 つあります。

- Cloud Discovery ウィジェットを使用する。

  この場合、サービスへのアクセスを1つずつブロックできます。

- Kaspersky Endpoint Security for Windows のプロパティを使用する。

  この場合、サービスへのアクセスを1つずつブロックすることも、カテゴリ全体をまとめてブロックすることもできます。

  Kaspersky Endpoint Security for Windows のポリシーのプロパティで Cloud Discovery 機能を有効にする方法について詳しくは、Kaspersky Endpoint Security for Windows のヘルプの Cloud Discovery のセクションを参照してください。

ウィジェットを使用してクラウドサービスへのアクセスをブロックまたは許可するには：

1. Cloud Discovery ウィジェットを開き、必要なクラウドサービスを選択します。
2. ［**サービスを使用する上位 10 デバイス**］ペインで、サービスをブロックまたは許可するセキュリティポリシーまたはプロファイルを見つけます。
3. 必要な行の［**ポリシーまたはプロファイルのアクセスステータス**］列で、次のいずれかを実行します。
   - サービスをブロックするには、ドロップダウンリストで［**ブロック**］を選択します。
   - サービスを許可するには、ドロップダウンリストで［**許可**］を選択します。
4. ［**保存**］をクリックします。

選択したサービスへのアクセスは、セキュリティポリシーまたはプロファイルに対してブロックまたは許可されています。

クライアントデバイスのリモート診断

Windows ベースと Linux ベースのクライアントデバイス上での次の操作のリモート実行についてリモート診断を使用できます：

- トレースの有効化と無効化、トレースレベルの変更、トレースファイルのダウンロード
- システム情報とアプリケーション設定のダウンロード
- イベントログのダウンロード
- アプリケーションのダンプファイルの生成
- 診断の開始および診断レポートのダウンロード
- アプリケーションの起動、停止、再起動

クライアントデバイスからダウンロードしたイベントログと診断レポートを、管理者自身による問題のトラブルシューティングに活用できます。また、テクニカルサポートにお問い合わせいただいた場合、テクニカルサポートの担当者がより詳細な分析を行うために、トレースファイル、ダンプファイル、イベントログ、診断レポートをクライアントデバイスからダウンロードするように求められる場合もあります。

リモート診断ウィンドウを開く

Windows ベースと Linux ベースのクライアントデバイスのリモート診断を実行するには、リモート診断ウィンドウを開く必要があります。

リモート診断ウィンドウを開くには：

1. リモート診断ウィンドウを開くデバイスを選択するには、次のいずれかを実行します：
   - デバイスが管理グループに属している場合は、メインメニューで、［**アセット（デバイス）**］→［**グループ**］→［**<グループ名>**］→［**管理対象デバイス**］の順に移動します。
   - デバイスが未割り当てデバイスグループに属している場合は、メインメニューで、［**検出と製品の導入**］→［**未割り当てデバイス**］の順に移動します。
2. 目的のデバイスの名前をクリックします。
3. デバイスのプロパティウィンドウが開いたら、［**詳細**］タブをクリックします。
4. 表示されたウィンドウで、［**リモート診断**］をクリックします。
   クライアントデバイスの［**リモート診断**］ウィンドウが開きます。管理サーバーとクライアントデバイス間の接続が確立されていない場合、エラーメッセージが表示されます。

あるいは、Linux ベースのクライアントデバイスに関するすべての診断情報を一度に取得する必要がある場合は、このデバイスで collect.sh スクリプトを実行できます。

アプリケーションのトレースの有効化と無効化

Xperf トレースを含む、アプリケーションのトレースを有効または無効にできます。

トレースの有効化および無効化

リモートデバイスでのトレースを有効または無効にするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。
   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。
3. アプリケーションリストで、トレースを有効または無効にするアプリケーションを選択します。
   リモート診断オプションのリストが表示されます。
4. トレースを有効にする場合：
   a. ［**トレース**］セクションで［**トレースを有効化**］をクリックします。
   b. ［**トレースレベルを変更**］ウィンドウで表示される設定の既定値は変更しないことを推奨します。設定値の編集が必要な場合は、テクニカルサポート担当者が必要な変更をご案内します。次の設定を使用できます：
      - **トレースレベル**
        トレースレベルでは、トレースファイルに含める情報の詳細度を指定できます。
      - **ローテーションありトレース**
        トレース情報を上書きし、トレースファイルのサイズが過剰に大きくなるの防止します。トレース情報を保存するために使用できるファイルの最大数と、各ファイルの最大サイズを指定します。トレースファイルの数が指定した最大数と同じになり、書き込み中のファイルのサイズが指定した最大サイズに達すると、新しいトレースファイルを作成できるように最も古いトレースファイルが削除されます。

        ローテーションありトレースは、Kaspersky Endpoint Security でのみ使用可能です。

   c. ［**保存**］をクリックします。

   選択したアプリケーションのトレースが有効になります。場合によっては、トレースを有効にするには、セキュリティ製品とタスクを再起動しなければならないことがあります。

   Linux ベースのクライアントデバイスでは、Kaspersky Security Agent コンポーネントのアップデーターのトレースは、ネットワークエージェント設定によって規制されます。したがって、Linux を実行しているクライアントデバイスでは、このコンポーネントに対して［**トレースを有効化**］および［**トレースレベルを変更**］がオフになっています。
5. 選択したアプリケーションのトレースを無効にする場合は、［**トレースを無効化**］をクリックします。
   選択したアプリケーションのトレースが無効になります。

Xperf トレースの有効化

Kaspersky Endpoint Security では、テクニカルサポート担当者がシステムのパフォーマンス情報の Xperf トレースを有効にするようにお願いする場合があります。

Xperf トレースを有効にして設定するか、無効にするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。

   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。
3. アプリケーションのリストから Kaspersky Endpoint Security for Windows を選択します。

   Kaspersky Endpoint Security for Windows のリモート診断オプションのリストが表示されます。
4. ［**Xperf トレース**］セクションで［**Xperf トレースを有効化**］をクリックします。

   Xperf トレースが既に有効になっている場合、［**Xperf トレースを無効化**］が代わりに表示されます。Kaspersky Endpoint Security for Windows の Xperf トレースを無効にする場合は、このボタンをクリックしてください。
5. ［**Xperf トレースのレベルを変更**］ウィンドウが開くので、テクニカルサポート担当者からの依頼内容に応じて、次の操作を実行してください：

   a. 次のいずれかのトレースレベルを選択します：

   - **低レベル**

     この種別のトレースファイルには、システムに関する最小限の量の情報が含まれています。

     既定では、このオプションがオンです。

   - **高レベル**

     この種別のトレースファイルには*低レベル*のトレースファイルより詳細な情報が含まれています。*低レベル*のトレースファイルではパフォーマンスを十分に評価できない場合などに、テクニカルサポートの担当者から提出を求められることがあります。*高レベル*のトレースファイルには、ハードウェア、オペレーティングシステム、プロセスとアプリケーションの開始と終了のリスト、パフォーマンスの評価に使用されたイベント、Windows システム評価ツールからのイベントなどに関する情報を含む技術情報が含まれます。

   b. 次のいずれかの Xperf トレース種別を選択します：

   - **基本**

     Kaspersky Endpoint Security の動作中にトレース情報が取得されます。

     既定では、このオプションがオンです。

   - **再起動時**

     管理対象デバイスでのオペレーティングシステムの起動時にトレース情報を受信します。このトレース種別は、デバイスが起動してから Kaspersky Endpoint Security が起動するまでの間にシステムパフォーマンスに影響を与える問題が発生している場合に使用すると効果的です。

［**ローテーションファイルのサイズ（MB）**］を有効にし、トレースファイルのサイズが過剰に大きくなるのを防止するように依頼される場合もあります。続いて、トレースファイルの最大サイズを設定します。ファイルが指定した最大サイズに達すると、最も古いトレース情報が削除され、新しい情報が上書きされます。

c. ローテーションするファイルサイズを定義します。

d. ［**保存**］をクリックします。

Xperf トレースが有効になり設定されます。

6. Kaspersky Endpoint Security for Windows の Xperf トレースを無効にする場合は、［**Xperf トレース**］セクションの［**Xperf トレースを無効化**］をクリックしてください。

Xperf トレースが無効になります。

アプリケーションのトレースファイルのダウンロード

デバイスの設定で［**管理サーバーから切断しない**］がオンになっているか、プッシュサーバーまたは接続ゲートウェイが使用中であるかのいずれかに合致した場合のみ、クライアントデバイスからトレースファイルをダウンロードできます。いずれの条件も満たさない場合は、ダウンロードできません。

［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

アプリケーションのトレースファイルをダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。

［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。

3. アプリケーションのリストで、トレースファイルをダウンロードするアプリケーションを選択します。
4. ［**トレース**］セクションで、［**トレースファイル**］をクリックします。

トレースファイルのリストが表示された［**デバイスのトレースログ**］ウィンドウが開きます。

5. ダウンロードするファイルをトレースファイルのリストから選択します。
6. 次のいずれかの手順を実行します：

- ［**ダウンロード**］をクリックして、選択したファイルをダウンロードします。ダウンロードするファイルを 1 つまたは複数選択できます。
- 選択したファイルの一部をダウンロード：

a. ［**一部をダウンロード**］をクリックします。

複数のファイルの一部を同時にダウンロードすることはできません。複数のトレースファイルを選択すると、［**一部をダウンロード**］がオフになります。

b. ウィンドウが開いたら、名前を指定し、必要に応じてダウンロードするファイルの部分を指定します。

Linux ベースのデバイスの場合、ファイル部分名の編集は使用できません。

c. ［**ダウンロード**］をクリックします。

選択したファイル、またはその一部が指定の場所にダウンロードされます。

トレースファイルの削除

不要になったトレースファイルを削除することができます。

トレースファイルを削除するには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. 表示された［モート診断］ウィンドウで、［**イベントログ**］タブを選択します。
3. ［**トレースファイル**］セクションで、削除するトレースファイルに応じて［**Windows Update ログ**］または［**リモートインストールログ**］をクリックします。
   トレースファイルのリストが表示された［**デバイスのトレースログ**］ウィンドウが開きます。
4. 削除するファイルをトレースファイルのリストから1つまたは複数選択します。
5. ［**削除**］をクリックします。

選択したトレースファイルが削除されます。

アプリケーション設定のダウンロード

デバイスの設定で［**管理サーバーから切断しない**］がオンになっているか、プッシュサーバーまたは接続ゲートウェイが使用中であるかのいずれかに合致した場合のみ、クライアントデバイスからアプリケーション設定をダウンロードできます。いずれの条件も満たさない場合は、ダウンロードできません。

［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

クライアントデバイスからアプリケーション設定をダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［ **カスペルスキー製品**］タブを選択します。
3. ［**アプリケーション設定**］セクションで［**ダウンロード**］をクリックして、クライアントデバイスにインストールされたアプリケーションの設定に関する情報をダウンロードします。

情報を含む ZIP アーカイブが指定された場所にダウンロードされます。

クライアントデバイスからシステム情報のダウンロード

デバイスの設定で［**管理サーバーから切断しない**］がオンになっているか、プッシュサーバーまたは接続ゲートウェイが使用中であるかのいずれかに合致した場合のみ、クライアントデバイスから自分のデバイスにシステム情報をダウンロードできます。いずれの条件も満たさない場合は、ダウンロードできません。

［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

クライアントデバイスからアプリケーション設定をダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. ［リモート診断］ウィンドウで［**システム情報**］タブを選択します。
3. ［**ダウンロード**］をクリックして、クライアントデバイスに関するシステム情報をダウンロードします。

情報を含むファイルが指定された場所にダウンロードされます。

イベントログのダウンロード

デバイスの設定で［**管理サーバーから切断しない**］がオンになっているか、プッシュサーバーまたは接続ゲートウェイが使用中であるかのいずれかに合致した場合のみ、クライアントデバイスから自分のデバイスにイベントログをダウンロードできます。いずれの条件も満たさない場合は、ダウンロードできません。

［**管理サーバーから切断しない**］をオンにできるデバイスの合計数の上限は 300 です。

リモートデバイスからイベントログをダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. ［リモート診断］ウィンドウの［**イベントログ**］タブで、［**全デバイスのログ**］をクリックします。
3. ［**全デバイスのログ**］ウィンドウで、関連するログを 1 つまたは複数選択します。
4. 次のいずれかの手順を実行します：

   - ［**ファイル全体をダウンロード**］をクリックして、選択したログをダウンロードします。
   - 選択したログの一部をダウンロード：

     a. ［**一部をダウンロード**］をクリックします。
     複数のログの一部を同時にダウンロードすることはできません。複数のイベントログを選択すると、［**一部をダウンロード**］がオフになります。

     b. ウィンドウが開いたら、名前を指定し、必要に応じてダウンロードするログの部分を指定します。

     c. ［**ダウンロード**］をクリックします。

選択したイベントログ、またはその一部が指定の場所にダウンロードされます。

アプリケーションの起動、停止、再起動

クライアントデバイス上でアプリケーションを起動、停止、再起動することができます。

アプリケーションを起動、停止、再起動するには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。
2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。

［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。

3. アプリケーションのリストで、起動、停止、または再起動するアプリケーションを選択します。

4. 次のいずれかのボタンをクリックして処理を選択します：

- **アプリケーションの停止**
  アプリケーションが現在実行されていないと、このボタンは使用できません。
- **アプリケーションの再開**
  アプリケーションが現在実行されていないと、このボタンは使用できません。
- **アプリケーションの開始**
  アプリケーションの実行が現在停止されていないと、このボタンは使用できません。

選択した処理に応じて、必要なアプリケーションがクライアントデバイス上で起動、停止、再起動します。

ネットワークエージェントを再起動すると、デバイスと管理サーバーとの現在の接続が失われることを伝えるメッセージが表示されます。

アプリケーションのリモート診断の実行と結果のダウンロード

リモートデバイスでアプリケーションの診断を開始して、結果をダウンロードするには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。

2. リモート診断ウィンドウで［**カスペルスキー製品**］タブを選択します。
   ［**アプリケーションの管理**］セクションに、デバイスにインストールされているカスペルスキー製品のリストが表示されます。

3. アプリケーションのリストで、リモート診断を実行するアプリケーションを選択します。
   リモート診断オプションのリストが表示されます。

4. ［**診断レポート**］セクションで［**診断を実行**］をクリックします。
   リモート診断が開始され、診断レポートが生成されます。診断が完了すると、［**診断レポートをダウンロード**］が使用可能になります。

5. ［**診断レポートをダウンロード**］をクリックしてレポートをダウンロードします。

レポートが指定した場所にダウンロードされます。

クライアントデバイスでのアプリケーションの実行

場合によっては、テクニカルサポートの担当者の指示に従って、クライアントデバイス上でアプリケーションを実行する必要があります。そのデバイスにアプリケーションをインストールする必要はありません。そのデバイスにアプリケーションをインストールする必要はありません。

クライアントデバイス上でアプリケーションを実行するには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。

2. ［リモート診断］ウィンドウで［**リモートでアプリケーションを実行**］タブを選択します。

3. ［**アプリケーションファイル**］セクションで、［**参照**］をクリックして、クライアントデバイス上で実行するアプリケーションを含む ZIP アーカイブを選択します。

   ZIP アーカイブにはユーティリテフォルダーが含まれている必要があります。このフォルダーには、リモートデバイスで実行する実行ファイルが含まれています。

   必要に応じて、実行ファイル名とコマンドラインの引数を指定できます。これを行うには、**リモートデバイス上で実行されるアーカイブ内の実行ファイル**と［**コマンドラインの引数**］フィールドに入力します。

4. ［**アップロードして実行**］をクリックして、クライアントデバイス上で指定したアプリケーションを実行します。

5. カスペルスキーのサポート担当者の指示に従ってください。

アプリケーションのダンプファイルの生成

アプリケーションダンプファイルを使用すると、ある時点でクライアントデバイスで実行されているアプリケーションのパラメータを表示できます。このファイルには、アプリケーション用にロードされたモジュールに関する情報も含まれています。

ダンプファイルの生成は、Windows ベースのクライアントデバイスで実行されている 32 ビットプロセスでのみ使用可能です。Linux を実行しているクライアントデバイスおよび 64 ビットプロセスの場合、この機能はサポートされていません。

