kaspersky

Kaspersky Endpoint Security for Linux

目次

Kaspersky Endpoint Security 12.1 for Linux

Kaspersky Endpoint Security 12.1 for Linux（「Kaspersky Endpoint Security」または「本製品」）は、Linux® OS を搭載したデバイスを、ネットワーク攻撃や詐欺などの様々な脅威から保護する仕様となっています。

このアプリケーションは、物理デバイスと仮想マシンの両方を保護することができます。Kaspersky Endpoint Security を、Kaspersky Security for Virtualization Light Agent の一部として使用して、Linux ゲスト OS を実行している仮想マシンを保護することができます。

次のアプリケーションの機能コンポーネントとタスクは、デバイスの保護と制御の主な機能を提供します：

- **ファイル脅威対策**は、ユーザーデバイスのファイルシステムの感染を防止します。*ファイル脅威対策*コンポーネントは、Kaspersky Endpoint Security の起動時に自動的に起動し、開いたり、保存したり、起動したりしたすべてのファイルをリアルタイムでスキャンします。

  次のスキャン タスクを使用して、保護されたデバイスをオンデマンドでスキャンすることもできます：

  - **マルウェアのスキャン**。このアプリケーションは、デバイスのローカルディスクにあるファイルシステムオブジェクト、および SMB や NFS プロトコルを介してアクセスされるマウントされた共有リソースにマルウェアが存在するかどうかをスキャンします。このタスクを使用して、デバイス全体のスキャンまたはオブジェクトスキャンを実行できます。

  - **簡易スキャン**：このアプリケーションは、ブートセクター、スタートアップオブジェクト、プロセスメモリ、カーネルメモリをスキャンします。

- **リムーバブルドライブのスキャン**。*リムーバブルドライブのスキャン*コンポーネントを使用すると、リムーバブルドライブのデバイスへの接続をリアルタイムで監視し、リムーバブルドライブとそのブートセクターをスキャンしてマルウェアを検出することができます。Kaspersky Endpoint Security は次のリムーバブルドライブをスキャンできます：CD、DVD、Blu-ray ディスク、フラッシュドライブ（USB モデムを含む）、外付けハードディスク、フロッピーディスク。

- **コンテナのスキャン**：*コンテナースキャン*コンポーネントを使用すると、ネームスペースと実行中のコンテナにマルウェアがないかリアルタイムでスキャンできます。Docker コンテナ管理システム、CRI-O フレームワーク、Podman ユーティリティ、runc ユーティリティとの連携がサポートされています。*コンテナースキャン*タスクを使用して、コンテナとイメージをオンデマンドでスキャンできます。

- **ウェブ脅威対策**。*ウェブ脅威対策*コンポーネントを使用すると、受信トラフィックをスキャンし、インターネットからの悪意のあるファイルのダウンロードを防止し、フィッシング、アドウェア、その他の悪意のある Web サイトをブロックすることができます。Kaspersky Endpoint Security は暗号化された接続をスキャンできます。

- **ネットワーク脅威対策**。*ネットワーク脅威対策*は、受信ネットワークトラフィックにネットワーク攻撃に特有の動作が含まれていないかどうかスキャンします。

- **ファイアウォール管理**。*ファイアウォール管理*コンポーネントを使用すると、オペレーティングシステムのファイアウォール設定を監視し、設定したネットワークパケットルールに従ってすべてのネットワークアクティビティをフィルタリングすることができます。

- **アンチクリプター**。*アンチクリプター* コンポーネントを使用すると、SMB/NFS プロトコルを介したネットワークアクセスで、ローカルディレクトリにあるファイルへのリモートデバイスの呼び出しをスキャンし、リモートの悪意のある暗号化からファイルを保護できます。

- **デバイスコントロール**。*デバイスコントロール*コンポーネントは、クライアントデバイスに搭載または接続されたデバイス（例：ハードディスク、カメラ、Wi-Fi モジュールなど）へのユーザーアクセスを管理します。これにより、外部デバイスの接続時に感染からクライアントデバイスを保護したり、データの消失や漏洩を防止したりできます。デバイスへのユーザーアクセスは、設定したアクセス体制とルールによって管理されます。

- **アプリケーションコントロール**。*アプリケーションコントロール*コンポーネントにより、ユーザーデバイス上のアプリケーションの起動を管理できます。これは、アプリケーションへのアクセスを制限することにより、デバイスの感染リスクを軽減します。アプリケーションの起動は、設定したアプリケーションコントロールルールによって制御されます。

- **インベントリ**：*インベントリ*タスクは、クライアントデバイスに保存されているすべてのアプリケーションの実行ファイルに関する情報を提供します。この情報は、アプリケーションコントロールルールを作成する際などに有用です。

- **ウェブコントロール**。*ウェブコントロール*は、Web リソースへのユーザーアクセスを制御します。これにより、トラフィックの消費を削減し、作業時間の不適切な使用を減らすことができます。ユーザーが ウェブコントロールによってアクセスが制限されている Web サイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックするか、警告を表示します。

- **ふるまい検知**。*ふるまい検知*コンポーネントは、オペレーティングシステム内のアプリケーションからの悪意のあるアクティビティを監視できます。悪意のある動作を検知した時、Kaspersky Endpoint Security はその動作を実行しているアプリケーションのプロセスを終了させることができます。

- **システム変更監視**では、オペレーティングシステムのファイルやディレクトリの変更を追跡できます。*システム変更監視*コンポーネントは、コンポーネントの設定で指定された監視範囲のオブジェクトで実行されたアクションをリアルタイムで監視します。*システム整合性チェック*タスクを使用して、オンデマンドでシステムの整合性をチェックできます。このチェックは、監視範囲に含まれるオブジェクトの現在の状態を、ベースラインとして事前に設定された初期状態と比較することによって実行されます。

Kaspersky Endpoint Security は、感染したオブジェクトを検出し、そこで検出された脅威を無効化します。このためにアプリケーションが使用できるのは次のとおりです：

- 定義データベースを使用した、感染したファイルの検知と駆除。スキャン処理中に、各ファイルに脅威が存在するかどうか解析されます。ファイルのコードを特定の脅威のコードと比較し、一致する可能性のあるものを探します。

- Kaspersky Security Network。Kaspersky Security Network のデータを使用すると、Kaspersky Endpoint Security による様々な脅威への対応が早くなり、一部の保護コンポーネントのパフォーマンスが改善され、誤検知の可能性が低減されます。

Kaspersky Endpoint Security は、駆除または削除の前に、デバイス上の Backup にファイルのバックアップコピーを保存します。駆除後、駆除されたファイル内の重要な情報へのアクセスが部分的または完全に失われた場合、コピーからファイルを復元できます。

スキャンタスクの実行中に、Kaspersky Endpoint Security は、変更から保護されているファイル（「immutable」属性および「append-only」属性のファイル、「immutable」属性および「append-only」属性のディレクトリ内のファイル）を駆除および削除できます。バックアップは、駆除または削除前に作成されたこれらのファイルのコピーを保存します。必要に応じて、バックアップのコピーからファイルを復元することができます。スキャンタスクが完了すると、駆除されたファイルの「不変」属性と「追加のみ」属性がリセットされます。

Kaspersky Endpoint Security は、通知専用モードで動作します。*通知専用モード*は、脅威が検出された場合、アプリケーションのコンポーネントやタスクが、悪意のあるオブジェクトの駆除や削除、アクセスの拒否、アプリケーションの活動のブロックなどを試みないアプリケーションの動作モードです。代わりに、検知された脅威についてのみユーザーに通知します。

Kaspersky Endpoint Security は、アプリケーションの機能を拡張するために、他のカスペルスキーソリューションとの統合に対応しています：

- Kaspersky Managed Detection and Response との連携によって、組織を標的とした脅威を継続的に探索、検知、排除します。

- Kaspersky Endpoint Detection and Response (KATA) と Kaspersky Anti Targeted Attack Platform のコンポーネントである Kaspersky Endpoint Detection and Response（KATA）の連携を設定することで、組織の IT インフラを確実に保護し、ゼロデイ攻撃、標的型攻撃、高度持続的脅威を含む脅威を迅速に検知します。

- Kaspersky Endpoint Detection and Response Optimum との連携を設定することで、エクスプロイト、ランサムウェア、ファイルレス攻撃、デバイスやデータに危害を加える攻撃者による正規のシステムツールの使用などの脅威から組織の IT インフラストラクチャが保護されます。

Kaspersky Endpoint Security をコンテナアプリケーション（以下、KESL コンテナ）として外部システムに組み込み、リポジトリ内のコンテナイメージをスキャンできます。

仮想環境の保護に Kaspersky Endpoint Security Light Agent モードを使用している場合、KESL コンテナ機能はサポートされません。

アプリケーションを最新の状態に保つため、アプリケーションの追加機能が提供されます：

- 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を使用して、本製品をアクティベートします。

  Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、アクティベーションは Protection Server（Kaspersky Hybrid Cloud Security for Virtualization Light Agent のコンポーネント）で実行されます。

- Kasperskyのアップデートサーバーから、管理サーバーを介して、またはユーザーが指定したソースから、スケジュールやオンデマンドで定義データベースと機能をアップデートします。

  Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、製品は Protection Server（Kaspersky Hybrid Cloud Security for Virtualization Light Agent のコンポーネント）から定義データベースと製品モジュールのアップデートを受信します。

- ユーザーロールに従った、製品機能のユーザーアクセスの管理。

- アプリケーションの実行中に発生したイベントについての管理者への通知。

- 整合性チェックツールを使用した製品コンポーネントの整合性チェック。

Kaspersky Endpoint Security を管理するには、次の方法を使用します：

- Kaspersky Security Center Web コンソール、Kaspersky Security Center Cloud コンソール、または管理コンソールを介して、Kaspersky Security Center を使用します。

- コマンドラインからコントロールコマンドを使用する。

- グラフィカルユーザーインターフェイスを使用する。

  Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、Kaspersky Security Center Cloud コンソールおよびグラフィカルユーザーインターフェースを使用して製品を管理することはできません。

米国領土では、貿易制限に従い、2024 年 9 月 10 日東部夏時間（EDT）午前 12 時以降、更新機能（ウイルス対策シグネチャの更新およびコードベースの更新を含む）および KSN 機能がアプリケーションで利用できなくなります。