アプリケーションのダンプファイルを生成するには：

1. クライアントデバイスのリモート診断ウィンドウを開きます。

2. ［リモート診断］ウィンドウで［**リモートでアプリケーションを実行**］タブをクリックして選択します。

3. ［**ダンプファイルの生成**］セクションで、ダンプファイルを生成するアプリケーションの実行ファイルを指定します。

4. ［**ダウンロード**］をクリックして、指定したアプリケーションのダンプファイルを保存します。

   指定したアプリケーションがクライアントデバイスで実行されていない場合、エラーメッセージが表示されます。

Linux ベースのクライアントデバイスでのリモート診断の実行

Kaspersky Security Center Cloud コンソールを使用すると、クライアントデバイスから基本的な診断情報をダウンロードできます。あるいは、カスペルスキーの collect.sh スクリプトを使用して、Linux ベースのデバイスに関する診断情報を取得することもできます。このスクリプトは、診断が必要な Linux ベースのクライアントデバイス上で実行され、診断情報、このデバイスのシステム情報、アプリケーションのトレースファイル、デバイスログ、および緊急終了したアプリケーションのダンプファイルを含むファイルを生成します。

collect.sh スクリプトを使用して、Linux ベースのクライアントデバイスに関するすべての診断情報を一度に取得することを推奨します。Kaspersky Security Center Cloud コンソールを通じて診断情報をリモートでダウンロードする場合は、リモート診断インターフェイスのすべてのセクションを実行する必要があります。また、Linux ベースのデバイスの診断情報は完全には取得されない可能性があります。

生成された診断情報を含むファイルをカスペルスキーテクニカルサポートに送信する必要がある場合は、ファイルを送信する前にすべての機密情報を削除してください。

collect.sh スクリプトを使用して Linux ベースのクライアントデバイスから診断情報をダウンロードするには、次の手順を実行します：

1. collect.sh スクリプトをダウンロードする アーカイブ collect.tar.gz に含まれています。
2. ダウンロードしたアーカイブを、診断する必要がある Linux ベースのクライアントデバイスにコピーします。
3. 次のコマンドを実行して、アーカイブ collect.tar.gz を解凍します：

   ```
   # tar -xzf collect.tar.gz
   ```

4. 次のコマンドを実行して、スクリプトの実行権限を指定します：

   ```
   # chmod +x collect.sh
   ```

5. 管理者権限を持つアカウントを使用して、collect.sh スクリプトを実行します：

   ```
   # ./collect.sh
   ```

診断情報を含むファイルが生成され、フォルダー /tmp/$HOST_NAME-collect.tar.gz に保存されます。

SIEM システムへのイベントのエクスポート

このセクションでは、SIEM システムへのイベントのエクスポートの設定について説明します。

シナリオ：SIEM システムへのイベントのエクスポートの設定

このセクションでは、管理サーバーから外部 SIEM システムにイベントをエクスポートする手順について説明します。イベントに関する情報を外部 SIEM システムにエクスポートすると、SIEM システムの管理者は、管理対象デバイスまたはデバイスのグループで発生したセキュリティシステムイベントに迅速に対処できます。

必須条件

Kaspersky Security Center Cloud コンソールでイベントのエクスポートの設定を開始する前に：

- イベントのエクスポート方法の詳細を参照してください。
- システムの設定値を確認してください。

このシナリオのステップは、任意の順序で実行できます。

実行するステップ

イベントを SIEM システムにエクスポートするプロセスは、次の段階で構成されます：

- **Kaspersky Security Center Cloud コンソールからイベントを受信するように SIEM システムを設定する**

  SIEM システムで Kaspersky Security Center Cloud コンソールからイベントを受信するように設定する必要があります。

- **エクスポートするイベントをマーキングする**

  SIEM システムにどのイベントをエクスポートするかをマーキングする必要があります。最初に、すべてのカスペルスキー製品で発生する一般的なイベントをマークします。続けて、 特定のカスペルスキー製品で発生するイベントをマークすることもできます。

- **イベントを SIEM システムにエクスポートするための Kaspersky Security Center Cloud コンソールの設定**

  SIEM システムへのイベントのエクスポートを開始するように、Kaspersky Security Center Cloud コンソールを設定する必要があります。

結果

エクスポートするイベントを選択した場合、SIEM システムへのイベントのエクスポートの設定後にエクスポート結果を表示できます。

事前準備

Kaspersky Security Center Cloud コンソールでイベントの自動エクスポートを設定する場合は、SIEM システム設定の一部を指定する必要があります。Kaspersky Security Center Cloud コンソールの設定を準備できるように、SIEM システムの設定を事前に確認しておいてください。

SIEM システムへのイベントの自動送信を正しく設定するには、次の設定の値を把握する必要があります：

- **SIEM システムサーバーアドレス**

  現在使用している SIEM システムがインストールされているサーバーの IP アドレスです。SIEM システム設定でこの値を確認してください。

- **SIEM システムサーバーのポート**

  Kaspersky Security Center Cloud コンソールと SIEM システムサーバー間の接続を確立するために使用するポート番号。Kaspersky Security Center Cloud コンソールの設定と SIEM システムのレシーバ設定でこの値を指定します。

- **プロトコル**

  Kaspersky Security Center Cloud コンソールから SIEM システムへのメッセージの送信に使われるプロトコル。Kaspersky Security Center Cloud コンソールの設定と SIEM システムのレシーバ設定でこの値を指定します。

イベントのエクスポートについて

Kaspersky Security Center Cloud コンソールでは、管理サーバーと管理対象デバイスにインストールされた他のカスペルスキー製品の動作中に発生したイベントの情報を受信できます。イベントに関する情報は管理サーバーデータベースに保存されます。

イベントのエクスポートは、組織および技術レベルでセキュリティ問題に対処し、セキュリティ監視サービスを提供し、各種ソリューションからの情報を統合できる、一元化されたシステム内で使用できます。これらは SIEM システムで、ネットワークのハードウェアとアプリケーション、またはセキュリティオペレーションセンター（SOC）によって生成されたセキュリティアラートとイベントをリアルタイムで分析します。

これらのシステムは、ネットワーク、セキュリティ、サーバー、データベース、アプリケーションなど多くのソースからのデータを受信します。SIEM システムは、重要なイベントを見逃すことがないように、監視対象データを統合する機能も提供します。さらに、緊急のセキュリティ問題を管理者に通知するために、相互に関連するイベントとアラートの分析を自動的に実行します。アラートはダッシュボードから発することも、メールなどのサードパーティのチャネルから送信することもできます。

Kaspersky Security Center Cloud コンソールから外部 SIEM システムにイベントをエクスポートするプロセスには、イベントの送信元である Kaspersky Security Center Cloud コンソールとイベントのレシーバである SIEM システムの 2 つが関係します。イベントを正常にエクスポートするには、SIEM システムと Kaspersky Security Center Cloud コンソールの両方で設定する必要があります。どちらを先に設定してもかまいません。Kaspersky Security Center Cloud コンソールからのイベントの送信を設定してから、SIEM システムによるイベントの受信を設定するか、逆の順序でこれらの設定を行うこともできます。

イベントのエクスポートの Syslog 形式

Syslog 形式のイベントを任意の SIEM システムに送信できます。Syslog 形式を使用すると、管理サーバーおよび管理対象デバイスにインストールされたカスペルスキー製品で発生したイベントをすべてリレーできます。Syslog 形式でイベントをエクスポートする場合は、SIEM システムにリレーするイベントの種別を正確に選択できます。

SIEM システムによるイベントの受信

SIEM システムは、Kaspersky Security Center Cloud コンソールからイベントを受信して適切に解析する必要があります。これらの目的に対応できるように、SIEM システムを適切に設定する必要があります。設定は、利用する具体的な SIEM システムによります。ただし、レシーバとパーサーの設定など、すべての SIEM システムの設定で一般的なステップがいくつかあります。

SIEM システムでのイベントのエクスポートの設定

Kaspersky Security Center Cloud コンソールから外部 SIEM システムにイベントをエクスポートするプロセスには、イベントの送信元である Kaspersky Security Center Cloud コンソールとイベントのレシーバである SIEM システムの 2 つが関係します。イベントのエクスポートは、SIEM システムと Kaspersky Security Center Cloud コンソールの両方で設定する必要があります。

SIEM システムで指定する設定は、使用している個々のシステムにより異なります。一般に、すべての SIEM システムでレシーバを設定する必要があり、受信イベントを解析するためのメッセージパーサーを任意で設定します。

レシーバの設定

Kaspersky Security Center Cloud コンソールから送信されたイベントを受信するには、SIEM システムでレシーバを設定する必要があります。一般に、SIEM システムで次の設定を指定する必要があります：

- **ポート**

  Kaspersky Security Center Cloud コンソールに接続するためのポート番号を指定します。このポートは、SIEM システムとの設定時に Kaspersky Security Center Cloud コンソールで指定するポートと同じである必要があります。

- **メッセージのプロトコルまたはソースの種別**

  Syslog 形式を指定します。

使用する SIEM システムによっては、レシーバ設定をさらにいくつか指定する必要があります。

メッセージパーサー

エクスポートされたイベントはメッセージとして SIEM システムに渡されます。SIEM システムでイベントに関する情報が利用できるように、これらのメッセージを適切に解析する必要があります。メッセージパーサーは SIEM システムの一部です。イベントの ID、重大度、説明、パラメータなど関連フィールドにメッセージの内容を分けるために使用します。メッセージの内容を分けることで、SIEM システムは Kaspersky Security Center Cloud コンソールから受信したイベントを処理して、SIEM システムデータベースに保管することができます。

Syslog 形式で SIEM システムにエクスポートするイベントのマーキング

このセクションでは、SIEM システムに Syslog 形式でエクスポートするイベントをマークする方法について説明します。

Syslog 形式で SIEM システムにエクスポートするイベントのマーキングについて

イベントの自動エクスポートを有効にしたら、外部 SIEM システムにエクスポートするイベントをマーキングする必要があります。

次の条件のいずれかに基づいて、外部システムへの Syslog 形式でのイベントのエクスポートを設定できます：

- 一般的なイベントのマーキング。イベントの設定または管理サーバーの設定でエクスポートするイベントをポリシー内でマークすると、特定のポリシーで管理されているすべてのアプリケーションで発生した選択済みのイベントが SIEM システムに送信されます。エクスポートされたイベントがポリシー内で選択されている場合、このポリシーで管理されている個別アプリケーションの当該イベントを再定義することはできません。

- 管理対象アプリケーションのイベントのマーキング。管理対象デバイスにインストールされた管理対象アプリケーションへエクスポートするイベントをマークすると、そのアプリケーションで発生したイベントのみが SIEM システムに送信されます。

Syslog 形式でエクスポートするカスペルスキー製品のイベントのマーキング

管理対象デバイスにインストールされた特定の管理対象アプリケーションで発生したイベントをエクスポートする場合は、エクスポートするイベントをそのアプリケーションのポリシーでマークします。この場合、マークされたイベントが、ポリシーの範囲に含まれるすべてのデバイスからエクスポートされます。

特定の管理対象アプリケーションからエクスポートするイベントをマークするには：

1. メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動します。
2. イベントをマークするアプリケーションのポリシーをクリックします。
   ポリシーの設定ウィンドウが表示されます。
3. ［**イベントの設定**］セクションに移動します。
4. SIEM にエクスポートするイベントに隣接するチェックボックスをオンにします。
5. ［**Syslog を使用しての SIEM システムへのエクスポート用にマークする**］をクリックします。

   SIEM システムにエクスポートするイベントは、イベントのリンクをクリックして開く［**イベント登録**］セクションでマーキングすることもできます。

6. チェックマーク（⌄）がイベントまたは SIEM システムにエクスポートするためにマーキングしたイベントの［**Syslog**］列に表示されます。
7. ［**保存**］をクリックします。

管理対象アプリケーションからマークされたイベントを、SIEM システムへエクスポーされる準備ができています。

特定の管理デバイスのために、SIEM システムへエクスポートするイベントをマークできます。以前エクスポートしたイベントがアプリケーションのポリシーでマークされた場合、管理対象デバイスのためにマークされたイベントを再定義することはできません。

管理対象デバイスにエクスポートするイベントをマークするには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
   管理対象デバイスのリストが表示されます。
2. 管理対象デバイスのリストで、必要なデバイスの名前のリンクをクリックします。
   選択したデバイスのプロパティウィンドウが表示されます。
3. ［**アプリケーション**］セクションに移動します。
4. アプリケーションのリストで、必要なアプリケーションの名前のリンクをクリックします。
5. ［**イベントの設定**］セクションに移動します。
6. SIEM にエクスポートするレイベントに隣接するチェックボックスをオンにします。
7. ［**Syslog を使用しての SIEM システムへのエクスポート用にマークする**］をクリックします。

   SIEM システムにエクスポートするイベントは、イベントのリンクをクリックして開く［**イベント登録**］セクションでマークすることもできます。

8. チェックマーク（✓）がイベントまたは SIEM システムにエクスポートするためにマーキングしたイベントの［**Syslog**］列に表示されます。

これで、SIEM システムへのエクスポートが設定済みの場合は、マーキングされたイベントが管理サーバーから SIEM システムへ送信されるようになりました。

Syslog 形式でエクスポートする一般的なイベントのマーキング

Syslog 形式を使用して、管理サーバーが SIEM システムにエクスポートする一般的なイベントをマーキングすることができます。

SIEM システムにエクスポートする一般的なイベントをマークするには：

1. 次のいずれかの手順を実行します：
   - メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（）をクリックします。
   - メインメニューで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に移動し、ポリシーのリンクをクリックします。
2. 表示されたウィンドウで、［**イベントの設定**］タブを選択します。
3. ［**Syslog を使用しての SIEM システムへのエクスポート用にマークする**］をクリックします。

SIEM システムにエクスポートするイベントは、イベントのリンクをクリックして開く［**イベント登録**］セクションでマーキングすることもできます。

4. チェックマーク（✓）がイベントまたは SIEM システムにエクスポートするためにマーキングしたイベントの［**Syslog**］列に表示されます。

これで、SIEM システムへのエクスポートが設定済みの場合は、マーキングされたイベントが管理サーバーから SIEM システムへ送信されるようになりました。

Syslog 形式を使用したイベントのエクスポートについて

Syslog 形式を使用すると、管理サーバー、管理対象デバイスにインストールされた他のカスペルスキー製品で発生したイベントを SIEM システムにエクスポートできます。

Syslog は標準メッセージロギングプロトコルです。メッセージを生成するソフトウェア、メッセージを保管するシステム、メッセージを報告、分析するソフトウェアを分けることができます。各メッセージには、メッセージを生成したソフトウェアの種別を示す機能コードのラベルが付けられ、重要度が割り当てられます。

Syslog 形式は、インターネット技術タスクフォース（インターネット標準）によって公開されている RFC（Request for Comments）の文書で定義されています。Kaspersky Security Center Cloud コンソールから外部システムへのイベントのエクスポートには、RFC 5424 標準が使用されます。

Kaspersky Security Center Cloud コンソールで、Syslog 形式を使用して外部システムにイベントがエクスポートされるように設定できます。

エクスポートのプロセスは次の 2 つのステップで構成されます：

1. イベントの自動エクスポートの有効化。このステップでは、イベントを SIEM システムに送信するように Kaspersky Security Center Cloud コンソールを設定します。自動エクスポートを有効にすると、Kaspersky Security Center Cloud コンソールは即座にイベントの送信を開始します。

2. 外部システムにエクスポートするイベントの選択。このステップでは、SIEM システムにエクスポートするイベントを選択します。

イベントを SIEM システムにエクスポートするための Kaspersky Security Center Cloud コンソールの設定

SIEM システムにイベントをエクスポートするには、Kaspersky Security Center Cloud コンソールでエクスポートのプロセスを設定する必要があります。

Kaspersky Security Center Cloud コンソールで SIEM システムへのエクスポートを設定するには：

1. メインメニューで、目的の管理サーバーの名前の横にある設定アイコン（  ）をクリックします。
   管理サーバーのプロパティウィンドウが開きます。

2. ［**全般**］タブで、［**SIEM**］セクションを選択します。

3. ［**設定**］をクリックします。
   ［**エクスポート設定**］セクションが開きます。

4. ［**エクスポート設定**］セクションで設定を指定します：

- **SIEM システムサーバーアドレス**

  現在使用している SIEM システムがインストールされているサーバーの IP アドレスです。SIEM システム設定でこの値を確認してください。

- **SIEM システムのポート**

  Kaspersky Security Center Cloud コンソールと SIEM システムサーバー間の接続を確立するために使用するポート番号。Kaspersky Security Center Cloud コンソールの設定と SIEM システムのレシーバ設定でこの値を指定します。

- **プロトコル**

SIEM システムへのメッセージの送信には、TLS over TCP プロトコルのみ使用できます。そのためには、TLS 設定を指定します：

- **サーバー認証**

  ［**サーバー認証**］フィールドでは、**信頼する証明書**または **SHA フィンガープリント**を選択できます：

  - **信頼できる証明書**：信頼できる証明書認証局（CA）から証明書のリストを含むファイルを受け取り、ファイルを Kaspersky Security Center Cloud コンソールにアップロードできます。Kaspersky Security Center Cloud コンソールは、SIEM システムサーバーの証明書も信頼できる CA によって署名されているかどうかを確認します。

    信頼できる証明書を追加するには、［**CA 証明書を参照**］をクリックして、証明書をアップロードします。

  - **SHA フィンガープリント**：SIEM システム証明書の SHA-1 サムプリントを Kaspersky Security Center Cloud コンソールに指定できます。SHA-1 サムプリントを追加するには、［**サムプリント**］フィールドでサムプリントを入力し、［**追加**］をクリックします。

  ［**クライアント認証を追加する**］を使用して、Kaspersky Security Center Cloud コンソールを認証する証明書を生成することができます。このようにして、Kaspersky Security Center Cloud コンソールが発行した自己署名証明書を使用します。この場合、SIEM システムサーバーの認証に、信頼できる証明書と SHA フィンガープリントの両方を使用することができます。

- **サブジェクト名 / サブジェクト代替名を追加する**

  サブジェクト名は、証明書を受け取るドメインの名前です。SIEM システムサーバーのドメイン名が SIEM システムサーバー証明書のサブジェクト名と一致しない場合、Kaspersky Security Center Cloud コンソールは SIEM システムサーバーに接続できません。しかし、SIEM システムサーバーは証明書内で名前が変更された場合にドメイン名を変更することがあります。この場合、サブジェクト名を［**サブジェクト名 / サブジェクト代替名を追加する**］で指定することができます。指定されたサブジェクト名のいずれかが SIEM システム証明書のサブジェクト名と一致する場合、Kaspersky Security Center Cloud コンソールは SIEM システムサーバー証明書を検証します。

- **クライアント認証を追加する**

  クライアント認証用に、自身の証明書を挿入するか、Kaspersky Security Center Cloud コンソールで生成することができます。

  - **証明書を挿入する**:CA など、任意の発行元から受け取った証明書を使用できます。次のいずれかの証明書タイプを使用して、証明書とその秘密鍵を指定する必要があります：

    - **X.509 証明書 PEM**：［**証明書のファイル**］フィールドに証明書のファイルをアップロードし、［**鍵のファイル**］フィールドに秘密鍵のファイルをアップロードします。両方のファイルは相互に依存せず、ファイルを読み込む順序は重要ではありません。両方のファイルがアップロードされたら、秘密鍵をデコードするためのパスワードを［**パスワードまたは証明書の検証**］で指定します。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

    - **X.509 証明書 PKCS12**：証明書と秘密鍵を含む単一のファイルを［**証明書のファイル**］フィールドにアップロードします。ファイルをアップロードしたら、秘密鍵をデコードするためのパスワードを［**パスワードまたは証明書の検証**］で指定します。秘密鍵がエンコードされていない場合、パスワードの値は空である可能性があります。

- **鍵を生成する**：Kaspersky Security Center Cloud コンソールで自己署名証明書を生成できます。Kaspersky Security Center Cloud コンソールは生成された自己署名証明書を保存し、証明書の公開部分または SHA-1 フィンガープリントを SIEM システムに渡すことができます。

5. 必要に応じて、管理サーバーデータベースからアーカイブイベントをエクスポートし、アーカイブイベントのエクスポートを開始する日付を設定できます：

   a. ［**エクスポートの開始日を設定**］をクリックします。

   b. 表示されたセクションの［**エクスポートの開始日**］に、開始日を指定します。

   c. ［**OK**］をクリックします。

6. オプションを［**SIEM システムデータースへのイベントの自動エクスポートが［有効］です**］に切り替えます。

7. SIEM システム接続が正常に設定されていることを確認するには、［**接続の確認**］をクリックします。

   接続のステータスが表示されます。

8. ［**保存**］をクリックします。

SIEM システムへのエクスポートが設定されました。これで、イベントの受信を SIEM システムで設定した場合は、マーキングされたイベントが管理サーバーから SIEM システムにエクスポートされます。エクスポートの開始日を設定した場合、管理サーバーは指定された日付からも管理サーバーデータベース内のマーキングされたイベントをエクスポートします。

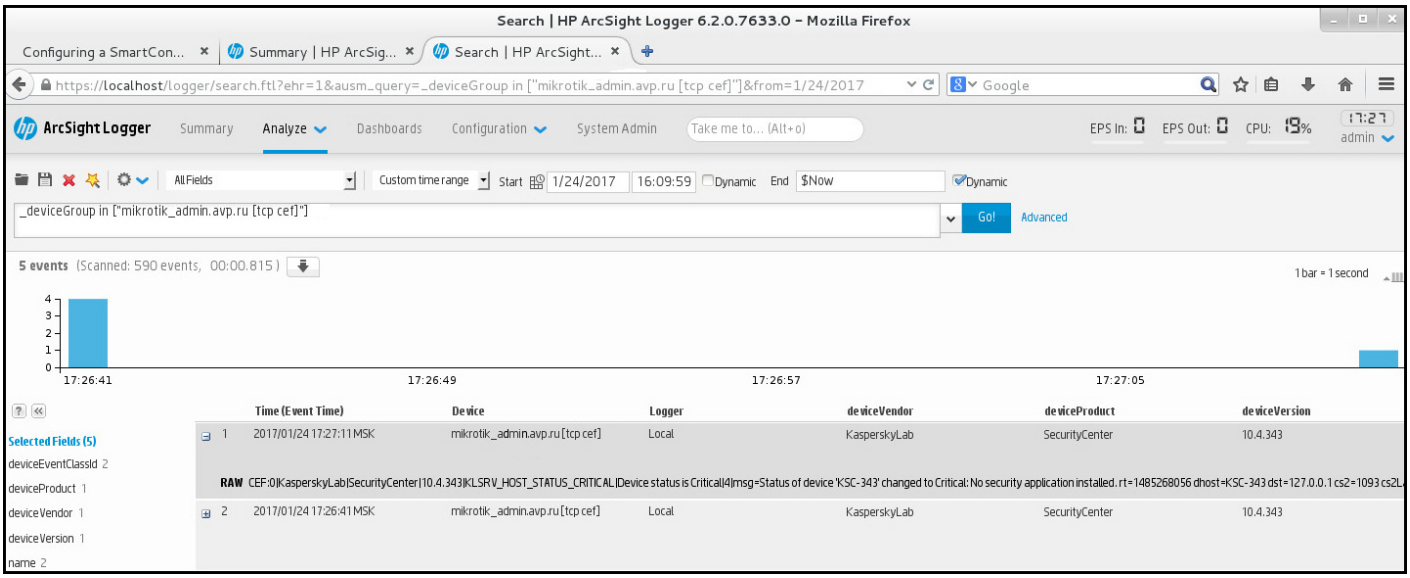
エクスポート結果の表示

イベントのエクスポート手順が正常に完了するようにコントロールすることができます。それには、イベントのエクスポートとともにメッセージが SIEM システムで受信されているかどうかを確認します。

Kaspersky Security Center Cloud コンソールから送信されたイベントが SIEM システムで受信され、適切に解析されている場合、設定は両者で適切に行われています。イベントが受信されない場合は、Kaspersky Security Center Cloud コンソールで指定した設定を SIEM システムの設定と比べて確認してください。

次の図は、ArcSight にエクスポートされたイベントを示します。たとえば、最初のイベントは重大な管理サーバーイベントです：「*デバイスのステータスが「緊急」です。*」

エクスポートされたイベントの SIEM システムでの表示は、使用している SIEM システムによって異なります。


Search | HP ArcSight Logger 6.2.0.7633.0 – Mozilla Firefox
Configuring a SmartCon...
Summary | HP ArcSig...
Search | HP ArcSight...
https://localhost/logger/search.ftl?ehr=1&ausm_query=_deviceGroup in ["mikrotik_admin.avp.ru [tcp cef]"]&from=1/24/2017
ArcSight Logger
Summary
Analyze
Dashboards
Configuration
System Admin
Take me to... (Alt+0)
EPS In:
EPS Out:
CPU:
admin
All Fields
Custom time range
Start
1/24/2017
16:09:59
Dynamic
End
$Now
Dynamic
_deviceGroup in ["mikrotik_admin.avp.ru [tcp cef]"]
Go!
Advanced
5 events (Scanned: 590 events, 00:00.815)
1 bar = 1 second
17:26:41
17:26:49
17:26:57
17:27:05
Time (Event Time)
Device
Logger
deviceVendor
deviceProduct
deviceVersion
Selected Fields (5)
deviceEventClassId 2
deviceProduct 1
deviceVendor 1
deviceVersion 1
name 2
1
2017/01/24 17:27:11 MSK
mikrotik_admin.avp.ru [tcp cef]
Local
KasperskyLab
SecurityCenter
10.4.343
RAW
CEF:0|KasperskyLab|SecurityCenter|10.4.343|KLSRV_HOST_STATUS_CRITICAL|Device status is Critical|4|msg=Status of device 'KSC-343' changed to Critical: No security application installed. rt=1485268056 dhost=KSC-343 dst=127.0.0.1 cs2=1093 cs2L
2
2017/01/24 17:26:41 MSK
mikrotik_admin.avp.ru [tcp cef]
Local
KasperskyLab
SecurityCenter
10.4.343

イベントの例

マネージドサービスプロバイダー（MSP）向けのクイックスタートガイド

クイックスタートガイドは、マネージドサービスプロバイダー（MSP）の管理者を対象としています。

Kaspersky Security Center Cloud コンソールでは、マルチ手ナンシーがサポートされます。このガイドには、顧客のアカウント（テナント）を管理し、デバイスにセキュリティ製品をインストールするためのヒントが記されています。

Kaspersky Security Center Cloud コンソールの概要

Kaspersky Security Center Cloud コンソールは、カスペルスキーがホストおよび維持する製品です。ユーザーが Kaspersky Security Center Cloud コンソールをコンピューターまたはサーバーにインストールする必要はありません。Kaspersky Security Center Cloud コンソールにより、管理者はカスペルスキーのセキュリティ製品を企業ネットワークのデバイスにインストールしたり、リモートでスキャンを実行してタスクをアップデートしたり、管理対象アプリケーションのセキュリティポリシーを管理したりできます。管理者は、組織用デバイスのステータスのスナップショット、詳細なレポート、粒度の細かい保護ポリシーの設定を備えた、詳細なダッシュボードを使用できます。

Kaspersky Security Center Cloud コンソールの主な機能

Kaspersky Security Center Cloud コンソールでは、次のような操作が可能です：

- ネットワーク上のデバイスへのカスペルスキー製品のインストールおよびインストールされた製品の管理。
- 管理グループの階層を作成して、いくつかのクライアントデバイスを1つの単位として管理する。
- 仮想管理サーバーを作成し、階層に配置する。
- ワークステーションやサーバーを含む、ネットワークデバイスを保護する：
  - カスペルスキー製品で構築されたアンチマルウェアによる保護システムを管理する。
  - 次のような、検知とレスポンス（EDR および MDR）の機能を使用する（Kaspersky Endpoint Detection and Response または Kaspersky Managed Detection and Response のライセンスが必要）：
    - インシデントの分析と調査
    - 脅威の活動連鎖の図表の作成によるインシデントの可視化
    - レスポンスに対する手動の許可または拒否、またはすべてのレスポンスに対する自動許可の設定
- Kaspersky Security Center Cloud コンソールをマルチテナントアプリケーションとして使用する。
- クライアントデバイスにインストールされているカスペルスキー製品をリモートで管理する。
- クライアントデバイスに対するカスペルスキー製品のライセンスの一元的な配信を実行する。
- ネットワーク上のデバイスのセキュリティポリシーを作成して管理する。

- ユーザーアカウントを作成して管理する。
- ユーザーロールを作成して管理する（RBAC）。
- ネットワーク上のデバイスにインストールされた製品のタスクを作成して管理する。
- 各クライアント組織のセキュリティシステムのステータスに関するレポートを個別に表示する。

MSP 向けの Kaspersky Security Center Cloud コンソールのライセンスの概要

Kaspersky Security Center Cloud コンソールの使用開始時に、試用版のワークスペースを要求する（この場合、ワークスペースに組み込みの 30 日の試用版ライセンスが付与されます）か、製品版ライセンスのアクティベーションコードを入力できます。

試用版のワークスペースは製品版に変換できません。試用版ライセンスの有効期間の終了後も Kaspersky Security Center Cloud コンソールを引き続き使用するには、試用版のワークスペースを削除して、製品版ライセンスで別のワークスペースを作成する必要があります。

その後、管理サーバーリポジトリに1つ以上の製品版ライセンスを追加できます。

MSP 向けの検知とレスポンスの機能の概要

Kaspersky Security Center Cloud コンソールのインターフェイスでは、他のカスペルスキー製品の機能を統合できます。たとえば、次の製品を統合して、Kaspersky Security Center Cloud コンソールの機能に 検知とレスポンスの機能を追加できます：

- Kaspersky Endpoint Detection and Response Optimum

  Kaspersky Endpoint Detection and Response Optimum は、組織の IT インフラストラクチャを複雑なサーバー脅威から保護するために設計されたソリューションです。脅威の自動検知と、検知された脅威への対応を組み合わせたこのソリューションの機能により、新しい脆弱性攻撃、ランサムウェア、ファイルレス攻撃、正規のシステムツールを使用する手法などの複雑な攻撃に耐えることができます。

  Kaspersky Endpoint Protection Platform（EPP）製品がセキュリティインシデントを検知すると、セキュリティインシデントに関する重要なデータを含む詳細なカードが Kaspersky Security Center Cloud コンソールで生成されます。インシデントカードは次の製品のいずれかによって生成されます：

  - Kaspersky EPP 製品とともにインストールされる Kaspersky Endpoint Agent
  - 組み込みの EDR Optimum 機能を備えた Kaspersky Endpoint Security 11.7.0 for Windows 以降（Kaspersky Endpoint Agent の追加インストール不要）

  インシデントカードは、インシデントの分析と調査を可能にします。また、脅威の活動連鎖の図表の作成によりインシデントを可視化できます。グラフでは、検知された脅威の導入の段階について、時系列で説明します。作成されたグラフには、攻撃に関与するモジュールと、これらのモジュールが実行する処理についての情報が含まれます。

  レスポンス処理のチェーン（信頼されていないオブジェクトに対する実行ブロックルールの作成、選択された侵害インジケーター（IOC）に基づくデバイスグループ内の類似インシデントの検索、信頼されていないオブジェクトの隔離、侵害されたデバイスのネットワークからの隔離）も開始できます。

  製品のアクティベーションに関する情報については、Kaspersky Endpoint Detection and Response Optimum のヘルプを参照してください。

統合すると、この製品は Kaspersky Security Center Cloud コンソールのインターフェイスに［**アラート**］セクションを追加します（［**監視とレポート**］→［**アラート**］）。

- Kaspersky Managed Detection and Response

  Kaspersky Managed Detection and Response は、自動の防御壁を回避し、数が増え続ける脅威に対する 24 時間体制の保護を、専門技術とスタッフを見つけるのに苦労している組織や、社内リソースに制限のある組織に提供します。カスペルスキーの MDR SOC アナリスト、またはサードパーティ企業がインシデントを調査し、インシデントを解決するためのレスポンスを提案します。ユーザーは提案されたレスポンスを手動で許可または拒否できます。すべてのレスポンスを自動許可するオプションをオンにすることもできます。

  製品のアクティベーションに関する情報については、Kaspersky Managed Detection and Response のヘルプを参照してください。

  統合すると、この製品は Kaspersky Security Center Cloud コンソールのインターフェイスに［**インシデント**］セクションを追加します（［**監視とレポート**］→［**インシデント**］）。

Kaspersky Endpoint Detection and Response または Kaspersky Managed Detection and Response の機能を参照するインターフェイス要素は、Kaspersky Security Center Cloud コンソールの［**インターフェイスのオプション**］セクションでいつでも表示または非表示にできます。

Kaspersky Security Center Cloud コンソールの使用を開始する

このセクションのシナリオを実行すると、Kaspersky Security Center Cloud コンソールを使用する準備が完了します。

使用を開始するためのシナリオ

このシナリオは段階的に進行します：

1. **アカウントの作成**

   Kaspersky Security Center Cloud コンソールの使用を開始するには、アカウントが必要です。

   アカウントを作成するには：

   1. ブラウザーを開いて、https://ksc.kaspersky.com と入力します。
   2. ［**アカウントの作成**］をクリックします。
   3. 画面上の指示に従ってください。

2. **ワークスペースの作成**

   アカウントの作成後に、会社を登録してワークスペースを作成できます。

   Kaspersky Security Center Cloud コンソールの使用開始時に、試用版のワークスペースを要求する（この場合、ワークスペースに組み込みの 30 日の試用版ライセンスが付与されます）か、製品版ライセンスのアクティベーションコードを入力できます。