Kaspersky Endpoint Security の使用モードについて

Kaspersky Endpoint Security は、次のいずれかのモードで使用できます：

- 標準モードで操作でワークステーションとサーバーを保護する（「標準モード」）。Kaspersky Endpoint Security は、Linux オペレーティングシステムが動作するデバイスを保護するためのスタンドアロン製品として使用されます。

- Kaspersky Hybrid Cloud Security for Virtualization Light Agent の一部として Light Agent モードで仮想環境を保護する（「Light Agent モード」）。Kaspersky Endpoint Security は、Linux ゲスト OS を実行する仮想マシンを保護する Kaspersky Endpoint Security for Virtualization Light Agent ソリューションの Light Agent コンポーネントです。

既定では、本製品は標準モードで使用されます。

本製品を Light Agent モードで使用する場合は、以下の手順が必要です：

1. Kaspersky Hybrid Cloud Security for Virtualization Light Agent を使用して保護する必要がある各仮想マシンに Kaspersky Endpoint Security をインストールします。仮想マシンテンプレートに本製品をインストールすることもできます。

   インストール中に、次のいずれかの方法でアプリケーションを Light Agent モードで使用することを指定する必要があります。

   - 対話または自動モードで製品をインストール後に設定します（コマンドラインを使ってインストールした場合）

   - アプリケーションインストールパッケージのプロパティ、またはインストールパッケージに含まれる autoinstall.ini 設定情報ファイル（Kaspersky Security Center を使用してインストールする場合）。

   Kaspersky Endpoint Security のインストール後は、製品の使用モードを変更できません。

   Light Agent モードを有効にすると、Kaspersky Endpoint Security の Light Agent モードで以下の設定を行うこともできます：

   - 仮想インフラストラクチャで保護する仮想マシンのロール：サーバーまたはワークステーション。仮想マシンのロールは、その仮想マシン上で製品が使用されるライセンスと、使用可能な機能を決定します。

   - VDI 保護モード。一時的な仮想マシンの作成に使用する仮想マシンテンプレートに本製品をインストールする場合は、このモードを有効にすることを推奨します。VDI 保護モードは、一時的な仮想マシン上での Kaspersky Endpoint Security の動作を最適化します。

2. Light Agent と SVM の接続設定、および Light Agent と Integration Server の接続を設定します。

Light Agent モードの Kaspersky Endpoint Security は、Kaspersky Hybrid Cloud Security for Virtualization Light Agent ソリューションの他のコンポーネント、つまり SVM にインストールされている Integration Server および Protection Server と対話します（詳細については、Kaspersky Endpoint Security for Virtualization Light Agent のヘルプを参照してください）。Protection Server と対話するために、Kaspersky Endpoint Security は、この Protection Server がインストールされている SVM への接続を確立して維持します。

Light Agent が統合サーバーを通じて SVM に関する情報を受信する場合、または保護サーバーと Light Agent 間の接続を保護する場合は、統合サーバーへの接続が要求されます。

Kaspersky Endpoint Security ポリシーの接続設定は、プロパティから Kaspersky Security Center 管理コンソールまたは Kaspersky Security Center Web コンソールを使用して行います。

次のコマンドを使用すると、Light Agent モードでの製品の動作設定に関する情報や、Integration Server および SVM への接続に関する情報を取得できます：`kesl-control --ksvla-info`、`kesl-control --viis-info`、`kesl-control --svm-info`。

製品の使用モードに関する情報は、［**コンポーネント**］セクションの対象デバイスにある Kaspersky Endpoint Security のプロパティの Kaspersky Security Center に表示されます。**仮想環境を保護する Light Agent モード**の行に、次のように情報が表示されます：

- *実行中*ステータスは、本製品が Light Agent モードで使用されていることを意味します。
- *インストールされていない*ステータスは、本製品が標準モードで使用されていることを意味します。

Light Agent モードで製品をアクティベートする際の注意事項

Kaspersky Endpoint Security を Light Agent モードで使用する場合、製品を個別にアクティベートする必要はありません。Kaspersky Security for Virtualization Light Agent のみを有効化します。有効化は、SVM にライセンスを追加することによって、Protection Server 側（Kaspersky Security for Virtualization Light Agent のコンポーネント）で実行されます。詳細については、Kaspersky Hybrid Cloud Security for Virtualization Light Agent のヘルプを参照してください。

Kaspersky Endpoint Detection and Response Optimum 機能を有効化するには、EDR Optimum ライセンスを SVM に追加する必要もあります。Kaspersky Kaspersky Hybrid Cloud Security for Virtualization Light Agent ソリューションのコンポーネントを有効化するためのライセンスには、この機能は含まれません。

ソリューションをアクティベートし、Light Agent を SVM に接続すると、Protection Server コンポーネントから Light Agent にライセンス情報が送信されます。接続する SVM を選択する時、Light Agent は他の設定の中でも特に、SVM に追加されたライセンスの種別を判断します。SVM に追加されたライセンスの種別が、仮想インフラストラクチャ（サーバーまたはワークステーション）内における保護対象の仮想マシンの役割と一致しない場合、Light Agent は SVM に接続しません。詳細については、Kaspersky Hybrid Cloud Security for Virtualization Light Agent のヘルプを参照してください。

`kesl-control -L --query` コマンドを使用すると、保護された仮想マシン上の Light Agent for Linux を有効化するために使用されるライセンスに関する情報を表示できます。

Kaspersky Endpoint Security において、*ライセンスの追加*タスクや、ライセンスの追加および削除コマンドを使用してライセンスを管理することはできません。

Light Agent モードでの定義データベースとモジュールのアップデートについて

Light Agent モードの Kaspersky Endpoint Security は、Kaspersky Security for Virtualization Light Agent の一部として動作するために必要な特別なマルウェア対策データベースを使用します。Kaspersky Endpoint Security は、Protection Server から定義データベースとモジュールのアップデートを受信します。詳細については、『Kaspersky Hybrid Cloud Security for Virtualization Light Agent のヘルプ』を参照してください。

保護された仮想マシン上のデータベースと機能は、Kaspersky Endpoint Security の特別なアップデートローカルタスクを使用してアップデートされ、SVM 上のフォルダーがアップデート元として指定されます。アップデートタスクは自動的に開始されます。このタスクを削除したり、設定を変更したりすることはできません。

SVM 上のフォルダー以外のアップデート元はサポートされていません。グループアップデートタスクの使用はサポートされていません。

最後のマルウェア対策データベースと機能のアップデートは、Protection Server 側でもロールバックされます。SVM 上の定義データベースとモジュールの更新をロールバックすると、保護された仮想マシン上で特別なアップデートローカルタスクが自動的に開始されます。このタスクを完了することにより、Light Agent は以前の一連のマルウェア対策データベースの使用に戻ります。

Kaspersky Endpoint Security のローカルタスクおよびグループタスクの *ロールバック*はサポートされていません。

Light Agent モードで本製品を使用するその他の特徴

Kaspersky Endpoint Security が Light Agent モードで使用されている場合：

- KESL コンテナ機能はサポートされていません。
- Kaspersky Security Center Cloud コンソールおよびグラフィカルユーザーインターフェースを使用した製品管理はできません。
- クラウドデータベースの使用はサポートされていません。
- Kaspersky Endpoint Security は、KSN プロキシサーバーを使用して KSN サーバーと対話します。KSN との直接通信には対応していません。
- Integration Server、SVM、または KSN サーバーに接続する場合、アプリケーションのプロキシサーバーの使用には対応していません。
- Kaspersky Symphony XDR との連携には対応していません。

配布キット

Kaspersky Endpoint Security 配布キットに含まれているファイル、および Kaspersky Security Center を使用して製品をリモートでインストールするために必要なファイルは、カスペルスキーの Web サイトからダウンロードできます。

配布キットには、次のファイルを含む Kaspersky Endpoint Security のインストールパッケージが含まれています：

- kesl-12.1.0-<ビルド番号>.i386.rpm、kesl_12.1.0-<ビルド番号>_i386.deb

メインのアプリケーションファイルが含まれています。パッケージは、パッケージマネージャーの種別に基づき 32 ビットオペレーティングシステムにインストールできます。

- kesl-12.1.0-<ビルド番号>.x86_64.rpm、kesl_12.1.0-<ビルド番号>_amd64.deb

  メインのアプリケーションファイルが含まれています。パッケージは、パッケージマネージャーの種別に基づき 64 ビットオペレーティングシステムにインストールできます。

- kesl-12.1.0-<ビルド番号>.aarch64.rpm、kesl_12.1.0-<ビルド番号>_arm64.deb

  メインのアプリケーションファイルが含まれています。関連するパッケージマネージャーのパッケージは、ARM® アーキテクチャの 64 ビットオペレーティングシステムにインストールできます。

- kesl-gui-12.1.0-<ビルド番号>.i386.rpm、kesl-gui_12.1.0-<ビルド番号>_i386.deb

  製品のグラフィカルユーザーインターフェイスのファイルが含まれています。パッケージは、パッケージマネージャーの種別に基づき 32 ビットオペレーティングシステムにインストールできます。

- kesl-gui-12.1.0-<ビルド番号>.x86_64.rpm、kesl-gui_12.1.0-<ビルド番号>_amd64.deb

  製品のグラフィカルユーザーインターフェイスのファイルが含まれています。パッケージは、パッケージマネージャーの種別に基づき 64 ビットオペレーティングシステムにインストールできます。

- kesl-gui-12.1.0-<ビルド番号>.aarch64.rpm、kesl-gui_12.1.0-<ビルド番号>_arm64.deb

  製品のグラフィカルユーザーインターフェイスのファイルが含まれています。関連するパッケージマネージャーのパッケージは、ARM アーキテクチャの 64 ビットオペレーティングシステムにインストールできます。

- kesl-12.1.0.<ビルド番号>.zip

  Kaspersky Security Center を使用して製品をリモートインストールする際に使用されるファイル（license.<言語 ID> ファイルや ksn_license.<言語 ID> ファイルなど）が含まれています。

  > Kaspersky Security Center ネットワークエージェントは配布キットには含まれていません。［**Kaspersky Security Center**］セクションのアプリダウンロードページからダウンロードできます。