   > 試用版のワークスペースは製品版に変換できません。試用版ライセンスの有効期間の終了後も Kaspersky Security Center Cloud コンソールを引き続き使用するには、試用版のワークスペースを削除して、製品版ライセンスで別のワークスペースを作成する必要があります。

   会社を登録してワークスペースを作成するには：

1. ブラウザーを開いて、https://ksc.kaspersky.com と入力します。
2. ［**サインイン**］をクリックします。
3. 画面上の指示に従ってください。

3 Kaspersky Security Center Cloud コンソールの初期セットアップの実行

作成したワークスペースの初回の使用時に、クイックスタートウィザードの実行が自動的に要求されます。クイックスタートウィザードでは、必要最小限のタスクとポリシーを作成し、設定を最小限に調整して、カスペルスキー製品のインストールパッケージの作成を開始できます。画面上の指示に従ってください。

初期セットアップの終了後、Kaspersky Security Center Cloud コンソールを使用する準備が完了します。

顧客のデバイスを管理する場合の推奨事項

このセクションでは、保護対象の顧客のデバイスを管理する場合の推奨事項について説明します。

推奨事項は、Kaspersky Security Center を初めて使用しているか、オンプレミスバージョンを既に使用したことがあるかによって異なります。

- 以前に Kaspersky Security Center を使用したことがない場合は、2 つのオプションがあります：
  - 各顧客のデバイス用に仮想管理サーバーを作成する（推奨オプション）。この場合、他の顧客とは別に、専用の仮想管理サーバーで各顧客のデバイスを管理できます。同時に、プライマリ管理サーバーを使用して、すべての顧客用に共通のポリシーとタスクを作成できます。プライマリ管理サーバーで生成されるレポートには、すべての仮想管理サーバーからのデータを含めることができます。
  - 各顧客のデバイス用に管理グループを作成する。顧客のデバイスをさらにグループ化する場合は、親グループの下位に管理グループの階層を作成できます。たとえば、異なる部門で勤務する従業員のデバイス用に異なる保護設定を使用するには、下位グループが必要な場合があります。
- オンプレミスで実行されている Kaspersky Security Center を既に使用したことがある場合は、既存の管理グループと関連するオブジェクトを、オンプレミスの Kaspersky Security Center から Kaspersky Security Center Cloud コンソールに移行できます。

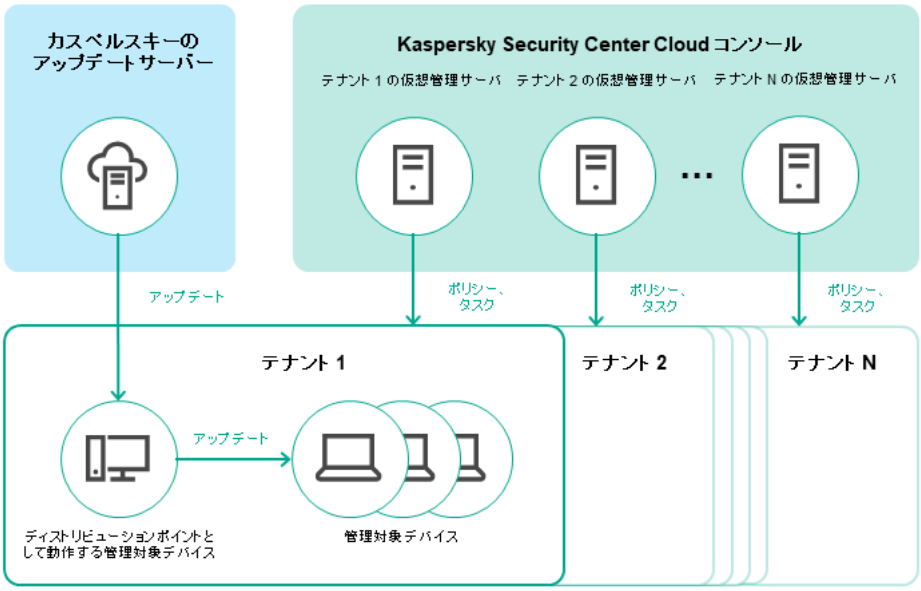
  仮想管理サーバーは移行できません。管理グループとその他のオブジェクトの移行後は、Kaspersky Security Center Cloud コンソールで仮想管理サーバーを作成できます。

  移行の設定に進みます。

仮想管理サーバーの管理者は、プライマリ管理サーバーからのみ、この仮想サーバーに移動できます。仮想管理サーバーの管理者は、プライマリ管理サーバーで作成されたすべてのオブジェクト（ウィジェット、レポート、ユーザーロールなど）を読み取ることができます。

標準的な導入スキーム（MSP 向け）

このセクションでは、MSP が複数テナントの管理に標準的に使用する導入スキームについて説明します。スキームは、各テナント用に個別に作成された仮想管理サーバーを使用した管理に基づいています。



標準的な導入スキーム（MSP 向け）

スキームを構成する主なコンポーネントは次の通りです：

- *Kaspersky Security Center Cloud コンソール*：ワークスペースの管理サービスのユーザーインターフェイスを提供します。Kaspersky Security Center Cloud コンソールを使用して、クライアント組織のネットワークの保護システムを導入、管理、維持できます。
- *カスペルスキーのアップデートサーバー*：カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。
- *仮想管理サーバー*：MSP 管理者は通常、各テナント用に仮想管理サーバーを作成して、対応するクライアント組織のネットワークの保護システムを導入、管理、維持します。
- *テナント*：保護するデバイスが属するクライアント組織。
- *管理対象デバイス*：Kaspersky Security Center Cloud コンソールによって保護されているクライアント企業のデバイス。保護する必要がある各デバイスには、ネットワークエージェントとカスペルスキーのセキュリティ製品のいずれかがインストールされている必要があります。
- *ディストリビューションポイントとして動作する管理対象デバイス*：ネットワークエージェントがインストールされており、アップデートの配信、ネットワークポーリング、アプリケーションのリモートインストール、管理グループやブロードキャストドメインでのコンピューター情報の取得に使用されるコンピューター。管理者が適切なデバイスを選択し、ディストリビューションポイントを手動で割り当てます。

シナリオ：製品導入（仮想管理サーバーからのテナント管理）

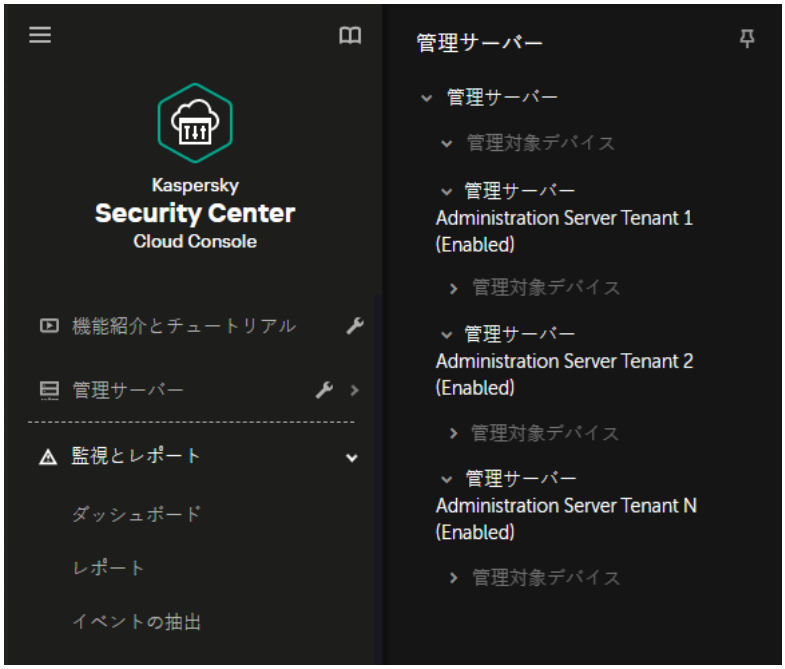
Kaspersky Security Center を使用したことがなく、仮想管理サーバーを使用してテナントを管理する場合は、このセクションの説明に従います。このシナリオを完了すると、顧客のデバイスを管理できます。

複数のテナントを管理する場合は、各テナントで個別にシナリオを実行してください。

このシナリオは段階的に進行します：

1. **仮想管理サーバーの作成**

顧客用に仮想管理サーバーを作成します。新しい仮想管理サーバーは、管理サーバーの階層に表示されます：



管理サーバーの階層の仮想管理サーバー

2 ディストリビューションポイントとして動作するデバイスの選択

顧客のデバイスの中から、ディストリビューションポイントとして動作するデバイスを決定します。

1つのワークスペース内に100個を超えるディストリビューションポイントは指定できません。

3 ネットワークエージェントのスタンドアロンインストールパッケージの作成

作成した仮想管理サーバーに切り替えて、ネットワークエージェントのスタンドアロンインストールパッケージを作成します。メインメニューで現在の管理サーバー名の右側にあるシェブロンアイコン（）をクリックして、必要な管理サーバーを選択すると、管理サーバーを切り替えることができます。スタンドアロンインストールパッケージの作成時に、デバイスの移動先となる管理対象デバイスの管理グループを指定します。

4 選択したディストリビューションポイントとして動作するデバイスへのネットワークエージェントのインストール

適切な任意の方法を使用できます：

- 手動インストール

  スタンドアロンインストールパッケージをデバイスに配布するには、たとえばリムーバブルドライブ（フラッシュドライブなど）にコピーしたり、共有フォルダーに配置したりできます。

- Active Directoryを使用した導入
- リモート監視および管理（RMM）ソフトウェアソリューションを使用した導入

5 ディストリビューションポイントの割り当て

ネットワークエージェントをインストールしたデバイスをディストリビューションポイントとして割り当てます。

6 ネットワークポーリング

ディストリビューションポイントでネットワークポーリングを設定して実行します。

Kaspersky Security Center Cloud コンソールでは、次のネットワークポーリングの方法を使用できます：

- IP アドレス範囲のポーリング
- Windows ネットワークのポーリング
- Active Directory のポーリング

スケジュールに応じたネットワークポーリングの完了後、顧客のデバイスが検出され、［**未割り当てデバイス**］グループに配置されます。

7. **検出されたデバイスの管理グループへの移動**

   自動的に必要な管理グループに検出されたデバイスを移動するルールを設定するか、必要な管理グループに手動でこれらのデバイスを移動します。顧客のデバイスを1つの管理グループで管理する場合は、管理対象デバイスグループにデバイスを移動できます。

8. **ネットワークエージェントと管理対象のカスペルスキー製品のインストールパッケージの作成**

   カスペルスキー製品のインストールパッケージを作成します。

9. **サードパーティのセキュリティ製品の削除**

   顧客のデバイスにサードパーティのセキュリティ製品がインストールされている場合は、カスペルスキー製品をインストールする前にそれらを削除します。

10. **クライアントデバイスへのカスペルスキー製品のインストール**

    顧客のデバイスにネットワークエージェントと管理対象のカスペルスキー製品をインストールするための、リモートインストールタスクを作成します。

    必要に応じて、異なる管理グループや異なるデバイスの抽出を対象に、管理対象のカスペルスキー製品をインストールするための複数のリモートインストールタスクを作成することもできます。

    タスクの作成後、それらの設定を構成できます。各タスクのスケジュールが要件に合致しているかを確認します。最初に、ネットワークエージェントをインストールするタスクを実行する必要があります。顧客のデバイスへのネットワークエージェントのインストール後、管理対象のカスペルスキー製品をインストールするタスクを実行する必要があります。

11. **カスペルスキー製品の初期導入の確認**

    カスペルスキー製品バージョンレポートを生成して表示します。管理対象のカスペルスキー製品が顧客のすべてのデバイスにインストールされていることを確認します。

12. **カスペルスキー製品用のポリシーの作成**

    必要なカスペルスキー製品用にポリシーを作成します。すべての顧客用に汎用的なポリシーを作成する場合は、現在の仮想管理サーバーをプライマリ管理サーバーに切り替えて、必要なカスペルスキー製品用にポリシーを作成します。

シナリオ：製品導入（管理グループからのテナント管理）

Kaspersky Security Center を使用したことがなく、管理グループを使用してテナントを管理する場合は、このセクションの説明に従います。このシナリオを完了すると、顧客のデバイスを管理できます。

このシナリオは段階的に進行します：

1. **管理グループの作成**

   各顧客に管理グループを作成します。

2 ディストリビューションポイント構造の計画

各顧客のデバイスの中から、ディストリビューションポイントとして動作するデバイスを決定します。

1つのワークスペース内に100個を超えるディストリビューションポイントは指定できません。

3 ネットワークエージェントのスタンドアロンインストールパッケージの作成

ネットワークエージェントのスタンドアロンインストールパッケージを作成します。

4 選択したディストリビューションポイントとして動作するデバイスへのネットワークエージェントのインストール

選択したディストリビューションポイントとして動作するデバイスにネットワークエージェントをインストールします。

適切な任意の方法を使用できます：

- 手動インストール

  スタンドアロンインストールパッケージをデバイスに配布するには、たとえばリムーバブルドライブ（フラッシュドライブなど）にコピーしたり、共有フォルダーに配置したりできます。

- Active Directoryを使用した導入
- リモート監視および管理（RMM）ソフトウェアソリューションを使用した導入

5 ディストリビューションポイントの割り当て

ネットワークエージェントをインストールしたデバイスをディストリビューションポイントとして割り当てます。

6 ネットワークポーリング

ディストリビューションポイントでネットワークポーリングを設定して実行します。

Kaspersky Security Center Cloudコンソールでは、次のネットワークポーリングの方法を使用できます：

- IPアドレス範囲のポーリング
- Windowsネットワークのポーリング
- Active Directoryのポーリング

スケジュールに応じたネットワークポーリングの完了後、顧客のデバイスが検出され、［**未割り当てデバイス**］グループに配置されます。

7 検出されたデバイスの管理グループへの移動

自動的に必要な管理グループに検出されたデバイスを移動するルールを設定するか、必要な管理グループに手動でこれらのデバイスを移動します。

8 ネットワークエージェントと管理対象のカスペルスキー製品のインストールパッケージの作成

クイックスタートウィザードを起動しなかった、またはインストールパッケージを作成するステップを省略した場合は、カスペルスキー製品のインストールパッケージを作成します。

9 サードパーティのセキュリティ製品の削除

顧客のデバイスにサードパーティのセキュリティ製品がインストールされている場合は、カスペルスキー製品をインストールする前にそれらを削除します。

10. **顧客のデバイスへのカスペルスキー製品のインストール**

    顧客のデバイスにネットワークエージェントと管理対象のカスペルスキー製品をインストールするための、リモートインストールタスクを作成します。

    必要に応じて、異なる管理グループや異なるデバイスの抽出を対象に、管理対象のカスペルスキー製品をインストールするための複数のリモートインストールタスクを作成することもできます。

    タスクの作成後、それらの設定を構成できます。各タスクのスケジュールが要件に合致しているかを確認します。最初に、ネットワークエージェントをインストールするタスクを実行する必要があります。顧客のデバイスへのネットワークエージェントのインストール後、管理対象のカスペルスキー製品をインストールするタスクを実行する必要があります。

11. **カスペルスキー製品の初期導入の確認**

    カスペルスキー製品バージョンレポートを生成して表示します。管理対象のカスペルスキー製品が顧客のすべてのデバイスにインストールされていることを確認します。

12. **カスペルスキー製品用のポリシーの作成**

    ［**アセット（デバイス）**］→［**グループ**］メニューの順に移動します。すべての顧客用に汎用的なポリシーを作成する場合は、［**管理サーバー**］**を選択します。**各顧客に特定のポリシーを作成する場合は、その顧客に対応する管理グループを選択します。必要なカスペルスキー製品用にポリシーを作成します。

オンプレミスの Kaspersky Security Center と Kaspersky Security Center Cloud コンソールの共同利用

オンプレミスで実行されている Kaspersky Security Center を既に使用したことがある場合は、このセクションの説明に従って、オンプレミスで実行されている既存の管理サーバーを、新しい Kaspersky Security Center Cloud コンソール管理サーバーのセカンダリ管理サーバーに変換できます。

オンプレミスの Kaspersky Security Center と Kaspersky Security Center Cloud コンソールの共同利用を設定した場合は、管理サーバーの階層を削除しない限り、オンプレミスの Kaspersky Security Center から Kaspersky Security Center Cloud コンソールには移行できません。

管理サーバーの階層を作成するには：

オンプレミスで実行されている既存の管理サーバーをセカンダリ管理サーバーとして追加します。

カスペルスキー製品のライセンス（MSP 向け）

Kaspersky Security Center Cloud コンソールでは、顧客のデバイスにカスペルスキー製品のライセンスを一元的に配信し、使用状況の監視およびライセンスの更新を実行できます。

複数のテナントを管理する場合は、次の方法でライセンスを配信できます：

- すべてのテナントに1つのライセンス
- 各テナントに個別のライセンス

顧客のデバイスにライセンスを配信するには：

1. 管理サーバーリポジトリに必要なライセンスを追加します。

2. 次のいずれかの手順を実行します：

- ライセンスの自動配信を設定する。

  この場合、 Kaspersky Security Center Cloud コンソールは適用可能なライセンスを1つ選択し、新しいデバイスが検出されるたびに自動的に配信します。

- ライセンスをデバイスに配信するためのライセンスの追加タスクを設定する。

  このタスクの設定時に、デバイスに配信する必要があるライセンスと、必要なデバイスが属する管理グループを選択します。

  1つのタスクで配信できるライセンスは1つのみです。したがって、複数のライセンスを配信する場合は、それぞれにタスクを作成する必要があります。

顧客のデバイスにインストールされているカスペルスキー製品がアクティベートされます。

監視とレポートの機能（MSP 向け）

Kaspersky Security Center Cloud コンソールでは、監視とレポートの機能を使用できます。これらの機能を使用して、組織のインフラストラクチャの状況、保護ステータス、統計情報を確認できます。

Kaspersky Security Center Cloud コンソールの導入時に、必要に応じて監視とレポートの機能の設定を最適な状態に編集できます。

Kaspersky Security Center Cloud コンソールでは、次のような監視とレポートの機能を使用できます：

- ダッシュボード
- レポート
- イベントの抽出
- メール通知

ダッシュボード

ウィジェットを使用すると、情報をグラフィカルに表示することで、組織のネットワークのセキュリティ傾向を監視できます（下の図を参照）。

ダッシュボードセクション

レポート

レポート機能を使用することで、組織ネットワークのセキュリティに関する詳細な数値データを取得し、これらの情報をファイルに保存したり、メールで送信したり、印刷することができます。メールでレポートの配信をスケジュールすることもできます（下の図を参照）。

イベントの抽出

イベントの抽出は、管理サーバーのデータベース内に保存されているイベントを一定の条件を指定して抽出し、画面上に表示できる機能です。Kaspersky Security Center Cloud コンソールには、定義済みのイベントの抽出（［**最近のイベント**］や［**緊急イベント**］など）がいくつかあります。カスタムのイベントの抽出を作成することもできます。

メール通知

Kaspersky Security Center Cloud コンソールと顧客のデバイスで発生するイベントに関するメール通知を設定できます。

クラウド環境での Kaspersky Security Center Cloud コンソールの操作

このセクションでは、Amazon Web Services、Microsoft Azure、Google Cloud などのクラウド環境での Kaspersky Security Center Cloud コンソールの運用とメンテナンスに関わる Kaspersky Security Center Cloud コンソールの機能について説明します。

クラウド環境での動作には、専用のライセンスが必要です。専用のライセンスがない場合、クラウドデバイスに関係するインターフェイス要素は操作できません。

クラウド環境で利用できるライセンスオプションについて

Kaspersky Security Center Cloud コンソールの試用モードと製品モードの両方で、クラウド環境での作業が可能です。

- 試用モードでは、ワークスペースの有効期間を通してすべてのクラウド環境の機能を使用できます。ライセンスは不要です。
- 製品モードでは、管理サーバーのプロパティで Kaspersky Hybrid Cloud Security のライセンスを現在のライセンスとして追加した場合のみ、クラウド環境の機能を使用できます。

いずれの場合も、脆弱性とパッチ管理は自動的にアクティベートされます。

Kaspersky Hybrid Cloud Security のライセンスを使用して、クラウド環境のサポート機能をアクティベートしようとすると、エラーが発生する場合があります。

クラウド環境での Kaspersky Security Center Cloud コンソールの操作の準備

このセクションでは、次のクラウド環境で Kaspersky Security Center Cloud コンソールを操作するために準備する方法について説明します：

- Amazon Web Services
- Microsoft Azure
- Google Cloud

Amazon Web Services クラウド環境での利用

このセクションでは、Amazon Web Services で Kaspersky Security Center Cloud コンソールを使用するための準備について説明します。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center Cloud コンソールのリリース日時点のものです。

Amazon Web Services クラウド環境での使用について

AWS プラットフォームを使用し、特にインスタンスを作成するには、Amazon Web Services のアカウントが必要です。無料のアカウントを https://aws.amazon.com/jp/ で作成できます。既存の Amazon アカウントも使用できます。

AMI、および AWS Marketplace の仕組みの詳細については、AWS Marketplace Help ページにアクセスしてください。AWS プラットフォームでの作業、インスタンスの使用、関連する概念の詳細については、Amazon Web Services のドキュメントを参照してください。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center Cloud コンソールのリリース日時点のものです。

Amazon EC2 インスタンスで IAM ユーザーアカウントを作成する

このセクションでは、Kaspersky Security Center Cloud コンソールを正常に動作させるために必要な手順について説明します。具体的な操作としては、AWS IAM（ID およびアクセス管理）ユーザーアカウントの操作が含まれます。また、クライアントデバイスにネットワークエージェントをインストールしてから、Kaspersky Security for Windows Server や Kaspersky Endpoint Security for Linux をインストールするために必要なクライアントデバイスでの手順についても説明します。

Kaspersky Security Center Cloud コンソールが AWS を使用する権限を持っているかどうかの確認

Kaspersky Security Center Cloud コンソールを使用して Amazon Web Services クラウド環境で操作するには、Kaspersky Security Center Cloud コンソールが AWS サービスの操作に使用する *IAM user account* を作成する必要があります。管理サーバーでの作業開始前に、IAM ユーザーアカウントおよび対応する *AWS IAM アクセスキー*（以降、*IAM アクセスキー*とも表記）を作成します。

IAM ユーザーアカウントの作成には、AWS 管理コンソールが必要です。AWS 管理コンソールを使用するには、AWS のアカウントのユーザー名とパスワードが必要です。

Kaspersky Security Center Cloud コンソールで使用する IAM ユーザーアカウントの作成

Kaspersky Security Center Cloud コンソールを使用するには、IAM ユーザーアカウントが必要です。すべての必要な権限を付与した IAM ユーザーアカウントを 1 個作成することも、ユーザーアカウントを 2 個作成することもできます。

IAM ユーザーには、Kaspersky Security Center Cloud コンソールの初期設定時に指定する必要のある *IAM アクセスキー*が自動的に作成されます。IAM アクセスキーは、アクセスキー ID と秘密鍵で構成されますIAM サービスの詳細については、AWS の次のリファレンスページを参照してください：

- https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/introduction.html
- https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2

必要な権限を持つ IAM ユーザーアカウントを作成するには：

1. AWS 管理コンソールを開き、正しいアカウントでログインします。
2. AWS サービスのリストから、**IAM** を選択します。
   ユーザー名のリストとツールの操作メニューを含むウィンドウが表示されます。
3. ユーザーアカウントに関するメニューを選択して、ユーザー名を追加します。
4. 追加するユーザーについては、次の AWS プロパティを指定します：
   - アクセスの種類：**プログラムによるアクセス**
   - アクセス権限の境界は設定しない
   - アクセス権限：**ReadOnlyAccess**
     アクセス権限の追加後、正しい権限を追加したかを確認します。選択が誤っている場合は前の画面に戻って再度選択します。
5. ユーザーアカウントの作成後、新しい IAM ユーザーの IAM アクセスキーを含む表が表示されます。アクセスキーの ID が［**アクセスキー ID**］列に表示されます。秘密鍵は［**シークレットアクセスキー**］列にアスタリスクとして表示されます。秘密鍵を表示するには、［**表示**］をクリックします。

新しく作成されたアカウントが、AWS アカウントに対応する IAM ユーザーアカウントの一覧に表示されます。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center Cloud コンソールのリリース日時点のものです。

Microsoft Azure クラウド環境での利用

このセクションでは、Microsoft Azure により提供されるクラウド環境での Kaspersky Security Center Cloud コンソールの操作とメンテナンスについての情報、およびこのクラウド環境での仮想マシンへの製品導入の詳細を説明します。

Microsoft Azure の使用について

Microsoft Azure プラットフォームを使用し、特に Azure Marketplace でアプリを購入して仮想マシンを作成するには、Azure サブスクリプションが必要です。Kaspersky Security Center Cloud コンソールで Microsoft Azure の作業を開始する前に、Azure アプリケーション ID を作成して、仮想マシンで製品をインストールするために必要な権限を付与します。

サブスクリプション、アプリケーション ID およびパスワードの作成

Microsoft Azure 環境で Kaspersky Security Center Cloud コンソールを使用するには、Azure サブスクリプション、Azure アプリケーション ID および Azure アプリケーションパスワードが必要です。既にサブスクリプションを保有している場合は、既存のサブスクリプションを使用できます。

Azure サブスクリプションを保有していると、Microsoft Azure プラットフォーム管理ポータルと Microsoft Azure サービスへのアクセスが許可されます。サブスクリプションの保有者は、Windows Azure プラットフォームを使用して Azure SQL、Azure ストレージなどのサービスを管理できます。

Microsoft Azure サブスクリプションを作成するには：

https://learn.microsoft.com/ja-jp/azure/cost-management-billing/manage/create-subscription に移動します。そこにある指示に従ってください。

サブスクリプションの作成の詳細については、Microsoft の Web サイトを参照してください。サブスクリプション ID を取得できます。後程、このサブスクリプション ID とアプリケーション ID およびパスワードを、Kaspersky Security Center Cloud コンソールに入力します。

Azure アプリケーション ID とパスワードを作成するには：

1. https://portal.azure.com に移動し、ログインしていることを確認します。
2. リファレンスページの指示に従って、アプリケーション ID を作成します。
3. アプリケーション設定の［**キー**］セクションに移動します。
4. ［**キー**］セクションで、［**説明**］と［**有効期限**］を入力し、［**値**］は空白のままにしておきます。
5. ［**保存**］をクリックします。

   ［**保存**］をクリックすると、［**値**］フィールドにシステムが自動的に生成した長い文字列が表示されます。この文字列が Azure アプリケーションパスワードとなります（例：yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU= など）。説明は入力した通りに表示されます。
6. パスワードをコピーして保管し、後程 Kaspersky Security Center Cloud コンソールでアプリケーション ID とパスワードを入力できるようにしておきます。

   パスワードはこの作成画面でのみコピーできます。この機会を逃すと、パスワードは表示されなくなり復元できません。

文書中で引用されている Web ページのアドレスの正確性は、Kaspersky Security Center Cloud コンソールのリリース日時点のものです。

Azure アプリケーション ID へのロールの割り当て

デバイスの検索を使用した仮想マシンの検出のみが目的の場合、Azure アプリケーション ID に「Reader」ロールを割り当てる必要があります。仮想マシンの検出だけでなく、Azure API を使用して仮想マシンへの保護の導入も行う場合、Azure アプリケーション ID に「Virtual Machine Contributor」ロールを割り当てる必要があります。

マイクロソフト社の Web サイトの説明に従って、Azure アプリケーション ID にロールを割り当てます。

Google Cloud での利用

このセクションでは、Google が提供するクラウド環境での Kaspersky Security Center Cloud コンソールの使用に関する情報を提供します。

Google API を使用して、Google Cloud Platform で Kaspersky Security Center Cloud コンソールを操作できます。Google アカウントが必要です。詳細については、https://cloud.google.com にある Google のドキュメントを参照してください。

次の認証情報を作成し Kaspersky Security Center Cloud コンソールに提供する必要があります：

- **クライアントのメール**

  クライアントのメールアドレスは、Google Cloud でプロジェクトの登録に使用したメールアドレスです。

- **プロジェクト ID**

  プロジェクト ID は、Google Cloud でプロジェクトの登録時に取得した ID です。

- **秘密鍵**

  秘密鍵は、Google Cloud でプロジェクトの登録時に秘密鍵として取得した文字列です。間違えないように、この文字列をコピーして貼り付けることを検討してください。

Kaspersky Security Center Cloud コンソールのクラウド環境設定ウィザード

このウィザードを使用して Kaspersky Security Center Cloud コンソールを設定する場合に必要な項目は次の通りです：

- クラウド環境用の特定の資格情報：
  - クラウドセグメントをポーリングするための権限が付与された IAM ユーザーアカウント（Amazon Web Services で使用する場合）
  - Azure アプリケーション ID パスワードとサブスクリプション（Microsoft Azure で使用する場合）
  - Google クライアントのメールアドレス、プロジェクト ID、秘密鍵（Google Cloud で使用する場合）
- インストールパッケージ：
  - Windows 用のネットワークエージェント
  - Linux 用のネットワークエージェント
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux の Web プラグイン
- 次のうち少なくとも 1 つ：
  - Kaspersky Endpoint Security for Windows のインストールパッケージと Web プラグイン（推奨）
  - Kaspersky Security for Windows Server のインストールパッケージと Web プラグイン

Kaspersky Hybrid Cloud Security ライセンスを使用してワークスペースを作成した場合は、Kaspersky Security Center Cloud コンソールへの初回接続時に、クラウド環境設定ウィザードが自動的に開始されます。また、クラウド環境設定ウィザードは手動でいつでも起動できます。

クラウド環境設定ウィザードを手動で起動するには：

メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**クラウド環境の設定**］の順に移動します。

ウィザードが起動します。

このウィザードの平均作業時間は約 15 分です。

ステップ 1：必要なプラグインとインストールパッケージのチェック

以下にリストされている必要な Web プラグインとインストールパッケージがすべてある場合、この手順は表示されません。

クラウド環境の構成には、次のコンポーネントが必要です：

- インストールパッケージ：
  - Windows 用のネットワークエージェント
  - Linux 用のネットワークエージェント
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux の Web プラグイン
- 次のうち少なくとも 1 つ：
  - Kaspersky Endpoint Security for Windows のインストールパッケージと Web プラグイン（推奨）
  - Kaspersky Security for Windows Server のインストールパッケージと Web プラグイン

    Kaspersky Security for Windows Server の代わりに、Kaspersky Endpoint Security for Windows を使用することを推奨します。

Kaspersky Security Center Cloud コンソールは、既にあるコンポーネントを自動的に検出し、不足しているコンポーネントのみをリスト表示します。［**ダウンロードするアプリケーションを選択**］をクリックし、必要なプラグインとインストールパッケージを選択して、一覧表示されたコンポーネントをダウンロードします。コンポーネントのダウンロード後、［**更新**］を使用して不足しているコンポーネントのリストを更新できます。

ステップ 2：アプリケーションのアクティベート方法の選択

このステップは、ワークスペースの作成時に Kaspersky Hybrid Cloud Security 以外のライセンスを使用し、Kaspersky Hybrid Cloud Security ライセンスを管理サーバーのアクティベーションフィールドに追加したことがない場合にのみ表示されます。この場合は、Kaspersky Hybrid Cloud Security ライセンスを使用して管理サーバーをアクティベートする必要があります。

ステップ 3：クラウド環境と認証の選択

次の設定を指定します：

- **クラウド環境**

  Kaspersky Security Center Cloud コンソールを導入するクラウド環境を選択します：AWS、Azure、または Google Cloud。

  複数のクラウド環境を使用する場合は、1 つの環境を選択してもう一度ウィザードを実行します。

- **接続名**

  接続の名前を入力します。名前を 256 文字以上にすることはできません。Unicode 文字のみを使用できます。

  この名前はクラウドデバイスの管理グループの名前としても使用されます。

  複数のクラウド環境を使用する予定の場合は、たとえば「Azure Segment」「AWS Segment」「Google Segment」のように、環境の名前を接続名に含めることを検討してください。

認証情報を入力し、指定したクラウド環境での認証を受信します。

AWS

AWS をクラウドセグメントの種別として選択した場合、クラウドセグメントをさらにポーリングするには、AWS IAM アクセスキーが必要です。次のキーデータを入力します：

- **アクセスキーの ID**

  IAM アクセスキーの ID（英数字の並び）：IAM ユーザーアカウント作成時に受け取ったキーの ID です。

  このフィールドは、認証のために AWS IAM アクセスキーを選択すると使用可能になります。

- **秘密鍵**

  IAM ユーザーアカウント作成時にアクセスキーの ID と一緒に受け取った秘密鍵です。

  秘密鍵の文字はアスタリスクで表示されます。秘密鍵を入力し始めると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを必要な間だけ押し続けます。