- docker-service-kesl64-12.1.0-<ビルド番号>.tgz

  KESL コンテナアプリケーションのイメージを作成するためのファイルが含まれています。

- ksn_license.<言語 ID>

  Kaspersky Security Network に関する声明の本文が含まれています。

- license.<言語 ID

  使用許諾契約書の本文が含まれています。使用許諾契約書には、本製品の使用条件が指定されています。

アプリケーションドキュメントに記載されていない、またはテクニカルサポートスペシャリストが推奨していない方法を使用してアプリケーションファイルを単独で変更すると、アプリケーションやオペレーティングシステムのパフォーマンスの低下や障害、デバイスの保護の低下、データへのアクセス不能や破損、KSN への追加統計の送信を可能につながる可能性があります。

システム要件

このセクションには、Kaspersky Endpoint Security のシステム要件が含まれています。

ハードウェア要件

Kaspersky Endpoint Security のハードウェア要件は次の通りです：

ハードウェアの最小要件：

- Core ™ 2 Duo 1.86 GHz 以上のプロセッサ
- 1 GB 以上のスワップ領域
- 1 GB 以上のメモリ（32 ビットオペレーティングシステムの場合）、2 GB 以上のメモリ（64 ビットオペレーティングシステムの場合）
- 4 GB 以上のハードディスク空き容量（インストール、一時ファイル、ログファイルの保存などに使用）
- グラフィカルユーザーインターフェイスを使用する場合、モニターは幅 1000 ピクセル、高さ 600 ピクセルのウィンドウを表示できる必要があります (画面のスケーリングが適用される場合、これらの寸法もスケーリングされます)
- Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、仮想ネットワークインターフェイスは帯域幅 100 Mbit/s です

Arm アーキテクチャの最小ハードウェア要件：

- Armv8.2-A Kunpeng 920 または Armv8-A Baikal-M (BE-M1000) プロセッサまたは m-TrusT Terminal
- 1 GB 以上のスワップ領域
- 2 GB 以上のメモリ
- 3 GB 以上のハードディスク空き容量（インストール、一時ファイル、ログファイルの保存などに使用）
- グラフィカルユーザーインターフェイスを使用する場合、モニターは幅 1000 ピクセル、高さ 600 ピクセルのウィンドウを表示できる必要があります（画面のスケーリングが適用される場合、これらの寸法もスケーリングされます）

Light Agent モードで Kaspersky Endpoint Security を使用して仮想環境を保護することは、Arm アーキテクチャに基づくオペレーティングシステムではサポートされていません。

ソフトウェア要件

Kaspersky Endpoint Security をインストールするには、次のいずれかのオペレーティングシステムがデバイスにインストールされている必要があります：

- 32 ビットオペレーティングシステム：

- Debian GNU/Linux 11.0 以降
- Debian GNU/Linux 12.0 以降
- Mageia™ 4

  Mageia 4 オペレーティングシステムを実行しているデバイスでは、Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response（KATA）との連携はサポートされていません。

- ALT 8 SP Workstation (8.4)
- ALT 8 SP Server (8.4)
- ALT SP Workstation リリース 10
- ALT SP Server リリース 10

- 64 ビットオペレーティングシステム：
  - AlmaLinux OS 8 以降
  - AlmaLinux OS 9 以降
  - AlterOS® 7.5 以降
  - Amazon™ Linux 2
  - Astra Linux Common Edition 2.12
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.5)
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.6)
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.7)
  - Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6)

    Light Agent モードで Kaspersky Endpoint Security を使用して仮想環境を保護することは、必須アクセス制御モードおよびクローズドソフトウェア環境モードで Astra Linux オペレーティングシステムを実行しているデバイスではサポートされていません。

  「モバイル」モードの Astra Linux オペレーティングシステムは、デスクトップモードのタブレットコンピューター（タブレット）にのみ対応しています。

  - CentOS 7.2 以降
  - CentOS Stream 8
  - CentOS Stream 9
  - Debian GNU/Linux 11.0 以降

- Debian GNU/Linux 12.0 以降
- EMIAS 1.0 以降
- EulerOS 2.0 SP10
- Kylin 10
- Linux Mint 20.3 以降
- Linux Mint 21.1 以降
- openSUSE Leap 15.0 以降
- Oracle Linux 7.3 以降
- Oracle Linux 8.0 以降
- Oracle Linux 9.0 以降
- Red Hat Enterprise Linux 7.2 以降
- Red Hat Enterprise Linux 8.0 以降
- Red Hat Enterprise Linux 9.0 以降
- Rocky Linux 8.5 以降
- Rocky Linux 9.1
- SberLinux 8.8 (Dykhtau)
- SberOS3.2.0
- SUSE Linux Enterprise Server 12.5 以降
- SUSE Linux Enterprise Server 15 以降
- Ubuntu® 20.04 LTS
- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS
- ALT 8 SP Workstation (8.4)
- ALT 8 SP Server (8.4)
- ALT Education 10.1
- ALT Workstation 10.1
- ALT Server 10.1
- ALT SP Workstation リリース 10

- ALT SP Server リリース 10
- Atlant、 Alcyone build、 version 2022.02
- GosLinux 7.17
- GosLinux 7.2
- MSVSPHERE 9.2 ARM
- MSVSPHERE 9.2 SERVER
- RED OS® 7.3
- RED OS 8.0
- ROSA Cobalt 7.9
- ROSA Chrome 12
- SynthesisM Client 8.6
- SynthesisM Server 8.6

- Arm アーキテクチャの 64 ビットオペレーティングシステム：
  - Astra Linux Special Edition RUSB.10152-02 (operational update 4.7)
  - CentOS Stream 9
  - EulerOS 2.0 SP10
  - SUSE Linux Enterprise Server 15
  - Ubuntu 22.04 LTS
  - ALT 8 SP Workstation (8.4)
  - ALT 8 SP Server (8.4)
  - ALT SP Workstation リリース 10
  - ALT SP Server リリース 10
  - RED OS 7.3

Light Agent モードで Kaspersky Endpoint Security を使用して仮想環境を保護することは、Arm アーキテクチャのオペレーティングシステムではサポートされていません。

fanotify の技術的な制限のため、本製品は次のファイルシステムをサポートしていません：autofs、binfmt_misc、cgroup、configfs、debugfs、devpts、devtmpfs、fuse、fuse.gvfsd-fuse、gfs2、gvfs、hugetlbfs、mqueue、nfsd、proc、parsecfs、pipefs、pstore、usbfs、rpc_pipefs、securityfs、selinuxfs、sysfs、tracefs。

サポートされる Kaspersky Security Center のバージョン

Kaspersky Endpoint Security と互換性がある Kaspersky Security Center のバージョンは次の通りです：

- Kaspersky Security Center 13.2。Kaspersky Endpoint Security は、管理コンソールから MMC 管理プラグインを使用して管理できます。
- Kaspersky Security Center 14Kaspersky Endpoint Security は、管理コンソールから MMC 管理プラグインを使用する管理と、Kaspersky Security Center Web コンソールから Web 管理プラグインを使用する管理が可能です。
- Kaspersky Security Center 14.2 Windows。Kaspersky Endpoint Security は、管理コンソールから MMC 管理プラグインを使用する管理と、Kaspersky Security Center Web コンソールから Web 管理プラグインを使用する管理が可能です。
- Kaspersky Security Center 14.2 Linux。Kaspersky Endpoint Security は、Kaspersky Security Center Web コンソールから Web 管理プラグインを使用して管理できます。
- Kaspersky Security Center 15 Linux。Kaspersky Endpoint Security は、Kaspersky Security Center Web コンソールから Web 管理プラグインを使用して管理できます。
- Kaspersky Security Center 15.1 Linux。Kaspersky Endpoint Security は、Kaspersky Security Center Web コンソールから Web 管理プラグインを使用して管理できます。

Kaspersky Endpoint Security を（Kaspersky Security for Virtualization Light Agent の一部として）Light Agent モードで使用して仮想環境を保護する場合、次のいずれかのバージョンの Kaspersky Security Center を使用してアプリケーションを管理することを推奨します。

- Kaspersky Security Center 14.2 Windows。
- Kaspersky Security Center 15 Linux。
- Kaspersky Security Center 15.1 Linux。

Kaspersky Endpoint Security は、Kaspersky Security Center から Kaspersky Security Center ネットワークエージェントを使用して管理されます。

Kaspersky Security Center ネットワークエージェントは、Kaspersky Endpoint Security の配布キットには含まれていません。［**Kaspersky Security Center**］セクションのアプリダウンロードページからダウンロードできます。

Kaspersky Endpoint Detection and Response (KATA) コンポーネントとの製品の連携を使用している場合は、次のバージョンの Kaspersky Security Center を使用してアプリケーションを管理することを推奨します。

- Kaspersky Security Center 14.2 Windows。
- Kaspersky Security Center 15 Linux。
- Kaspersky Security Center 15.1 Linux。

サポートされる Kaspersky Anti Targeted Attack Platform のバージョン

Kaspersky Endpoint Security は、次のバージョンの Kaspersky Anti Targeted Attack Platformと互換性があります。

- Kaspersky Anti Targeted Attack Platform 5.1。制限付きでサポートされます。
- Kaspersky Anti Targeted Attack Platform 6.0。
- Kaspersky Anti Targeted Attack Platform 6.1。

Kaspersky Anti Targeted Attack Platform ソリューションの詳細については、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

主な変更点

Kaspersky Endpoint Security に追加された機能と改良点は、次の通りです：

- Kaspersky Endpoint Detection and Response Optimum との連携を設定できるようになりました。これにより、エクスプロイト、ランサムウェア、ファイルレス攻撃、デバイスやデータに危害を加える攻撃者による正規のシステムツールの使用などの脅威から組織の IT インフラストラクチャが保護されます。

- アプリケーションに 2 つの現在のライセンスを追加できるようになりました。本製品を有効化するための主要なライセンスと、Kaspersky Endpoint Detection and Response Optimum 機能を有効化するための追加ライセンスです。主要なライセンスに Kaspersky Endpoint Detection and Response Optimum 機能が含まれていない場合は、追加のライセンスが必要です。

- Web リソースへのユーザーアクセスを制御する新しい *ウェブコントロール*コンポーネントが追加されました。これにより、トラフィックの消費を削減し、作業時間の不適切な使用を減らすことができます。ユーザーが ウェブコントロールによってアクセスが制限されている Web サイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックするか、警告を表示します。

- 新たに追加された Kaspersky Endpoint Security の安定性監視機能により、本製品が異常終了した回数を追跡し、不安定な動作について管理者に通知することができます。

- Kaspersky Security Center Web コンソールを使用して Kaspersky Endpoint Security をインストールする手順が改善されました。本製品のインストールパッケージのプロパティで、以前は autoinstall.ini 設定ファイルでのみ使用可能だった初期設定パラメータを指定できるようになりました。

- Kaspersky Security Center Web コンソールおよび Kaspersky Security Center 管理コンソールを使用して、より多くの製品設定を指定できるようになりました。以前は kesl.ini の設定情報ファイルでのみ編集できた設定を編集できます。

- スキャンタスクを実行するときに、グローバル除外とファイル脅威対策除外を有効または無効にできるようになりました。

- Kaspersky Symphony XDR との連携を設定できるようになりました。Kaspersky Endpoint Security アプリケーションが標準モードで使用されている場合、アプリケーションは「マルウェアスキャンの開始」および「データベースの更新」の応答処理を実行できます。Kaspersky Endpoint Security が Light Agent モードで使用されている場合、 Kaspersky Symphony XDR との連携には対応していません。

- アプリケーションが Kaspersky Security Center を使用して管理されている場合、クライアントデバイスにインストールされているか、クライアントデバイスに接続されているすべてのデバイス（以前にインストールされ接続されていたが現在は切断されているデバイスを含む）に関する情報を管理サーバーに送信できるようになりました。

- トラフィック傍受ルールが改善され、同じネットワーク上のコンテナの相互作用に対応できるようになりました。

- サポートされているオペレーティングシステムのリストが更新されました。

Kaspersky Endpoint Security のインストールの準備

全般的なアクション

Kaspersky Endpoint Security のインストールを開始する前に、次の処理を実行する必要があります：

- デバイスがアプリケーションのシステム要件を満たしていることを確認します。
- デバイスにサードパーティ製アンチウイルスソフトウェアがインストールされていないことを確認します。
- デバイスに Kaspersky Endpoint Agent for Linux がインストールされていないことを確認します。Kaspersky Endpoint Agent for Linux がインストールされている場合、インストールプロセス中に手動で遠隔操作しなければならないというメッセージが表示されます。
- デバイスに Perl インタープリター - バージョン 5.10 以上がインストールされていることを確認します。
- オペレーティングシステムに semanage 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ます。ユーティリティがインストールされていない場合は、パッケージマネージャに応じて、policycoreutils-python または policycoreutils-python-utils パッケージをインストールします。
- fanotify テクノロジーをサポートしていないオペレーティングシステムを搭載したデバイスでは、以下がインストールされていることを確認してください：
  - 製品のコンパイルとタスクの実行のためのパッケージ（gcc、binutils、glibc、glibc-devel、make）。
  - Kaspersky Endpoint Security モジュールをコンパイルするためのオペレーティングシステムカーネルのヘッダーファイルを含むパッケージ。
- オペレーティングシステムに応じて、以下のパッケージのいずれかをデバイスにインストールしてください：
  - SUSE Linux Enterprise Server 15 オペレーティングシステムを実行しているデバイスでは、パッケージ insserv-compat をインストールする必要があります。
  - Red Hat Enterprise Linux 8 または RED OS オペレーティングシステムを実行しているデバイスでは、パッケージ perl-Getopt-Long をインストールします。
  - Red Hat Enterprise Linux または RED OS オペレーティングシステムを実行しているデバイスでは、パッケージ perl-File-Copy をインストールします。このパッケージは製品の初期設定スクリプトを動作させるために必要ですが、既定では存在しないかもしれません。
- 既定では、Astra Linux オペレーティングシステムは ptrace をブロックしており（ptrace 機能をオフにします）、Kaspersky Endpoint Security の動作に影響を与える可能性があります。Kaspersky Endpoint Security を正しく動作させるには、Astra Linux のインストール時に ptrace のブロックを解除してください。Astra Linux が既にインストールされている場合、このモードをオン / オフにする方法については、Astra Linux ヘルプセンターのウェブサイトを参照してください（**ptrace のブロック**セクションの**保護とブロックメカニズムの設定**）。
- デバイスで 3.16 以前の Linux カーネルが使用されている場合、Kaspersky Managed Detection and Response（KATA）との連携には、auditd サービスが起動やインストールされていないことを確認する必要があります。
- ファイアウォール管理、ウェブ脅威対策、およびネットワーク脅威対策コンポーネントを動作させるには、デバイスに iptables ユーティリティをインストールする必要があります。

- Kaspersky Endpoint Security の管理プラグインが機能するには、Microsoft® Visual C++® 2015 再頒布可能パッケージアップデート 3 RC（https://www.microsoft.com/ja-jp/download/details.aspx?id=52685）が管理サーバーにインストールされている必要があります。

- 本製品が正常に動作するには、root アカウントが次のディレクトリの所有者であり、所有者のみが書き込みアクセス権を持っていることを確認してください：/var、/var/opt、/var/opt/kaspersky、/var/log/kaspersky、/opt、/opt/kaspersky、/usr/bin、/usr/lib、/

Kaspersky Endpoint Security を Light Agent モードでインストールする前の追加操作

（Kaspersky Hybrid Cloud Security for Virtualization Light Agent の一部として）仮想環境を保護するために Kaspersky Endpoint Security を Light Agent モードで使用する場合は、Kaspersky Endpoint Security のインストールを開始する前に、次の追加操作を行う必要があります：

- Kaspersky Hybrid Cloud Security for Virtualization Light Agent が導入されている仮想インフラストラクチャに応じて、保護する仮想マシンに以下のパッケージがインストールされていることを確認します：
  - Microsoft Hyper-V インフラストラクチャでは、Integration Services パッケージを仮想マシンにインストールする必要があります。
  - VMware vSphere インフラストラクチャでは、VMware Tools パッケージを仮想マシンにインストールする必要があります。
  - XenServer インフラストラクチャでは、XenTools を仮想マシンにインストールする必要があります。
  - HUAWEI FusionSphere インフラストラクチャでは、HUAWEI Tools パッケージを仮想マシンにインストールする必要があります。
  - KVM、OpenStack、VK Cloud、TIONIX Cloud Platform、Astra Linux、または Viola Virtualization Server に基づくインフラストラクチャでは、QEMU ゲストエージェントを仮想マシンにインストールする必要があります。

- 仮想マシン間のトラフィックを監視するネットワーク機器やソフトウェアの設定で、Light Agent モードの Kaspersky Endpoint Security と Kaspersky Hybrid Cloud Security for Virtualization Light Agent の他のコンポーネントとの対話に使用されるポートをネットワークトラフィックが通過できることを確認してください。ソリューションコンポーネントの詳細については、『Kaspersky Hybrid Cloud Security for Virtualization Light Agent のヘルプ』を参照してください。

Light Agent の操作に使用されるポート

ポート番号およびプロトコル	通信方向	目的および説明
7271 TCP	Light Agent から Integration Server へ。	Light Agent と Integration Server 間の対話。
8000 UDP	SVM から Light Agent へ。	SVM アドレスのリストを使用して、使用可能な SVM の情報を Light Agent に送信します。
8000 UDP	Light Agent から SVM へ。	Light Agent が SVM のステータスに関する情報を受信するためです。
11111 TCP	Light Agent から SVM へ。	接続が保護されていない場合に、Light Agent から Protection Server にサービス要求（ライセンス情報の取得など）を送信するためです。
11112 TCP	Light AgentからSVM へ。	接続が保護されている場合に、Light Agent から Protection Server にサービス要求（ライセンス情報の取得など）を送信す

		るためです。
9876 TCP	Light AgentからSVMへ。	接続が保護されていない場合に、Light Agent から Protection Server にファイルスキャン要求を転送します。
9877 TCP	Light AgentからSVMへ。	接続が保護されている場合に、Light Agent から Protection Server にファイルスキャン要求を送信します。
80 TCP	Light AgentからSVMへ。	Light Agent 上でソリューションの定義データベースと製品モジュールをアップデートします。
15000 UDP	Kaspersky Security Center から SVM へ。	Kaspersky Security Center で Protection Server を管理する場合。
15000 UDP	Kaspersky Security Center から Light Agents へ。	Kaspersky Security Center で Light Agent を管理する場合。
13000 TCP	Light Agent から Kaspersky Security Center へ。	接続が保護されている場合、Kaspersky Security Center で Light Agent を管理するためです。
14000 TCP	Light Agentから Kaspersky Security Centerへ。	接続が保護されていない場合、Kaspersky Security Center で Light Agent を管理するためです。

Kaspersky Endpoint Security のインストールと初期設定

Kaspersky Endpoint Security をインストールする前に、インストールの準備をする必要があります。

ここでは、Kaspersky Endpoint Security のインストールと初期設定、Kaspersky Security Center Network Agent のインストールと設定、および Kaspersky Endpoint Security の管理プラグインのインストールについて説明しています。インストールシナリオは、Kaspersky Endpoint Security を使用するモードによって異なります。

標準モード

Kaspersky Endpoint Security を標準モードで使用する場合、インストール手順には次の手順が含まれます。

1. **ネットワークエージェントのインストールと初期設定**

   Kaspersky Endpoint Security を Kaspersky Security Center で管理する場合は、保護対象デバイスに Kaspersky Security Center Network Agent をインストールし、設定します。

2. **Kaspersky Endpoint Security 管理プラグインのインストール**

   Kaspersky Endpoint Security を Kaspersky Security Center で管理する場合は、Kaspersky Endpoint Security 管理プラグインをインストールします。Kaspersky Security Center を管理するコンソールによって、以下の管理プラグインが使用されます：

   - Kaspersky Endpoint Security Web 管理プラグインを使用すると、Kaspersky Security Center Cloud コンソールと Kaspersky Security Center Web コンソールを使用して本製品を管理できます。Web プラグインは、Kaspersky Security Center Web Console がインストールされているデバイスにインストールされます。
   - Kaspersky Endpoint Security MMC 管理プラグインを使用すると、Kaspersky Security Center 管理コンソールを使用して本製品を管理できます。MMC プラグインは、Kaspersky Security Center 管理コンソールがインストールされているデバイスにインストールされています。

3. **製品パッケージとグラフィカルユーザーインターフェイスのインストール**

   Kaspersky Endpoint Security は、DEB および RPM 形式のパッケージで配信されます。本製品用とグラフィカルユーザーインターフェイス用の、別々のパッケージもあります。Kaspersky Endpoint Security と、必要に応じてグラフィカルユーザーインターフェイスを適切な形式のパッケージからインストールします。