  このフィールドは、認証のために AWS IAM アクセスキーを選択すると使用可能になります。

  入力した文字を表示するには、［**表示**］を押し続けます。

Azure

Azure をクラウドセグメントの種別として選択した場合は、クラウドセグメントの今後のポーリングに使用する接続について、以下の設定を指定します：

- **Azure アプリケーション ID**

  Azure ポータルで作成したアプリケーション ID です。

  ポーリングやその他の目的で使用する Azure アプリケーション ID を 1 つだけ指定できます。別の Azure セグメントでポーリングを実行する場合は、既存の Azure 接続を事前に削除する必要があります。

- **Azure サブスクリプション ID**

  Azure ポータルで作成したサブスクリプションです。

- **Azure アプリケーションパスワード**

  アプリケーション ID の作成時に取得したアプリケーション ID のパスワードです。

  パスワードの文字はアスタリスクで表示されます。パスワードの入力を開始すると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを押し続けます。

  入力した文字を表示するには、［**表示**］を押し続けます。

- **Azure ストレージアカウント名**

  Kaspersky Security Center Cloud コンソールで使用するために作成した Azure ストレージアカウントの名前です。

- **Azure ストレージのアクセスキー**

  パスワード（アクセスキー）は、Kaspersky Security Center Cloud コンソールで使用する Azure ストレージアカウントの作成時に取得したものです。

  キーは、Azure ストレージアカウントの概要セクションのアクセスキーに関するサブセクションで確認できます。

  入力した文字を表示するには、［**表示**］を押し続けます。

Google Cloud

Google Cloud をクラウドセグメントの種別として選択した場合は、クラウドセグメントの今後のポーリングに使用する接続について、以下の設定を指定します：

- **クライアントメールアドレス**

  クライアントのメールアドレスは、Google Cloud でプロジェクトの登録に使用したメールアドレスです。

- **プロジェクト ID**

  プロジェクト ID は、Google Cloud でプロジェクトの登録時に取得した ID です。

- **秘密鍵**

  秘密鍵は、Google Cloud でプロジェクトの登録時に秘密鍵として取得した文字列です。間違えないように、この文字列をコピーして貼り付けることを検討してください。

  入力した文字を表示するには、［**表示**］を押し続けます。

この指定した接続は本製品の設定に保存されます。

クラウド環境設定ウィザードを使用して指定できるセグメントは1つのみです。後で追加の接続を指定して、他のクラウドセグメントを管理することもできます。

［**次へ**］をクリックして先に進みます。

ステップ 4：セグメントのポーリングとクラウドとの同期設定

このステップでは、クラウドセグメントのポーリングが開始され、クラウドデバイス専用の管理グループが自動的に作成されます。ポーリング中に検出されたデバイスはこのグループに配置されます。クラウドセグメントのポーリングスケジュールが設定されます。既定では 5 分ごとです（後で設定を変更できます）。

未割り当てデバイスを自動的に移動する［**クラウドと同期**］ルールも作成されます。以降、クラウドネットワークがスキャンされるたびに、検出された仮想デバイスは［**管理対象デバイス**］の［**クラウド**］グループ内の対応するサブグループに移動されます。

［**管理グループをクラウドの階層構造と同期**］設定を定義します。

このオプションをオンにすると、［**クラウド**］グループが自動的に［**管理対象デバイス**］グループ内に作成され、クラウドデバイスの検索が開始されます。クラウドネットワークの各スキャンによって検出されたインスタンスと仮想マシンは、クラウドグループ内に配置されます。このグループ内の管理サブグループの構造は、クラウドセグメントの構造に対応します（AWS では、アベイラビリティーゾーンとプレイスメントグループは構造に反映されません。Azure では、サブネットは構造に反映されません）。クラウド環境のインスタンスとして識別されていないデバイスは**未割り当てデバイス**グループに分類されます。このグループ構造を使用して、インストールタスクをグループ化してアンチウイルス製品をインスタンスにインストールし、グループごとに異なるポリシーを設定することができます。

このチェックボックスをオフにしても、**クラウド**グループは作成され、デバイスの検索も開始されます。ただし、クラウドセグメントの構造に対応するサブグループはグループ内で作成されません。検出されたすべてのインスタンスは**クラウド**管理グループに属しているため、1つのリストに表示されます。同期を必要とする Kaspersky Security Center Cloud コンソールを使用している場合、［**クラウドと同期**］ルールのプロパティを編集し、このルールを強制的に実行することもできます。このルールを強制的に適用すると、クラウドセグメントの構造と一致するようにクラウドグループ内のサブグループの構造が変更されます。

既定では、このオプションはオフです。

［**次へ**］をクリックして先に進みます。

ステップ5：ポリシーとタスクを作成するアプリケーションの選択

この手順は、 Kaspersky Endpoint Security for Windows と Kaspersky Security for Windows Server の両方のインストールパッケージとプラグインがある場合にのみ表示されます。これらのアプリケーションの1つのみのプラグインとインストールパッケージがある場合、この手順はスキップされ、 Kaspersky Security Center Cloud コンソールは既存のアプリケーションのポリシーとタスクを作成します。

ポリシーとタスクを作成するアプリケーションを選択します：

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

ステップ6：Kaspersky Security Center Cloud コンソールでの Kaspersky Security Network の設定

Kaspersky Security Center Cloud コンソールを試用モードで実行している場合、または仮想管理サーバーで実行している場合、このステップは省略されます。

Kaspersky Security Center Cloud コンソールの動作に関する情報を Kaspersky Security Network（KSN）ナレッジベースに転送する設定を指定します。次のいずれかのオプションをオンにします：

- **Kaspersky Security Network への参加に同意する**

  Kaspersky Security Center Cloud コンソールとクライアントデバイスにインストールされている管理対象製品は、自動的に動作情報を Kaspersky Security Network に送信します。Kaspersky Security Network への参加により、ウイルスなどの脅威に関する情報を含んだデータベースのアップデートをより迅速に入手できるため、セキュリティへの緊急の脅威にすぐに対応できます。

- **Kaspersky Security Network への参加に同意しない**

  Kaspersky Security Center Cloud コンソールと管理対象製品は、Kaspersky Security Network に対して情報を提供しません。

  このオプションをオンにすると、Kaspersky Security Network の使用がオフになります。

カスペルスキーは、Kaspersky Security Network への参加を推奨しています。

管理対象アプリケーション向けの KSN の使用に同意するかどうかの選択も表示されます。Kaspersky Security Network の使用に同意する場合、管理対象アプリケーションからカスペルスキーへデータが送信されます。Kaspersky Security Network の使用に同意しない場合、管理対象アプリケーションはカスペルスキーへデータを送信しません。アプリケーションのポリシーで後から設定を変更できます。

［**次へ**］をクリックして先に進みます。

ステップ7： 保護の初期設定の作成

作成されたポリシーとタスクのリストを確認できます。

ポリシーとタスクの作成が完了するのを待ってから、［**次へ**］をクリックして進みます。ウィザードの最後のページで、［**終了**］をクリックして終了します。

Kaspersky Security Center Cloud コンソールを使用したネットワークセグメントのポーリング

AWS API ツール、Azure API ツールまたは Google API ツールを使用した、クラウドセグメントに対する定期的なポーリングによって、ネットワーク構造とそのネットワーク内のデバイスに関する情報を受信します。Kaspersky Security Center Cloud コンソールは、この情報を使用して、［未割り当てデバイス］フォルダーと［管理対象デバイス］フォルダーの内容を更新します。デバイスが管理グループに自動的に移動するように設定している場合、検出されたデバイスは管理グループに含まれます。

クラウドセグメントのポーリングを許可するには、対応する権限を IAM ユーザーアカウント（AWS の場合）、アプリケーション ID とパスワード（Azure の場合）、あるいは Google クライアントのメール、Google プロジェクト ID および秘密鍵（Google Cloud の場合）によって付与する必要があります。

各クラウドセグメント用に接続を追加したり削除したりできます。また、各クラウドセグメントのポーリングスケジュールを設定することもできます。

Kaspersky Security Center Cloud コンソールを使用したクラウドセグメントのポーリングに使用する接続の追加

利用可能な接続のリストにクラウドセグメントのポーリングに使用する接続を追加するには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**クラウド**］の順に選択します。
2. 表示されたウィンドウで［**プロパティ**］をクリックします。
3. 表示されたウィンドウの［**設定**］で、［**追加**］をクリックします。
   ［**クラウドセグメントの設定**］ウィンドウが表示されます。
4. クラウドセグメントのポーリングに使用する接続について、クラウド環境の名前を指定します：

- **クラウド環境**

  Kaspersky Security Center Cloud コンソールを導入するクラウド環境を選択します：AWS、Azure、または Google Cloud。

  複数のクラウド環境を使用する場合は、1つの環境を選択してもう一度ウィザードを実行します。

- **接続名**

  接続の名前を入力します。名前を 256 文字以上にすることはできません。Unicode 文字のみを使用できます。

  この名前はクラウドデバイスの管理グループの名前としても使用されます。

  複数のクラウド環境を使用する予定の場合は、たとえば「Azure Segment」「AWS Segment」「Google Segment」のように、環境の名前を接続名に含めることを検討してください。

5. 認証情報を入力し、指定したクラウド環境での認証を受信します。

- AWS を選択した場合は、次を指定してください：
  - **アクセスキーの ID**

    IAM アクセスキーの ID（英数字の並び）：IAM ユーザーアカウント作成時に受け取ったキーの ID です。

    このフィールドは、認証のために AWS IAM アクセスキーを選択すると使用可能になります。

  - **秘密鍵**

    IAM ユーザーアカウント作成時にアクセスキーの ID と一緒に受け取った秘密鍵です。

    秘密鍵の文字はアスタリスクで表示されます。秘密鍵を入力し始めると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを必要な間だけ押し続けます。

    このフィールドは、認証のために AWS IAM アクセスキーを選択すると使用可能になります。

    入力した文字を表示するには、［**表示**］を押し続けます。

- Azure を選択した場合は、次の設定を指定してください：
  - **Azure アプリケーション ID**

    Azure ポータルで作成したアプリケーション ID です。

    ポーリングやその他の目的で使用する Azure アプリケーション ID を 1 つだけ指定できます。別の Azure セグメントでポーリングを実行する場合は、既存の Azure 接続を事前に削除する必要があります。

  - **Azure サブスクリプション ID**

    Azure ポータルで作成したサブスクリプションです。

  - **Azure アプリケーションパスワード**

    アプリケーション ID の作成時に取得したアプリケーション ID のパスワードです。

    パスワードの文字はアスタリスクで表示されます。パスワードの入力を開始すると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを押し続けます。

    入力した文字を表示するには、［**表示**］を押し続けます。

  - **Azure ストレージアカウント名**

    Kaspersky Security Center Cloud コンソールで使用するために作成した Azure ストレージアカウントの名前です。

  - **Azure ストレージのアクセスキー**

パスワード（アクセスキー）は、Kaspersky Security Center Cloud コンソールで使用する Azure ストレージアカウントの作成時に取得したものです。

キーは、Azure ストレージアカウントの概要セクションのアクセスキーに関するサブセクションで確認できます。

入力した文字を表示するには、［**表示**］を押し続けます。

Google Cloud を選択した場合は、次の設定を指定してください：

- **クライアントメールアドレス**

  クライアントのメールアドレスは、Google Cloud でプロジェクトの登録に使用したメールアドレスです。

- **プロジェクト ID**

  プロジェクト ID は、Google Cloud でプロジェクトの登録時に取得した ID です。

- **秘密鍵**

  秘密鍵は、Google Cloud でプロジェクトの登録時に秘密鍵として取得した文字列です。間違えないように、この文字列をコピーして貼り付けることを検討してください。

  入力した文字を表示するには、［**表示**］を押し続けます。

6. 必要に応じて、［**ポーリングのスケジュールを設定する**］をクリックし、既定の設定を変更します。

この接続は本製品の設定に保存されます。

追加したクラウドセグメントが初めてポーリングされた後、このセグメントに対応するサブグループが［**管理対象デバイス**］の［**クラウド**］管理グループに表示されます。

誤った資格情報を指定した場合、クラウドセグメントのポーリング中、インスタンスは検出されず、新しいサブグループは［**管理対象デバイス**］の［**クラウド**］管理グループに表示されません。

クラウドセグメントのポーリングに使用した接続を削除する

特定のクラウドセグメントをポーリングする必要がなくなった場合、利用可能な接続リストから、そのセグメントに対応する接続を削除できます。また、クラウドセグメントをポーリングするための権限が別の認証情報を持つ IAM ユーザーに移された場合にも、接続を削除できます。

接続を削除するには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**クラウド**］の順に選択します。
2. 表示されたウィンドウで［**プロパティ**］をクリックします。

3. 表示された［**設定**］ウィンドウで、削除するセグメントの名前をクリックします。

4. ［**削除**］をクリックします。

5. 表示されたウィンドウで、［OK］をクリックして処理を確定します。

接続が削除されます。この接続と対応しているクラウドセグメント内のデバイスが、管理グループから自動的に削除されます。

Kaspersky Security Center Cloud コンソールを使用したポーリングスケジュールの設定

クラウドセグメントのポーリングは、スケジュールに従って実行されます。ポーリングの頻度が設定可能です。

ポーリングの頻度は、クラウド環境設定ウィザードで 5 分に自動で設定されています。この値はいつでも変更でき、別のスケジュールを設定することができます。ポーリングの実行を 5 分間隔より多い頻度に設定しないでください。API 操作にエラーが生じる可能性があります。

クラウドセグメントのポーリングスケジュールを設定するには：

1. メインメニューで、［**検出と製品の導入**］→［**検出**］→［**クラウド**］の順に選択します。

2. 表示されたウィンドウで［**プロパティ**］をクリックします。

3. 表示された［**設定**］ウィンドウで、ポーリングスケジュールを設定するセグメントの名前をクリックします。
［**クラウドセグメントの設定**］ウィンドウが表示されます。

4. ［**クラウドセグメントの設定**］ウィンドウで、［**ポーリングのスケジュールを設定する**］をクリックします。
［**スケジュール**］ウィンドウが表示されます。

5. ［**スケジュール**］ウィンドウで、次の設定を指定します：

- **実行予定**
ポーリングスケジュールのオプション：
  - **N 日ごと**
  指定した日時から、日単位で指定した間隔ごとにポーリングを定期的に実行します。
  既定では、現在のシステム日時から、1 日ごとにポーリングが実行されます。
  - **N 分ごと**
  指定した時刻から、分単位で指定した間隔ごとにポーリングを定期的に実行します。
  既定では、現在のシステム時刻から、5 分ごとにポーリングが実行されます。
  - **曜日ごと**

指定した曜日（複数可）の指定した時刻にポーリングを定期的に実行します。
既定では、毎週金曜日の午後 6 時にポーリングが実行されます。

- **毎月、選択した週の指定日**

  毎月、指定した週・曜日の指定した時刻にポーリングを定期的に実行します。
  既定では、月内のいかなる日付も選択されておらず、開始時刻は午後 6 時です。

- **開始までの間隔（日）**

  N に相当する分または日数を指定します。

- **開始時刻**

  初回のポーリングを開始する時間を指定します。

- **未実行のタスクを実行する**

  ポーリングがスケジュールされている時間にワークスペースを使用できない場合、Kaspersky Security Center Cloud コンソールは、ワークスペースが再び使用可能になった直後に、またはポーリングの次回のスケジュールまで待機して、ポーリングを開始できます。

  このオプションをオンにすると、Kaspersky Security Center Cloud コンソールはワークスペースが再び使用可能になった直後にポーリングを開始します。

  このオプションをオフにすると、Kaspersky Security Center Cloud コンソールはポーリングの次回のスケジュールまでポーリングの実行を待機します。

  既定では、このオプションはオンです。

6. ［**保存**］をクリックして変更内容を保存します。

セグメントのポーリングスケジュールが設定され保存されます。

Kaspersky Security Center Cloud コンソールを使用したクラウドセグメントのポーリング結果の表示

クラウドセグメントのポーリング結果を確認できます。管理サーバーの管理対象であるクラウドデバイスのリストを表示して確認します。

クラウドセグメントのポーリング結果を表示するには：

メインメニューで、［**検出と製品の導入**］→［**検出**］→［**クラウド**］の順に選択します。

ポーリング可能なクラウドセグメントが表示されます。

Kaspersky Security Center Cloud コンソールを使用したクラウドデバイスのプロパティの表示

各クラウドデバイスのプロパティを表示できます。

クラウドデバイスのプロパティを表示するには：

1. メインメニューで、［**アセット（デバイス）**］→［**管理対象デバイス**］の順に移動します。
2. プロパティを表示するデバイスの名前をクリックします：
   プロパティウィンドウの［**全般**］セクションが表示されます。
3. 特定のクラウドデバイスのプロパティを表示する場合は、［**システム**］セクションをプロパティウィンドウで選択します。
   デバイスのクラウドプラットフォームに応じたプロパティが表示されます。
   AWS のデバイスでは、次のプロパティが表示されます：
   - **API を使用して検出されたデバイス**（値：**AWS**）
   - **クラウドのリージョン**
   - **クラウドの VPC**
   - **クラウドのアベイラビリティーゾーン**
   - **クラウドのサブネット**
   - **クラウドのプレイスメントグループ**（AWS API を使用して検出された Amazon EC2 インスタンスの場合のみ。それ以外の場合、この項目は表示されません）