   インストールするには、次のいずれかの方法があります：

   - Kaspersky Security Center を使用。
   - コマンドラインを使用。

4. **Kaspersky Endpoint Security の初期設定**

   クライアントデバイスの保護をオンにするために、初期設定を行う必要があります。

   Kaspersky Security Center を使用して Kaspersky Endpoint Security をインストールする場合は、インストール完了後、使用の開始手順に従ってください。

   Kaspersky Endpoint Security をコマンドラインを使用してインストールした場合、インストール完了後、初期設定スクリプトを実行するか、初期設定を自動モードで実行します。

Light Agent モード

Light Agent モードで Kaspersky Endpoint Security を使用して仮想環境を保護することは、Arm アーキテクチャに基づくオペレーティングシステムではサポートされていません。

Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合は、インストール手順に次の手順が含まれます：

1. **ネットワークエージェントのインストールと初期設定**

   仮想マシンおよび仮想マシンテンプレートへの Kaspersky Security Center Agent のインストールと設定。

   一時的な仮想マシンの作成に使用される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場合は、一時的な仮想マシンのパフォーマンスを最適化できる設定を構成することを推奨します。仮想マシンテンプレートへのインストールの詳細については、Kaspersky Security for Virtualization Light Agent のヘルプ を参照してください。

2. **Kaspersky Endpoint Security 管理プラグインのインストール**

   Kaspersky Endpoint Security 管理プラグインのインストール。Kaspersky Security Centerを管理するコンソールによって、以下の管理プラグインが使用されます：

   - Kaspersky Endpoint Security Web 管理プラグインを使用すると、Kaspersky Security Center Cloud コンソールと Kaspersky Security Center Web コンソールを使用して本製品を管理できます。Webプラグインは、Kaspersky Security Center Web Consoleがインストールされているデバイスにインストールされます。

   - Kaspersky Endpoint Security MMC 管理プラグインを使用すると、Kaspersky Security Center 管理コンソールを使用して本製品を管理できます。MMC プラグインは、Kaspersky Security Center 管理コンソールがインストールされているデバイスにインストールされています。

3. **Kaspersky Endpoint Security のパッケージのインストールと初期設定**

   Kaspersky Endpoint Security は、DEB および RPM 形式のパッケージで配信されます。必要な形式のパッケージから、Kaspersky Endpoint Security をインストールします。本製品用とグラフィカルユーザーインターフェイス用の、別々のパッケージもあります。

   仮想環境の保護に Kaspersky Endpoint Security Light Agent モードを使用している場合、グラフィカルユーザーインターフェイスはサポートされません。

   アプリケーションをインストールするには、次のいずれかの方法があります：

   - Kaspersky Security Center を使用。

     インストールを開始する前に、次のいずれかの方法でアプリケーションの初期設定を実行する必要があります：

     - インストールパッケージのプロパティの［**設定**］タブ（この方法は Kaspersky Security Center Web コンソールでのみ利用可能です）。

     - インストールパッケージに含まれている設定情報ファイルを使用します。

     Light Agent モード（設定情報ファイルで`KSVLA_MODE=yes`）を選択する必要があります。一時的な仮想マシンを作成するテンプレートに Kaspersky Endpoint Security をインストールする場合は、一時的な仮想マシン上のアプリケーションのパフォーマンスを最適化するために、VDI 保護モードも有効にすることをお勧めします（設定情報ファイルで`VDI_MODE=yes`）。

   - コマンドラインを使用。コマンドラインを使用してインストールを行う場合、初期設定時にアプリケーションの使用モードが選択されます。

4. **Kaspersky Endpoint Security の初期設定**

クライアントデバイスの保護をオンにするために、初期設定を行う必要があります。

Kaspersky Security Center を使用して Kaspersky Endpoint Security をインストールする場合は、インストール完了後、使用の開始手順に従ってください。

Kaspersky Endpoint Security をコマンドラインを使用してインストールした場合、インストール完了後、初期設定スクリプトを実行するか、初期設定を自動モードで実行します。初期設定の際に次のいずれかの方法で Light Agent モードを選択します：

- 初期構成スクリプトの「`Specifying the application usage`」ステップに `yes` と入力します。
- 初期セットアップ設定情報ファイルで `KSVLA_MODE=yes` 設定を指定します。

一時仮想マシンの作成に使用されるテンプレートに Kaspersky Endpoint Security をインストールする場合は、一時仮想マシンでの操作を最適化できる設定も構成することを推奨します。仮想マシンテンプレートへのインストールの詳細については、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください。

Kaspersky Security Center ネットワークエージェントのインストールと初期設定

Kaspersky Endpoint Security を Kaspersky Security Center で管理するには、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。

ネットワークエージェントは、クライアントデバイスと Kaspersky Security Center 管理サーバーとの接続を支援します。ネットワークエージェントは、一元的なリモート管理システムである Kaspersky Security Center へ接続するすべてのクライアントデバイスにインストールする必要があります。

Network Agent のインストールと初期設定を行うことができます：

- Kaspersky Security Center Web コンソールまたは管理コンソールを使用して管理者のワークステーションからリモートで行います。
- コマンドラインを使用して行います。

Kaspersky Security Center を使用したネットワークエージェントのインストール

Kaspersky Security Center を使用してネットワークエージェントのリモートインストールを開始する前に、リモートインストール用にデバイスを準備する必要があります（Kaspersky Security Center のヘルプ「Linux を実行しているデバイスの準備と、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リモートでインストールする」セクションを参照してください）。

ネットワークエージェントのインストールパッケージはリモートインストールに使用されます。ネットワークエージェントのインストールパッケージの作成に必要なファイルは、Kaspersky Web サイトの **Kaspersky Security Center** セクションからダウンロードできます。

ネットワークエージェントをリモートでインストールします：

1. 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作成します。

インストールパッケージの作成中に、ネットワークエージェントに関する使用許諾契約書の条項に同意する必要があります。使用許諾契約書の文言は、ネットワークエージェントの配布キットに含まれる license.txt ドキュメントで読むことができます。

インストールパッケージ設定で、ネットワークエージェントが接続する管理サーバーのアドレスと接続ポートを指定します。

2. リモート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方法についての詳細は、Kaspersky Security Center ヘルプを参照してください。

コマンドラインを使用したネットワークエージェントのインストールする

次のいずれかの方法で、コマンドラインを使用してネットワークエージェントをインストールできます：

- アンサーファイルを使って、サイレントモードでインストールと初期設定を実行します。アンサーファイルは、ネットワークエージェントのインストールと初期設定のためのカスタム設定を含むテキストファイルです。

- パッケージマネージャの種類に応じて、RPM または DEB 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し、対話モードでスクリプトを使用してネットワークエージェントの初期設定を実行します。スクリプトは、次のコマンドで実行されます：

  - 32 ビットオペレーティングシステム：

    ```
    # /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
    ```

  - 64 ビットオペレーティングシステム：

    ```
    # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
    ```

ネットワークエージェントのインストールは、root 権限で開始する必要があります。

サイレントモードでネットワークエージェントをインストール：

1. 応答ファイルを作成します。アンサーファイルには、ネットワークエージェントのインストールと初期設定のリストを < 設定 >=< 値 > の形式で入力します。

   アンサーファイルを正しく使用するには、次の必須設定を含める必要があります：

   - KLNAGENT_SERVER：管理サーバーの完全修飾ドメイン名（FQDN）または IP アドレス。

   - KLNAGENT_AUTOINSTALL：この設定は、サイレントモードでのインストールを有効にするかどうかを決定します。1 を指定します。

   - EULA_ACCEPTED：ネットワークエージェントの使用許諾契約書の条件に同意します。インストールを続行するには、使用許諾契約書の条項に同意する必要があります。使用許諾契約書の文言は、ネットワークエージェントの配布キットに含まれる license.txt ドキュメントで読むことができます。使用許諾契約書の条件を理解し、同意する場合は、1 を指定します。

   また、ネットワークエージェントのインストールと初期設定のために、その他の設定も追加できます。設定可能な項目については、Kaspersky Security Center のヘルプ（「Network Agent for Linux のサイレントモードでのインストール（アンサーファイル付き）」）を参照してください。

2. 次の例のように、アンサーファイルの完全な名前（パスを含む）を入力して、KLAUTOANSWERS 環境変数の値を設定します：

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

3. ネットワークエージェントをインストールします：

   - RPM パッケージから 32 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：

     ```
     # rpm -i klnagent-<ビルド番号>.i386.rpm
     ```

   - RPM パッケージから 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：

     ```
     # rpm -i klnagent64-<ビルド番号>.x86_64.rpm
     ```

   - RPM パッケージから ARM アーキテクチャ用 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：

     ```
     # rpm -i klnagent64-<ビルド番号>.aarch64.rpm
     ```

   - DEB パッケージから 32 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：

     ```
     # apt-get install ./klnagent_<ビルド番号>_i386.deb
     ```

   - DEB パッケージから 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：

     ```
     # apt-get install ./klnagent64_<ビルド番号>_amd64.deb
     ```

   - DEB パッケージから ARM アーキテクチャ用 64 ビットオペレーティングシステムにネットワークエージェントをインストールするには、次のコマンドを実行します：

     ```
     # apt-get install ./klnagent64_<ビルド番号>_arm64.deb
     ```

Kaspersky Endpoint Security 管理プラグインのインストール

Kaspersky Security Center を使用した Kaspersky Endpoint Security の管理に使用される Kaspersky Endpoint Security 管理プラグインは、次の通りです：

- Kaspersky Endpoint Security Web 管理プラグインを使用すると、Kaspersky Security Center Web コンソールと Kaspersky Security Center Cloud コンソールを使用して本製品を管理できます。
- Kaspersky Endpoint Security MMC 管理プラグインを使用すると、Kaspersky Security Center 管理コンソールを使用して本製品を管理できます。

Kaspersky Endpoint Security の異なるバージョンの管理プラグインを同時にインストールできます。そのため、管理する製品のバージョンに合わせて、異なるバージョンの管理プラグインで作成したポリシーも使用できます。

また、旧バージョンの管理プラグインで作成したポリシーとタスクを新しいバージョンに変換することもできます。

Kaspersky Endpoint Security Web プラグインのインストール

Kaspersky Security Center Web コンソールがインストールされたクライアントデバイスに Kaspersky Endpoint Security 管理 Web プラグインをインストールする必要があります。Web プラグインの機能は、ブラウザーで Kaspersky Security Center Web コンソールにアクセスできるすべての管理者が使用可能です。