   Azure のデバイスでは、次のプロパティが表示されます：
   - **API を使用して検出されたデバイス**（値：**Microsoft Azure**）
   - **クラウドのリージョン**
   - **クラウドのサブネット**

   Google Cloud のデバイスでは、次のプロパティが表示されます：
   - **API を使用して検出されたデバイス**（値：**Google Cloud**）
   - **クラウドのリージョン**
   - **クラウドの VPC**
   - **クラウドのアベイラビリティーゾーン**
   - **クラウドのサブネット**

クラウドとの同期：移動ルールの設定

クラウド環境設定ウィザードの処理中に、［クラウドと同期］ルールが自動的に作成されます。このルールにより、各ポーリング中に見つかったデバイスが［未割り当てデバイス］グループから［管理対象デバイス］の［クラウド］グループに自動的に移動されるため、デバイスを一元管理することが可能になります。既定では、ルールは作成後にアクティブになります。ルールはいつでも無効にしたり、実行したりすることができます。

［クラウドと同期］ルールのプロパティを変更する、またはルールを実行するには：

1. メインメニューで、［**検出と製品の導入**］→［**導入と割り当て**］→［**移動ルール**］の順に移動します。
   移動ルールのリストが表示されます。
2. 移動ルールのリストで、［**クラウドと同期**］を選択します。
   ルールのプロパティウィンドウが開きます。
3. 必要に応じて、［**クラウドセグメント**］タブの［**ルールの条件**］タブで次の設定を指定します：

- **デバイスがクラウドセグメント内にある**

  選択したクラウドセグメント内にあるデバイスにのみルールが適用されるようになります。オフにすると、検出されたすべてのデバイスにルールが適用されます。

  既定では、このオプションがオンです。

- **子オブジェクトも含む**

  選択されたセグメント内およびネストされたすべてのクラウドサブセクション内の全デバイスにルールが適用されるようになります。オフにすると、ルートセグメント内にあるデバイスにのみルールが適用されます。

  既定では、このオプションがオンです。

- **デバイスをネストされたオブジェクトから対応するサブグループに移動する**

  このオプションをオンにすると、ネストされたオブジェクトのデバイスがその構造に対応するサブグループに自動的に移動します。

  このオプションをオフにすると、ネストされたオブジェクトのデバイスがクラウドサブグループのルートに移動し、ルートより下の分岐は行われません。

  既定では、このオプションはオンです。

- **新しく検出されたデバイスの配置階層に対応するサブグループを作成する**

このオプションをオンにすると、デバイスが含まれるセクションに対応するサブグループが［**管理対象デバイス**］の［**クラウド**］グループの階層構造にない場合は、Kaspersky Security Center Cloud コンソールで対応するサブグループが作成されます。たとえば、デバイスの検索中に新しいサブネットが検出された場合、同じ名前のグループが［**管理対象デバイス**］の［**クラウド**］グループの下に新規に作成されます。

このオプションをオフにすると、Kaspersky Security Center Cloud コンソールで新しいサブグループは作成されません。たとえば、ネットワークのポーリング中に新しいサブネットが検出された場合、［**管理対象デバイス**］の［**クラウド**］グループにサブネットと同じ名前のグループが新規に作成されることはなく、サブネットに含まれていたデバイスは［**管理対象デバイス**］の［**クラウド**］グループに移動されます。

既定では、このオプションはオンです。

- **クラウドセグメントで何も検出されなかったサブグループを削除する**

  このチェックボックスをオンにすると、既存のクラウドオブジェクトのセクションに対応していないすべてのサブグループがクラウドグループから削除されます。

  このオプションをオフにすると、既存のクラウドオブジェクトのセクションに対応しないサブグループもすべて保持されます。

  既定では、このオプションはオンです。

［**管理グループをクラウドの階層構造と同期**］をクラウド環境設定ウィザードを使用して有効にすると、［**クラウドと同期**］ルールが［**新しく検出されたデバイスの配置階層に対応するサブグループを作成する**］および［**クラウドセグメントで何も検出されなかったサブグループを削除する**］が有効な状態で作成されます。

［**管理グループをクラウドの階層構造と同期**］を有効にしなかった場合、［**クラウドと同期**］ルールが、これらのオプションが無効な（クリアされた）状態で作成されます。お使いの Kaspersky Security Center Cloud コンソールで、［**管理対象デバイス**］の［**クラウド**］サブグループ内にあるサブグループの構造とクラウドセグメントの構造が一致する必要がある場合、［**新しく検出されたデバイスの配置階層に対応するサブグループを作成する**］と［**クラウドセグメントで何も検出されなかったサブグループを削除する**］をオンにして、ルールを実行します。

4. ［**API を使用して検出されたデバイス**］から、次のいずれかの値を選択します：

   - ［**いいえ**］。デバイスは AWS API、Azure API、Google API のいずれでも検出できません。これはデバイスがクラウド環境外にあるか、クラウド環境内にあるが何らかの理由により API では検出できないことを意味します。
   - **AWS**：AWS API を使用して検出されたデバイスで、これはデバイスが間違いなく AWS クラウド環境にあることを意味します。
   - **Azure**：Azure API を使用して検出されたデバイスで、これはデバイスが間違いなく Azure クラウド環境にあることを意味します。
   - **Google Cloud**:Google API を使用して検出されたデバイスで、これはデバイスが間違いなく Google Cloud 環境にあることを意味します。
   - 値なし：この基準は適用できません。

5. 必要に応じて、他のセクションで他のルールのプロパティを設定します。

移動ルールが設定されます。

Azure 仮想マシンへの製品のリモートインストール

Microsoft Azure 仮想マシンに製品をインストールするには、有効なライセンスが必要です。

Kaspersky Security Center Cloud コンソールでは次のシナリオがサポートされます：

- クライアントデバイスが Azure API によって検出され、製品のインストールも API によって実行される。Azure API を使用すると、次のアプリケーションのみをインストールできます：
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- クライアントデバイスが Azure API によって検出され、製品のインストールはディストリビューションポイントによって実行されるか、ディストリビューションポイントがない場合は、スタンドアロンインストールパッケージを使用して手動で実行される。この方法では、Kaspersky Security Center Cloud コンソールでサポートされている任意の製品をインストールできます。

Azure 仮想マシンで製品のリモートインストールタスクを作成するには：

1. メインメニューで、［**アセット（デバイス）**］→［**タスク**］の順に移動します。
2. ［**追加**］をクリックします。
   新規タスクウィザードが起動します。
3. ウィザードの指示に従います：
   a. ［**アプリケーションのリモートインストール**］をタスク種別として選択します。
   b. ［**インストールパッケージ**］ページで、［**Microsoft Azure API によるリモートインストール**］を選択します。
   c. デバイスにアクセスするアカウントを選択する際は、既存の Azure アカウントを使用するか、［**追加**］をクリックして Azure アカウントの資格情報を入力します：
      - **Azure アカウント名**
        指定する資格情報の任意の名前を入力します。タスクを実行するアカウントのリストにこの名前が表示されます。
      - **Azure アプリケーション ID**
        Azure ポータルで作成したアプリケーション ID です。
        ポーリングやその他の目的で使用する Azure アプリケーション ID を 1 つだけ指定できます。別の Azure セグメントでポーリングを実行する場合は、既存の Azure 接続を事前に削除する必要があります。
      - **Azure アプリケーションパスワード**

アプリケーション ID の作成時に取得したアプリケーション ID のパスワードです。

パスワードの文字はアスタリスクで表示されます。パスワードの入力を開始すると、［**入力した文字を表示する**］というボタンが表示されます。入力した文字を確認するには、このボタンを押し続けます。

d. ［**管理対象デバイス**］の［**クラウド**］グループから目的のデバイスを選択します。

ウィザードが完了すると、アプリケーションのリモートインストール用のタスクがタスクのリストに表示されます。

Kaspersky Security Center Cloud コンソールインターフェイスの言語の変更

Kaspersky Security Center Cloud コンソールインターフェースの言語を選択できます。

インターフェース言語を変更するには：

1. メインメニューで、［**設定**］→［**言語**］の順にクリックします。
2. サポートされているローカリゼーション言語のいずれかを選択します。

テクニカルサポートへの問い合わせ

このセクションでは、サポートを受ける方法および提供条件について説明します。

テクニカルサポートのご利用方法

Kaspersky Security Center Cloud コンソールのドキュメントや Kaspersky Security Center Cloud コンソールの情報源で問題の解決法が見つからない場合は、カスペルスキーテクニカルサポートに問い合わせてください。テクニカルサポート担当者が、Kaspersky Security Center Cloud コンソールのインストール方法や使用方法についてのお問い合わせに回答いたします。

カスペルスキーによる Kaspersky Security Center Cloud コンソールのサポートは、本製品のライフサイクル期間中に提供されます（製品のサポートライフサイクルページを参照）。テクニカルサポートに連絡する前に、サポートサービス規約をご確認ください。

テクニカルサポートサービスの内容については、サポートセンターのご案内を参照してください。

- テクニカルサポートサイトにアクセスする
- カスペルスキーカンパニーアカウントからテクニカルサポートへリクエストを送信

カスペルスキーカンパニーアカウントによるテクニカルサポート

カスペルスキーカンパニーアカウントは、カスペルスキー製品を使用する法人向けのポータルです。このポータルは、オンラインリクエストを通じてユーザーとカスペルスキーのエキスパートの交流を促進するよう設計されています。また、オンラインリクエストの進捗をモニターでき、リクエストの履歴を保存することができます。

カスペルスキーカンパニーアカウントでは、シングルアカウントで組織の全従業員を登録できます。シングルアカウントによって、登録従業員からカスペルスキーまでのオンラインリクエストを一元管理でき、カスペルスキーカンパニーアカウントを介して従業員の権限を管理することもできます。

カスペルスキーカンパニーアカウントのポータルは、次の言語で利用できます：

- 英語
- スペイン語
- イタリア語
- ドイツ語
- ポーランド語
- ポルトガル語
- ロシア語
- フランス語

- 日本語

カスペルスキーカンパニーアカウントについて詳しくは、テクニカルサポートサイトをご覧ください。

カスペルスキーのテクニカルサポートに必要な情報

カスペルスキーのテクニカルサポートに問い合わせる時に、次の情報を提供するよう求められる場合があります：

- Kaspersky Security Center Cloud コンソールに関する一般的な情報
- ワークスペース ID
- ライセンス情報
- インストール済みアプリケーションの数
- テナント ID とステータス

この情報は、［**アカウントメニュー**］→［**テクニカルサポート**］セクションで確認できます。この情報をコピーして共有し、問題を解決するためのサポートを依頼してください。

製品の情報源

カスペルスキーの Web サイトの Kaspersky Security Center Cloud コンソールのページ

Kaspersky Security Center Cloud コンソールのページで、製品とその機能に関する一般情報を見ることができます。

ナレッジベースの Kaspersky Security Center Cloud コンソールのページ

カスペルスキーのテクニカルサポートサイトに*ナレッジベース*のセクションがあります。

ナレッジベースの Kaspersky Security Center Cloud コンソールのページに、製品の購入、インストール、使用の方法について、役立つ情報、推奨事項、および FAQ への回答が掲載されています。

ナレッジベースの記事では、本製品だけではなく他のカスペルスキー製品に関連した質問にも回答しています。ナレッジベースの記事に、テクニカルサポートからのニュースが掲載されることもあります。

カスペルスキー製品の Web コミュニティの利用

特に緊急の対応が必要ではない場合は、カスペルスキーのフォーラムをご利用ください。ここでは、カスペルスキーのエキスパートやカスペルスキー製品のユーザーが、様々なトピックで意見交換しています。

フォーラムでは、これまでに公開されたトピックの閲覧、コメントの書き込み、新しいトピックの作成が可能です。

> オンラインの情報源を使用するには、インターネット接続が必要です。

問題の解決策が見つからない場合は、カスペルスキーのテクニカルサポートまでお問い合わせください。

既知の問題

Kaspersky Security Center Cloud コンソールには、本製品の動作には大きな影響を与えない複数の制限があります：

- *ディストリビューションポイントのリポジトリにアップデートをダウンロード*または*アップデート検証*タスクをインポートすると、**タスクが割り当てられるデバイスを選択する**オプションが有効になります。これらのタスクは、デバイスの抽出または特定のデバイスに割り当てることはできません。*ディストリビューションポイントのリポジトリにアップデートをダウンロードする*か、特定のデバイスに*アップデート検証*タスクを割り当てると、タスクは正しくインポートされません。

- Linux デバイスの*インベントリスキャン*タスクが完了した後、受信したファイルを分析のためにカスペルスキーに送信しようとすると、エラーが返されます。

- Active Directory フェデレーションサービス（ADFS）を使用して Kaspersky Security Center Cloud コンソールにログインしようとして、必要な権限がない場合も、Kaspersky Security Center Cloud コンソールは、権限がないことをユーザーに警告するのではなく、「資格情報が無効です」というエラーを返します。

- デバイスの管理タスクは、macOS を実行しているデバイスでは正常に動作しません。

- リモート診断ウィンドウで［**ファイル全体をダウンロード**］をクリックしても、正しくダウンロードされない場合があります。

Amazon EC2 インスタンス

Amazon Web Services を使用し、AMI イメージに基づいて作成された仮想マシン。

AMI（Amazon Machine Image）

仮想マシンを実行する場合に必要なソフトウェア設定が含まれるテンプレート。単一の AMI に基づいて複数のインスタンスを作成できます。

AWS IAM アクセスキー

ライセンス ID（「AKIAIOSFODNN7EXAMPLE」など）と秘密鍵（「wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY」など）で構成される組み合わせ。このペアは IAM ユーザーに属し、AWS サービスへのアクセス権限を取得するために使用されます。

AWS アプリケーションプログラムインターフェイス（AWS API）

Kaspersky Security Center Cloud コンソールによって使用され AWS プラットフォームのアプリケーションプログラミングインターフェイス。具体的には、クラウドセグメントのポーリングには AWS API ツールが使用されます。

AWS 管理コンソール

AWS リソースの表示と管理を行える Web インターフェイス。AWS 管理コンソールは Web 上（https://aws.amazon.com/console/）で使用できます。

HTTPS

データ転送用のセキュアプロトコル。ブラウザーと Web サーバーの通信に暗号を使用します。HTTPS は、企業データや財務データなどの制限付き情報へのアクセスに使用されます。

IAM ユーザー

AWS サービスのユーザー。IAM ユーザーには、クラウドセグメントポーリングを実行する権限があります。

IAM ロール

AWS ベースのサービスに対してリクエストを実行する権限の集合。IAM ロールは、特定のユーザーやグループとリンクしておらず、AWS IAM アクセスキーを使用せずにアクセス権を付与します。IAM ユーザー、EC2 インスタンス、AWS ベースのアプリケーションまたはサービスに IAM ロールを割り当てることができます。

ID およびアクセス管理（IAM）

他の AWS サービスとリソースへのユーザーアクセス管理を有効にする AWS サービス。

JavaScript

Web ページのパフォーマンスを拡張するプログラミング言語。JavaScript を使用して作成された Web ページでは、Web サーバーからの新しいデータでブラウザーの表示をアップデートすることなく、インターフェイス要素の表示を変更したり、新しいウィンドウを表示したりできます。JavaScript を使用して作成されたページを表示するには、ブラウザーの設定で JavaScript のサポートを有効にします。

Kaspersky Private Security Network（KPSN）

Kaspersky Private Security Network は、カスペルスキー製品がインストールされたデバイスのユーザーがデバイスから Kaspersky Security Network にデータを送信することなく、Kaspersky Security Network の評価データベースとその他の統計データにアクセスできるようにするソリューションです。Kaspersky Private Security Network は、次のいずれかの理由で Kaspersky Security Network にアクセスできない法人ユーザーの方を対象として開発されています：