Web プラグインのインストールは、次のように行います：

- Kaspersky Security Center Web コンソールの初期セットアップウィザードを使用します。

  Kaspersky Security Center Web コンソールを管理サーバーへ初めて接続する際は、Kaspersky Security Center Web コンソールによって初期セットアップウィザードの実行を促すプロンプトが自動的に表示されます。Kaspersky Security Center Web コンソールインターフェイスで初期セットアップウィザードを実行することもできます（**デバイスの検出と製品の導入 → 導入と割り当て → 初期セットアップウィザード**）。初期設定ウィザードは、インストールされた Web プラグインが最新であるかどうかを確認し、必要なアップデートをダウンロードすることもできます。Kaspersky Security Center Web コンソールの初期セットアップウィザードの詳細は、Kaspersky Security Center のヘルプセクションを参照してください。

- カスペルスキー Web プラグインのリストまたは外部ソースから配布キットを使用して手動で行います。

Kaspersky Endpoint Security の Web プラグインを手動でインストールします：

1. Kaspersky Security Center Web コンソールのメインウィンドウで、**設定 → Web プラグイン**を選択します。

   インストールされている Web プラグインのリストが開きます。

2. 次のいずれかの方法で、Kaspersky Endpoint Security Web プラグインのインストールを開始します：

   - カスペルスキーの Web プラグインのリストからインストールします：

     a. ［**追加**］をクリックします。

     利用可能なカスペルスキー Web プラグインのリストが表示されます。リストは、Web プラグインの新しいバージョンが公開されると自動的にアップデートされます。

     b. リストから **Kaspersky Endpoint Security <バージョン番号> for Linux** の Web プラグインを探し、名前をクリックします。

     c. Web プラグインの説明が表示されたウィンドウが開いたら、**プラグインをインストール**ボタンをクリックします。

     d. インストールが完了するまで待ち、情報ウィンドウで **OK** をクリックします。

   - 外部ソースからの Web プラグインのインストール（Web プラグインのインストールに必要なアーカイブは、配布キットに含まれています）：

     a. **リストから追加**ボタンをクリックします。

     b. 開いたウィンドウで、Web プラグインの配布キットを含む ZIP アーカイブへのパスと、TXT 形式の署名済みファイルへのパスを指定します。このファイルは Web プラグインと一緒にアーカイブに入っています。

     c. ［**追加**］をクリックします。

     d. インストールが完了するまで待ち、情報ウィンドウで **OK** をクリックします。

   新しいプラグインは、インストールされている Web プラグインのリストに表示されます（**設定 → Web プラグイン**）。

Kaspersky Security Center 管理サーバーへのプロパティで、Kaspersky Endpoint Security の配布パッケージに含まれていない言語版を選択すると、使用許諾契約書と Kaspersky Security Center Web コンソールのすべてのインターフェイスは英語で表示されます。

Kaspersky Endpoint Security MMC プラグインのインストール

Kaspersky Endpoint Security MMC 管理プラグインは、Kaspersky Security Center 管理コンソールがインストールされているのと同じクライアントデバイスにインストールする必要があります。

Kaspersky Endpoint Security 管理プラグインのインストール前に、Kaspersky Security Center と Redist C++ 2015（Microsoft Visual C++ 2015 再頒布可能パッケージ）がインストールされていることを確認してください。

MMC プラグインをインストールするには、

Kaspersky Security Center 管理コンソールがインストールされているデバイスで実行ファイルの klcfginst.msi を実行します。

ファイルは、Kaspersky Endpoint Security の配布キットに含まれています。

インストール後、Kaspersky Security Center 管理サーバーのプロパティのインストール済み MMC 管理プラグインの一覧に MMC 管理プラグインが表示されます。

インストールされている MMC 管理プラグインのリストを表示します：

1. Kaspersky Security Center 管理コンソールのツリーで、**管理サーバー <サーバー名>** ノードを選択し、次のいずれかの方法で管理サーバーのプロパティウィンドウを開きます：
   - **管理サーバー <サーバー名>** ノードのコンテキストメニューの**プロパティ**項目を使用します。
   - **管理サーバーセクション**の**管理サーバー <サーバー名>** ノードのワークスペースにある**管理サーバープロパティ**のリンクをクリックします。
2. 左側のリストで、**詳細設定**セクションの**インストールされているアプリケーション管理プラグインの情報**セクションを選択します。

   ウィンドウの右側には、インストールされている管理プラグインの一覧が表示され、Kaspersky Endpoint Security 用の MMC 管理プラグインが表示されます： **Kaspersky Endpoint Security <バージョン番号> for Linux**.

Kaspersky Security Center を使用した本製品のインストールと初期設定

Kaspersky Security Center Web コンソールまたは管理コンソールを使用して、管理者のワークステーションからリモートで Kaspersky Endpoint Security をクライアントデバイスにインストールできます。

リモートインストールに、Kaspersky Endpoint Security インストールパッケージを使用します。Kaspersky Endpoint Security のインストールパッケージは、サポートされているすべてのオペレーティングシステムとプロセッサアーキテクチャの種別に共通です。インストールパッケージを作成するには、Kaspersky Security Center Web コンソールまたは管理コンソールを使用します。

Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合（Kaspersky Hybrid Cloud Security for Virtualization Light Agent の一部として）、インストールパッケージのプロパティ（この方法は Web コンソールでのみ利用可能）、または設定情報ファイル autoinstall.ini でアプリケーションの初期設定を実行し、このファイルがインストールパッケージに含まれます。

Kaspersky Endpoint Security は、いくつかの方法で企業ネットワーク内のデバイスに導入できます。

Kaspersky Security Center Web コンソールがサポートする主要な導入方法は、次の通りです：

- 保護展開ウィザードを使用してアプリケーションをインストールします。
- リモートインストールタスクを使用したインストール。

Kaspersky Security Center 管理コンソールでは、主に次の導入方法をサポートしています：

- リモートインストールウィザードを使用して製品をインストールします。
- リモートインストールタスクを使用したインストール。

導入手順については、Kaspersky Security Center のヘルプを参照してください。

必要に応じて、Kaspersky Security Center のクライアントデバイスのリモート診断を使用して、アプリケーションのリモートインストールログを表示できます。

Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、インストール中のアプリケーションのアクティベーションと自動ライセンス配布はサポートされません。Kaspersky Endpoint Security が SVM への接続後、Protection Server からライセンスに関する情報を受信した場合、Kaspersky Endpoint Security を個別にアクティベートする必要はありません。

Kaspersky Security Center を使用したアプリケーションのインストールが完了したら、アプリケーションを動作させるための準備を行う必要があります。

クライアントデバイスにインストールされた Kaspersky Endpoint Security を Kaspersky Security Center で管理するには、これらのデバイスを管理グループに登録する必要があります。Kaspersky Endpoint Security のインストールを開始する前に、Kaspersky Endpoint Security がインストールされているデバイスを移動する、Kaspersky Security Center の管理グループを作成し、デバイスをこれらの管理グループに自動的に移動するようにルールを設定できます。デバイスを管理グループに移動するためのルールが設定されていない場合、Kaspersky Security Center は、管理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ているすべてのデバイスを［**未割り当てデバイス**］リストに移動します。この場合、手動でコンピューターを管理グループに移動する必要があります（詳細については、Kaspersky Security Center のヘルプを参照）。

Web コンソールで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、次のいずれかの方法でインストールパッケージを作成できます：

- 事前に用意したアーカイブファイルから。
- Kasperskyのサーバーでホストされている配布キットから。

仮想環境を保護するために Kaspersky Endpoint Security を Light Agent モードで使用する場合は、作成したインストールパッケージのプロパティの**設定**タブでアプリケーションの初期設定を実行する必要があります。インストールパッケージに含まれている設定情報ファイルを使用して、アプリケーションの初期設定を実行することもできます。

インストールパッケージを作成するためのアーカイブを準備します：

1. アーカイブ kesl.zip を、本製品のダウンロードページからダウンロードします。アーカイブは、**Kaspersky Endpoint Security for Linux**（**Additional distribution -> Files for Product remote installation**）に配置されています。

2. アーカイブ kesl.zip を Kaspersky Security Center 管理サーバーがアクセスできるフォルダーに解凍します。製品をインストールするオペレーティングシステムの種別とそのパッケージマネージャーの種別に対応する配布ファイルを、同じフォルダーに配置します：

   - Kaspersky Endpoint Security をインストールするには：
     - kesl-12.1.0-<ビルド番号>.i386.rpm（rpm を使用する 32 ビットオペレーティングシステムの場合）
     - kesl_12.1.0-<ビルド番号>_i386.deb（dpkg を使用する 32 ビットオペレーティングシステムの場合）
     - kesl-12.1.0-<ビルド番号>.x86_64.rpm（rpm を使用する 64 ビットオペレーティングシステムの場合）
     - kesl_12.1.0-<ビルド番号>_amd64.deb（dpkg を使用する 64 ビットオペレーティングシステムの場合）
     - kesl-12.1.0-<ビルド番号>.x86_64.rpm（rpm を使用する ARM アーキテクチャ用 64 ビットオペレーティングシステムの場合）
     - kesl_12.1.0-<ビルド番号>_amd64.deb（dpkg を使用する ARM アーキテクチャ用 64 ビットオペレーティングシステムの場合）
   - GUI をインストールするため：
     - kesl-gui-12.1.0-<ビルド番号>.i386.rpm（rpm を使用する 32 ビットオペレーティングシステムの場合）
     - kesl-gui_12.1.0-<ビルド番号>_i386.deb（dpkg を使用する 32 ビットオペレーティングシステムの場合）
     - kesl-gui-12.1.0-<ビルド番号>.x86_64.rpm（rpm を使用する 64 ビットオペレーティングシステムの場合）
     - kesl-gui_12.1.0-<ビルド番号>_amd64.deb（dpkg を使用する 64 ビットオペレーティングシステムの場合）
     - kesl-gui-12.1.0-<ビルド番号>.x86_64.rpm（rpm を使用する ARM アーキテクチャ用 64 ビットオペレーティングシステムの場合）
     - kesl-gui_12.1.0-<ビルド番号>_amd64.deb（dpkg を使用する ARM アーキテクチャ用 64 ビットオペレーティングシステムの場合）