- デバイスがインターネットに接続されていない。
- 国外や企業 LAN の外へのデータの送信が、法律または社内のセキュリティポリシーで禁止されている。

Kaspersky Security Center Cloud コンソールのアカウント

アカウントの追加と削除、セキュリティプロファイル（セキュリティポリシー）の設定など、Kaspersky Security Center Cloud コンソールを設定するために必要なユーザーアカウント。このアカウントで、マイ カスペルスキーサービス を使用できます。このアカウントは、Kaspersky Security Center Cloud コンソールの使用の開始時に作成します。

Kaspersky Security Center Cloud コンソールのオペレーター

Kaspersky Security Center Cloud コンソールシステムで管理している保護システムのステータスと動作を監視するユーザー。

Kaspersky Security Center Cloud コンソールの管理者

Kaspersky Security Center Cloud コンソールシステムを使用して、アプリケーションの動作をリモートで一元管理する担当者。

Kaspersky Security Network（KSN）

ファイル、Web リソース、ソフトウェアの評価情報が定期的に更新されるカスペルスキーのデータベースへのアクセスを提供するクラウドサービスの基盤。KSN を使用することで、カスペルスキー製品がより迅速に新しい脅威に対応します。また、一部の保護コンポーネントのパフォーマンスが向上し、誤検知の可能性が減ります。

SSL

インターネットおよびローカルネットワークで使用されるデータ暗号化プロトコル。Secure Sockets Layer（SSL）は Web アプリケーションで使用され、クライアントとサーバーの間のセキュアな接続を確立します。

UEFI 保護デバイス

BIOS レベルで Kaspersky Anti-Virus for UEFI が統合されているデバイス。統合された保護により、システムが起動した瞬間からデバイスのセキュリティを確保し、同時に、ソフトウェアが統合されていないデバイスでの保護が、セキュリティ製品の起動後にのみ機能し始めるようにします。

Web 管理プラグイン

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

アップデート

カスペルスキーのアップデートサーバーから取得した新しいファイル（定義データベースまたはソフトウェアモジュール）を置換または追加する処理。

アプリケーションタグ

アプリケーションのグループ化または検索に使用できるサードパーティアプリケーションのラベル。アプリケーションに割り当てたタグは、デバイスの抽出の条件として使用できます。

アプリケーションの一元管理

Kaspersky Security Center Cloud コンソールが備える管理サービスを使用した、アプリケーションのリモート管理。

アプリケーションの直接管理

ローカルインターフェイスを使用したアプリケーション管理。

イベントの重要度

カスペルスキー製品の動作時に発生したイベントのプロパティ。次のレベルに分かれています：

- 緊急
- 機能エラー
- 警告
- 情報

イベント発生の状況によって、同じ種別のイベントで重要度が異なる場合があります。

イベントリポジトリ

管理サーバーデータベースのうち、Kaspersky Security Center Cloud コンソールで発生するイベントに関する情報の保管専用の領域です。

インストールパッケージ

カスペルスキー製品のリモートインストール用に作成されるファイルセット。リモート管理システム Kaspersky Security Center Cloud コンソールを使用して作成します。インストールパッケージには、アプリケーションをインストールし、インストール後にすぐに実行させるのに必要な設定の範囲が含まれます。設定は、アプリケーションの既定値になります。インストールパッケージは、配布キットに含まれる拡張子が kpd および kud のファイルを使用して作成されます。

ウイルスアウトブレイク

デバイスをウイルスに感染させるための、一連の意図的な試み。

ウイルスアクティビティのしきい値

指定した種別のイベントに関して設定する、制限時間内で許容するイベント発生数の上限。この値を超過すると、ウイルスアクティビティが増加してウイルスアウトブレイクの脅威があると判断されます。ウイルスアウトブレイクの脅威に対してタイムリーな対応が可能になるため、ウイルスアウトブレイクの発生中に重要な役割を果たします。

隔離

感染の可能性があるファイルおよび検知時点で駆除できないファイルを格納する特別なリポジトリです。

カスペルスキーのアップデートサーバー

カスペルスキーの HTTP サーバーで、カスペルスキー製品はこれらのサーバーから定義データベースやソフトウェアモジュールのアップデートをダウンロードします。

仮想管理サーバー

クライアント組織のネットワークの保護システムを管理する Kaspersky Security Center Cloud コンソールのコンポーネント。

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

- 仮想管理サーバーはセカンダリ管理サーバーとしてのみ動作できます。
- 仮想管理サーバーでは、セカンダリ管理サーバー（仮想サーバーを含む）の作成がサポートされていません。

管理グループ

機能およびインストールされているカスペルスキー製品に応じてデバイスをまとめたグループ。複数のデバイスを1つのグループとして管理できます。1つのグループに下位のグループとして他のグループを含めることができます。グループにインストールされている各アプリケーションに対してグループポリシーやグループタスクを作成することができます。

管理サーバー

企業ネットワークにインストールされているすべてのカスペルスキー製品に関する情報を一元的に保管する Kaspersky Security Center Cloud コンソールのコンポーネント。製品の管理にも使用できます。

管理対象デバイス

ネットワークエージェントがインストールされているコンピューター、またはカスペルスキーのセキュリティ製品がインストールされているモバイルデバイス。

強制インストール

カスペルスキー製品のリモートインストール方法。指定したクライアントデバイスに、ソフトウェアをインストールできます。強制インストールでは、タスクで使用されるアカウントに、クライアントデバイス上でアプリケーションをリモート実行する権限が必要です。この方法は、Microsoft Windows オペレーティングシステムが実行され、この機能をサポートするデバイスに製品をインストールする場合に推奨されます。

グループタスク

管理グループに定義され、そのグループ内のすべてのクライアントデバイスで実行されるタスク。

現在のライセンス

アプリケーションによって現在使用されているライセンス。

互換性がないアプリケーション

サードパーティ製のアンチウイルス製品、または Kaspersky Security Center Cloud コンソールを使用した管理に対応していないカスペルスキー製品。

脆弱性

マルウェアの開発者がオペレーティングシステムやプログラムに侵入してその完全性を損なわせるために利用する可能性のあるオペレーティングシステムまたはプログラムの欠陥。オペレーティングシステムに多くの脆弱性があると、機能の信頼性が損なわれます。侵入したウイルスによってオペレーティングシステム自体またはインストールされているアプリケーションで障害が引き起こされる可能性があるためです。

接続ゲートウェイ

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

タスク

カスペルスキー製品によって実行される機能はタスクとして実装されます。ファイルのリアルタイム保護、デバイスの完全スキャン、定義データベースのアップデートなどのタスクがあります。

タスク設定

各タスク種別に固有のアプリケーション設定です。

追加の定額制サービスのライセンス

製品を使用する権限を認定する、現在使用されていないライセンス。

定義データベース

定義データベースの公開時点で、カスペルスキーが把握しているコンピューターセキュリティへの脅威についての情報を含むデータベース。定義データベース内のエントリによって、スキャンしているオブジェクトで悪意のあるコードを検知できます。定義データベースはカスペルスキーのエキスパートにより作成され、1時間ごとにアップデートされます。

ディストリビューションポイント

ネットワークエージェントがインストールされており、アップデートの配信、ネットワークポーリング、アプリケーションのリモートインストール、管理グループやブロードキャストドメインでのコンピューター情報の取得に使用されるコンピューター。管理者が適切なデバイスを選択し、ディストリビューションポイントを手動で割り当てます。

適用可能なアップデート

カスペルスキーのソフトウェアモジュールに関する一連のアップデート（一定期間に蓄積された重大なアップデートを含む）。

デバイスの所有者

デバイスで特定の操作が必要になった際に管理者が連絡できるユーザー。

デバイスのタグ

デバイスのグループ化、説明、または検索に使用することができるデバイスのラベルです。

特定のデバイスに対するタスク

任意の管理グループに属する一連のクライアントデバイスに割り当てられ、それらのデバイスで実行されるタスク。

認証エージェント

起動可能なハードディスクの暗号化後に、暗号化されたハードディスクへのアクセス権を取得してオペレーティングシステムを読み込むための認証手順を完了することができるインターフェイス。

ネットワークエージェント

管理サーバーと特定のネットワークノード（ワークステーションまたはサーバー）にインストールされているカスペルスキー製品との間のやり取りを受け持つ Kaspersky Security Center Cloud コンソールのコンポーネント。このコンポーネントは、カスペルスキーの Microsoft® Windows® 用の製品に共通した機能です。Unix 系の OS および macOS 用には、それぞれ異なるバージョンのネットワークエージェントがあります。

ネットワークのアンチウイルスによる保護

組織のネットワークにウイルスやスパムが侵入する危険性を軽減し、ネットワーク攻撃やフィッシングなどの脅威を防ぐ一連の技術的、組織的対策。ネットワークセキュリティは、セキュリティ製品およびサービスを使用して企業のセキュリティポリシーに従い、正しく適用することで向上します。

ネットワーク保護ステータス

企業ネットワーク内のデバイスのセキュリティレベルを定義する現在の保護ステータス。ネットワーク保護ステータスには、インストール済みセキュリティ製品、ライセンスの使用、検知された脅威の数と種類のような要因を含みます。

パッチの重要度

パッチの属性の1つ。Microsoft のパッチおよびサードパーティのパッチには、5 つの重要度があります：

- 緊急
- 高
- 中
- 低
- 不明

サードパーティのパッチまたは Microsoft のパッチの重要度は、パッチが修正する脆弱性のうち、最も高い重要度によって決定されます。

非武装地帯（DMZ）

非武装地帯は、サーバーを含むローカルネットワークのセグメントで、グローバル Web からの要求に応えます。組織のローカルネットワークのセキュリティを確保するために、非武装地帯から LAN へのアクセスがファイアウォールで保護されます。

復元

隔離またはバックアップ内のオブジェクトを、隔離、感染駆除、削除される前の元のフォルダーまたはユーザーが指定したフォルダーに移動すること。

ブロードキャストドメイン

OSI 基本参照モデル（Open Systems Interconnection Basic Refernce Model）のレベルにおける、ブロードキャストチャネルを使用してすべてのノードがデータ交換を行えるネットワークの論理領域。

プログラム設定

あらゆる種類のタスクに共通していて、アプリケーションの動作全体を管理するアプリケーション設定（アプリケーションパフォーマンス設定、レポート設定、バックアップ設定など）。

ホーム管理サーバー

ネットワークエージェントのインストール中に指定した管理サーバー。ホーム管理サーバーは、ネットワークエージェントの接続プロファイルを設定するために使用できます。

保護ステータス

コンピューターのセキュリティレベルを定義する現在の保護ステータス。

ポリシー

ポリシーは、アプリケーションの設定を決定するとともに、管理グループ内のコンピューターにインストールされたアプリケーションを設定する権限を管理します。各アプリケーションについて個別にポリシーを作成する必要があります。各管理グループのコンピューターにインストールされたアプリケーションについて複数のポリシーを作成できますが、各管理グループ内で1つのアプリケーションについて一度に適用されるポリシーは1つだけです。

ポリシーのプロファイル

ポリシー設定の名前付きサブセットです。このサブセットはポリシーとともに対象デバイスに配信され、プロファイルの有効化条件と呼ばれる特定の条件下でポリシーを補完する機能を果たします。

ライセンス情報ファイル

拡張子が「KEY」のファイル。このファイルを使用することで、カスペルスキー製品を試用版または製品版ライセンスで使用できます。

ライセンスの有効期間

ユーザーがアプリケーションの機能および追加サービスへのアクセス権を有する期間。使用できるサービスは、ライセンスの種別によって異なります。

リモートインストール

Kaspersky Security Center Cloud コンソールを使用した、カスペルスキー製品のインストール。

ローカルインストール

組織のネットワーク上のデバイスにセキュリティ製品をインストールするには、セキュリティ製品の配布パッケージからインストールを手動で開始する方法、またはコンピューターに事前にダウンロードしておいた公開済みインストールパッケージを手動で起動する方法があります。

ローカルタスク

1台のクライアントコンピューターを対象として定義、実行されるタスク。

ワークスペース

特定の会社用に作成した Kaspersky Security Center Cloud コンソールのインスタンス。顧客がワークスペースを作成すると、会社のデバイスにインストールされているセキュリティ製品を管理するために必要なインフラストラクチャとクラウドベースの管理コンソールをカスペルスキーが作成して設定します。

サードパーティ製のコードに関する情報

サードパーティ製のコードに関する情報はファイル legal_notices.txt に記載されています。

ファイル legal_notices.txt は、Network Agent for Windows および Network Agent for Linux のインストールフォルダーにもあります。

ワークスペースで使用されているサードパーティ製のコードの詳細については、Kaspersky Endpoint Security Cloud のドキュメントを参照してください。

商標に関する通知

登録商標とサービスマークに関する権利は各所有者に帰属します。

Adobe、Acrobat、Flash、PostScript、Reader、Shockwave は Adobe の米国および他の国における登録商標または商標です。

AMD64 は、Advanced Micro Devices, Inc. の商標または登録商標です。

Amazon、Amazon EC2、Amazon Web Services、AWS および AWS Marketplace は、Amazon.com, Inc. またはその関連会社の商標です。

Apache は、Apache Software Foundation の登録商標または商標です。

Apple、App Store、AppleScript、FileVault、iPhone、iTunes、Mac、Mac OS、macOS、OS X、Safari、および QuickTime は、Apple Inc. の商標です。

Arm は、Arm Limited（またはその子会社）の米国および / またはその他の国における登録商標です。

Bluetooth の表記、マークおよびロゴは、Bluetooth SIG, Inc. に所有権があります。

Ubuntu LTS は Canonical Ltd の登録商標です。

Cisco、Cisco Jabber、IOS は、米国およびその他の国における Cisco Systems, Inc. およびその子会社の登録商標です。

Citrix および XenServer は、米国特許商標庁およびその他の国における Citrix Systems, Inc. およびその子会社の登録商標です。

Cloudflare、Cloudflare のロゴ、および Cloudflare Workers は、米国およびその他の法域における Cloudflare, Inc. の商標や登録商標です。

Corel と CorelDRAW は、カナダ、米国およびその他の国における Corel Corporation およびその子会社の商標または登録商標です。

Dropbox は、Dropbox, Inc. の商標です。

Radmin は、Famatech の登録商標です。

Firebird は、Firebird Foundation の登録商標です。

Foxit は、Foxit Corporation の登録商標です。

FreeBSD は、FreeBSD Foundation の登録商標です。

Google、Android、Chrome、Dalvik、Firebase、Google Chrome、Google Earth、Google Maps、Google Play、Google Public DNS は、Google LLC の商標です。

EulerOS は、Huawei Technologies Co., Ltd. の商標です。

Intel および Core は米国およびその他の国における Intel Corporation の商標です。

IBM および QRadar は、世界各国で International Business Machines Corporation が所有する登録商標です。

Node.js は Joyent Inc. の商標です。

Linux は、米国およびその他の国における Linus Torvalds 氏の登録商標です。

Logitech は Logitech の米国および他の国における登録商標または商標です。

Microsoft、Active Directory、ActiveSync、ActiveX、BitLocker、Excel、Hyper-V、InfoPath、Internet Explorer、Microsoft Edge、MS-DOS、MultiPoint、Office 365、OneNote、Outlook、PowerPoint、PowerShell、Segoe、Skype、SQL Server、Tahoma、Visio、Win32、Windows、Windows Azure、Windows Media、Windows Mobile、Windows Phone、Windows Server、および Windows Vista は、Microsoft グループ企業が所有する商標です。

CVE は、The MITRE Corporation の登録商標です。

Mozilla、Firefox、Thunderbird は、米国およびその他の国における Mozilla Foundation の商標です。

Novell は、米国およびその他の国における Novell Enterprises Inc. の登録商標です。

NetWare は、米国およびその他の国における Novell, Inc. の登録商標です。

Oracle、Java、JavaScript は、Oracle とその関連会社の両方またはいずれかの登録商標です。

Parallels、Parallels ロゴ、および Coherence は、Parallels International GmbH の商標または登録商標です。

Python は Python Software Foundation の登録商標または商標です。

Red Hat、Red Hat Enterprise Linux、CentOS、Fedora は、Red Hat, Inc. またはその子会社の米国および他の国における商標または登録商標です。

BlackBerry は、Research In Motion Limited の米国における登録商標であり、その他の国における登録商標または登録出願中の商標です。

SAMSUNG は、米国およびその他の国における SAMSUNG の登録商標です。

Debian は、Software in the Public Interest, Inc. の登録商標です。

Splunk は、Splunk, Inc. の米国およびその他の国における登録商標です。

SUSE は、米国およびその他の国における SUSE LLC の登録商標です。

Symbian の商標は Symbian Foundation Ltd. が所有します。

VMware、VMware vSphere、VMware Workstation は、VMware, Inc. の米国およびその他の国における商標または登録商標です。

UNIX は米国およびその他の国における登録商標で、X/Open Company Limited のライセンス契約の下で排他的に使用されています。