   グラフィカルユーザーインターフェイスをインストールしない場合は、これらのファイルをフォルダに配置しないことで、インストールパッケージをより小さくできます。

Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、グラフィカルユーザーインターフェイスはサポートされません。

グラフィカルユーザーインターフェイスを使用しない場合は、作成したインストールパッケージのプロパティまたは autoinstall.ini 設定情報ファイルで `USE_GUI=No` を設定する必要があることに注意してください。設定しない場合、インストールが失敗します。

作成したインストールパッケージを使用して、本製品を複数の種別のオペレーティングシステムまたはパッケージマネージャーにインストールする場合は、すべての種別のオペレーティングシステムとパッケージマネージャーに必要なファイルをフォルダーに配置します。

3. 設定情報ファイルを使用してアプリケーションの初期設定を実行する場合は、autoinstall.ini 設定情報ファイルを開き、必要に応じて編集します。Autoinstall.ini ファイルは、アーカイブ kesl.zip を解凍したフォルダーにあります。

   Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合は、設定情報ファイル autoinstall.ini で `KSVLA_MODE=yes` に設定する必要があります。

   作成したインストールパッケージのプロパティの**設定**タブで、アプリケーションの初期設定を実行することもできます。

4. Kaspersky Endpoint Security を標準モードで使用する予定で、以前にダウンロードしたデータベースを使用したい場合は、必要なすべてのオペレーティングシステムタイプのデータベースを含む準備されたアーカイブをフォルダーに配置します。autoinstall.ini 設定情報ファイルを開き、「`UPDATE_EXECUTE=no`」を指定します。autoinstall.ini ファイルは、kesl.zip アーカイブを解凍したフォルダーにあります。

5. 準備したファイルはすべて、ZIP、CAB、TAR、TAR.GZ 形式のアーカイブに任意の名前で格納します。

Kaspersky Endpoint Security のインストールパッケージを Kaspersky Security Center Web コンソールで作成します：

1. Web コンソールのメインウィンドウで、以下のセクションのいずれかを選択します：

   - ［**デバイスの検出と導入**］→［**導入と割り当て**］→［**インストールパッケージ**］。
   - ［**操作**］→［**リポジトリ**］→［**インストールパッケージ**］。

   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開きます。

2. ［**追加**］をクリックします。

   インストールパッケージの作成ウィザードが開始されます。ウィザードの指示に従います。

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の作成方法を選択します：

   - **ファイルからインストールパッケージを作成することもできます。**インストールパッケージは、事前に用意したアーカイブから作成されます。Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合は、このオプションをオンに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します。**インストールパッケージは、Kasperskyのサーバーにある配布パッケージから作成されます。

Kaspersky Security Center Cloud コンソールでは、ファイルからインストールパッケージを作成することはできません。

4. 選択したパッケージ作成方法によって異なります：

   - パッケージ名を指定し、［**参照**］をクリックして、インストールパッケージを作成するために用意したアーカイブへのパスを指定します。

   - Kaspersky Endpoint Security の配布パッケージを選択します。右側のウィンドウで、配布パッケージに関する情報を読み、［**インストールパッケージのダウンロードと作成**］をクリックします。インストールパッケージの作成プロセスが開始されます。

5. インストールパッケージの作成中に、使用許諾契約書とプライバシーポリシーの条項に同意します。ウィザードに表示されたら、お客様とカスペルスキーとの間で締結する使用許諾契約書、およびデータの処理と転送について説明しているプライバシーポリシーの内容を確認します。インストールパッケージの作成を続行するには、使用許諾契約書とプライバシーポリシーの条件を理解して同意することを確認します。

インストールパッケージが作成され、インストールパッケージのリストに追加されます。インストールパッケージを使用すると、企業ネットワークのデバイスに本製品をインストールしたり、製品のバージョンをアップデートしたりできます。

インストールパッケージのプロパティの**設定**タブで、アプリケーションの初期設定を実行できます（以下の表を参照）。

Kaspersky Endpoint Security のインストールパッケージは、Kaspersky Security Center Web コンソールのバージョン 14.2 未満では設定できません。設定情報ファイル autoinstall.ini を使用して設定を編集してください。

インストールパッケージの設定

セクション	説明
ロケールを指定します	本製品の操作中に使用されるロケールを指定するには、このチェックボックスをオンにします。RFC 3066 で指定されている形式のロケール。この設定が指定されていない場合、既定のロケールが使用されます。
本製品をアクティベートします	チェックボックスをオンにしてアプリケーションをアクティベートします。 インストール後に製品をアクティベートすることもできます。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。
アップデート元を選択します。	アップデート元を指定します： • **カスペルスキーのアップデートサーバー**。 • **Kaspersky Security Center** • **ローカルネットワークまたはインターネット上の他のアップデート元**。

	この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。
インストール後にデータベースアップデートタスクを実行します。	本製品のインストール後にアップデートタスクを実行するには、このチェックボックスをオンにします。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。
プロキシサーバー設定を指定する。	インターネットへの接続に使用されるプロキシサーバーのアドレスを指定するには、このチェックボックスをオンにします。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。
カーネルソースをインストールします	カーネルモジュールのコンパイルを自動的に開始するには、このチェックボックスをオンにします。
グラフィカルユーザーインターフェイスを使用します。	グラフィカルユーザーインターフェイスの使用を有効にするには、このチェックボックスをオンにします。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。
admin ロールでユーザーを指定。	管理者（admin）ロールを割り当てるユーザーを指定するには、チェックボックスをオンにします。
SELinux を自動的に設定します。	Kaspersky Endpoint Security と連動するように SELinux を自動的に設定する場合は、チェックボックスをオンにします。
権限付きグループからユーザーを削除する	アプリケーションをインストールする前に、「kesladmin」および「keslaudit」の特権グループからユーザーを削除するには、このチェックボックスをオンにします。 チェックボックスがオンになっていて、「nogroup」のグループが存在しない場合は、インストールが失敗し、特権グループからユーザーを手動で削除するように要求します。
アプリケーションをインストール後初めて起動する際に、保護機能とスキャンタスクを無効にする。	インストール後に保護コンポーネントとスキャンタスクを無効にしてアプリケーションを起動するには、このチェックボックスをオンにします。 保護コンポーネントを無効にしたインストールは、たとえば、製品の動作における問題を再現し、トレースファイルを作成するのに便利です。 必要なコンポーネントとタスクを有効にすると、アプリケーションの再起動後も、有効にしたコンポーネントとタスクは引き続き動作します。
アプリケーションを Light Agent モードで使用します	アプリケーションを Light Agent モード（Kaspersky Security for Virtualization Light Agentの一部として）で使用して仮想環境を保護する場合は、チェックボックスをオンにします。

	このチェックボックスをオフにすると、アプリケーションは標準モードで使用することになります。
VDI 保護モードを有効にする。	VDI 保護モードを有効にするには、このチェックボックスをオンにします。本製品を一時的な仮想マシンの作成に使用する仮想マシンテンプレートにインストールする場合は、こちらを推奨します。 この設定は、製品が Light Agent モードで使用されている場合にのみ適用されます。
保護された仮想マシンがサーバーとして使用されます。	アプリケーションをインストールする仮想マシンが仮想インフラストラクチャ内でサーバーとして使用されている場合は、このチェックボックスをオンにします。 この設定は、製品が Light Agent モードで使用されている場合にのみ適用されます。

管理コンソールでのインストールパッケージの作成

Kaspersky Endpoint Security のインストールパッケージを作成する前に、パッケージに含めるファイルを準備する必要があります。

インストールパッケージを作成するためのファイルを準備します：

1. アーカイブ kesl.zip を、本製品のダウンロードページからダウンロードします。アーカイブは、**Kaspersky Endpoint Security for Linux**（**Additional distribution -> Files for Product remote installation**）に配置されています。

2. アーカイブ kesl.zip を Kaspersky Security Center 管理サーバーがアクセスできるフォルダーに解凍します。製品をインストールするオペレーティングシステムの種別とそのパッケージマネージャーの種別に対応する配布ファイルを、同じフォルダーに配置します：

   - Kaspersky Endpoint Security をインストールするには：
     - kesl-12.1.0-<ビルド番号>.i386.rpm（rpm を使用する 32 ビットオペレーティングシステムの場合）
     - kesl_12.1.0-<ビルド番号>_i386.deb（dpkg を使用する 32 ビットオペレーティングシステムの場合）
     - kesl-12.1.0-<ビルド番号>.x86_64.rpm（rpm を使用する 64 ビットオペレーティングシステムの場合）
     - kesl_12.1.0-<ビルド番号>_amd64.deb（dpkg を使用する 64 ビットオペレーティングシステムの場合）
     - kesl-12.1.0-<ビルド番号>.x86_64.rpm（rpm を使用する ARM アーキテクチャ用 64 ビットオペレーティングシステムの場合）
     - kesl_12.1.0-<ビルド番号>_amd64.deb（dpkg を使用する ARM アーキテクチャ用 64 ビットオペレーティングシステムの場合）
   - GUI をインストールするため：

- kesl-gui-12.1.0-<ビルド番号>.i386.rpm（rpm を使用する 32 ビットオペレーティングシステムの場合）
- kesl-gui_12.1.0-<ビルド番号>_i386.deb（dpkg を使用する 32 ビットオペレーティングシステムの場合）
- kesl-gui-12.1.0-<ビルド番号>.x86_64.rpm（rpm を使用する 64 ビットオペレーティングシステムの場合）
- kesl-gui_12.1.0-<ビルド番号>_amd64.deb（dpkg を使用する 64 ビットオペレーティングシステムの場合）
- kesl-gui-12.1.0-<ビルド番号>.x86_64.rpm（rpm を使用する ARM アーキテクチャ用 64 ビットオペレーティングシステムの場合）
- kesl-gui_12.1.0-<ビルド番号>_amd64.deb（dpkg を使用する ARM アーキテクチャ用 64 ビットオペレーティングシステムの場合）

グラフィカルユーザーインターフェイスをインストールしない場合は、これらのファイルをフォルダに配置しないことで、インストールパッケージをより小さくできます。

Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、グラフィカルユーザーインターフェイスはサポートされません。

グラフィカルユーザーインターフェイスを使用しない場合は、作成したインストールパッケージのプロパティまたは autoinstall.ini 設定情報ファイルで `USE_GUI=No` を設定する必要があることに注意してください。設定しない場合、インストールが失敗します。

作成したインストールパッケージを使用して、本製品を複数の種別のオペレーティングシステムまたはパッケージマネージャーにインストールする場合は、すべての種別のオペレーティングシステムとパッケージマネージャーに必要なファイルをフォルダーに配置します。

3. 設定情報ファイルを使用してアプリケーションの初期設定を実行する場合は、autoinstall.ini 設定情報ファイルを開き、必要に応じて編集します。Autoinstall.ini ファイルは、アーカイブ kesl.zip を解凍したフォルダーにあります。

   Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合は、設定情報ファイル autoinstall.ini で `KSVLA_MODE=yes` に設定する必要があります。

4. Kaspersky Endpoint Security を標準モードで使用する予定で、以前にダウンロードしたデータベースを使用したい場合は、必要なすべてのオペレーティングシステムタイプのデータベースを含む準備されたアーカイブをフォルダーに配置します。autoinstall.ini 設定情報ファイルを開き、「`UPDATE_EXECUTE=no`」を指定します。autoinstall.ini ファイルは、kesl.zip アーカイブを解凍したフォルダーにあります。

Kaspersky Security Center 管理コンソールで Kaspersky Endpoint Security のインストールパッケージを作成します：

1. コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］の順に選択します。
2. ［**インストールパッケージの作成**］をクリックします。

   インストールパッケージの作成ウィザードが開始されます。

3. 表示されたウィザードのウィンドウで、［**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**］をクリックします。

4. 新しいインストールパッケージの名前を入力して、次のステップに進みます。

5. Kaspersky Endpoint Security の配布パッケージを選択します。［**参照**］をクリックして表示されるウィンドウで、kesl.kud ファイルへのパスを指定します。このファイルはアーカイブ kesl.zip を解凍したフォルダーにあります。

   ウィンドウに製品名が表示されます。

   次のステップに進みます。

6. お客様とカスペルスキーとの間で締結する使用許諾契約書、およびデータの処理と転送について説明しているプライバシーポリシーの内容を確認します。

   インストールパッケージの作成を続行するには、使用許諾契約書とプライバシーポリシーの条件を理解して同意することを確認します。確認するには、開いたウィンドウで、両方のチェックボックスを選択します。

   次のステップに進みます。

7. ウィザードにより、製品のインストールに必要なファイルが Kaspersky Security Center 管理サーバーにダウンロードされます。ダウンロードが完了するまで時間がかかる場合があります。

8. ウィザードを完了します。

作成されたインストールパッケージは、Kaspersky Security Center 管理コンソールツリーの［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］フォルダーに保存されます。インストールパッケージは何度でも使用できます。

統合データベースを含むインストールパッケージを作成するために、定義データベースを含むアーカイブを準備する

場合によっては、事前にダウンロードされた定義データベースを使用してリモートインストールパッケージを作成することが必要になる場合があります。たとえば、Astra Linux Special Edition オペレーティングシステムを実行しているデバイスに製品をインストールする場合、または準備された現在のデータベースを使用して製品をすぐにインストールする場合（後でデータベースを個別にアップデートすることを避けるため）。

製品をインストールするための統合データベースを含むインストールパッケージを作成するには、次の手順を実行します：

1. コマンドラインまたは Kaspersky Security Center を使用してデバイスに Kaspersky Endpoint Security をインストールし、初期設定を実行します。

2. 定義データベースをアップデートします。データベースをアップデートするには、製品の初期設定中、またはインストール後に、コマンドラインでアップデートタイプのタスクを実行するか、Kaspersky Security Center 管理コンソールまたは Kaspersky Security Center Web コンソールでアップデートタスクを実行します。

3. 統合データベースを含むインストールパッケージを作成するオペレーティングシステムのアーキテクチャに応じて、/var/opt/kaspersky/kesl/private/updates/ ディレクトリの内容を次のサブディレクトリのいずれかにコピーします：/i386/、/x86_64/、または /arm64/。

4. ネストされたディレクトリの構造を維持しながら、データベースを含むディレクトリを kesl-bases.tgz アーカイブに配置します。アーカイブ内のオペレーティングシステムの必要なアーキテクチャに必要なデータベースを含むサブディレクトリを 1 つだけ配置できます。または、異なるアーキテクチャの複数のオペレーティングシステムにインストールするインストールパッケージを作成する場合、データベースを含むすべ

てのサブディレクトリ（/i386/、/x86_64/、/arm64/）を、異なるアーキテクチャ用の単一のアーカイブに配置することができます。

5. Kaspersky Security Center 管理コンソールまたは Kaspersky Security Center Web コンソール でインストールパッケージを作成する時に、作成されたアーカイブを定義データベースとともに使用できます。

Autoinstall.ini 設定情報ファイルでの設定

設定情報ファイル Autoinstall.ini では、以下の表に示す設定を指定できます。適用されるアプリケーション設定のセットは、製品の使用モードによって異なります。

Autoinstall.ini 設定情報ファイルでの設定

設定	説明	値
KSVLA_MODE	Kaspersky Endpoint Security の使用モード	［yes］-Kaspersky Endpoint Security は、仮想環境を保護するために Light Agent モードで使用されます（Kaspersky Hybrid Cloud Security for Virtualization Light Agent の一部として）。 ［no］（既定値）– Kaspersky Endpoint Security を標準モードで使用します。
SERVER_MODE	保護対象仮想マシンのロール（サーバーまたはワークステーション） この設定は、製品が Light Agent モードで使用されている場合にのみ適用されます。	yes（既定値）– 保護対象仮想マシンがサーバーとして使用されます。 ［いいえ］- 保護された仮想マシンはワークステーションとして使用されます。
VDI_MODE	VDI 保護モードを有効にして、一時的な仮想マシン上の製品のパフォーマンスを最適化します。 この設定は、アプリケーションが Light Agent モードで使用されている場合にのみ適用されます。	yes – VDI 保護モードを有効にします。Kaspersky Endpoint Security を一時的な仮想マシンの作成に使用する仮想マシンテンプレートにインストールする場合は、こちらを推奨します。 no（既定値）– VDI 保護モードを有効にしません。
EULA_AGREED	必須の設定。 使用許諾契約書の条件の同意。	yes（既定値）– 製品のインストール手順を続行するには、使用許諾契約書の条件に同意する必要があります。 no – 使用許諾契約書に同意しない。製品のインストールが中断されます。
PRIVACY_POLICY_AGREED	必須の設定。 プライバシーポリシーの条項の同意。	yes（既定値）– プライバシーポリシーの条項に同意して、アプリケーションのインストール手順を続行します。

		no – プライバシーポリシーに同意しません。製品のインストールが中断されます。
USE_KSN	必須の設定。 Kaspersky Security Network の使用を有効にする：KSN の使用を有効にするには、Kaspersky Security Network に関する声明の条項に同意する必要があります。	yes – Kaspersky Security Network に関する声明の条項に同意し、KSN の使用を有効にします。 no –（既定値）Kaspersky Security Network に関する声明に同意しません。 Kaspersky Endpoint Security が標準モードで使用されており、KSN の使用を有効にしている場合、アプリケーションのクラウドモードが自動的に有効になります。このモードでは、Kaspersky Endpoint Security はマルウェアデータベースの軽量バージョンを使用します。
GROUP_CLEAN	必須の設定。 ［Kesladmin］および［keslaudit］特権グループからのユーザーの削除。	［yes］- 特権グループからユーザーを削除します。値が yes で［nogroup］グループがない場合、インストールは失敗し、特権グループからユーザーを手動で削除するよう要求されます。 ［no］- 特権グループからユーザーを削除しないでください。
LOCALE	オプション設定。 Kaspersky Security Center に送信される製品イベントに使用されるロケール。	RFC 3066 で指定されている形式のロケール。 Locale 設定が指定されていない場合、オペレーティングシステムのローカリゼーション言語が使用されます。製品がオペレーティングシステムのローカリゼーション言語を判別できなかった場合、またはオペレーティングシステムのローカリゼーションがサポートされていない場合は、既定値の en_US.utf8 が使用されます。 グラフィカルインターフェイスとコマンドラインのロケールは、LANG 環境変数の値によって異なります。Kaspersky Endpoint Security でサポートされていないロケールが LANG 環境変数の値として指定されている場合、グラフィカルインターフェイスとコマンドラインは英語で表示されます。
INSTALL_LICENSE	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。	

	この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。	
UPDATER_SOURCE	アップデート元。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。	SCServer – Kaspersky Security Center 管理サーバーをアップデート元として使用する。 KLServers – カスペルスキーのサーバーをアップデート元として使用する。この値は既定で使用されます。 アップデート元のアドレス
PROXY_SERVER	インターネットへの接続に使用するプロキシサーバーのアドレス。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。	プロキシサーバーのアドレス
UPDATE_EXECUTE	設定中に製品の定義データベースアップデートタスクを開始する。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。	yes（既定値）– アップデートタスクを開始します。 no – アップデートタスクを開始しない。
KERNEL_SRCS_INSTALL	カーネルモジュールのコンパイルの自動開始。	yes（既定値）- カーネルモジュールをコンパイルします。 no – カーネルモジュールをコンパイルしない。
USE_GUI	グラフィカルユーザーインターフェイスを使用する。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。	yes – グラフィカルユーザーインターフェイスの使用の有効化。 no（既定値）– グラフィカルユーザーインターフェイスの使用を無効にします。
ADMIN_USER	管理者ロール（admin）を割り当てられたユーザー。	No
CONFIGURE_SELINUX	Kaspersky Endpoint Security と	yes（既定値）– Kaspersky Endpoint

	連携するための SELinux の自動設定。	Security と連携するよう SELinux を自動設定します。 no – Kaspersky Endpoint Security と連携するよう SELinux を自動設定しない。
DISABLE_PROTECTION	インストール後にアプリケーションの機能コンポーネントを無効にします。 コンポーネントを無効にしてインストールすると、アプリケーションの問題を再現してトレースファイルを作成する必要がある場合などに便利です。 DISABLE_PROTECTION=yes でアプリケーションのインストール後に必要なコンポーネントを有効にすると、製品の再起動後も有効にされたコンポーネントが機能し続けます。	［yes］：インストール後の製品起動時に保護コンポーネントとスキャンタスクを無効にします。 ［no］：インストール後のアプリケーション起動時に保護コンポーネントとスキャンタスクを無効にしません。
DISABLE_FILEAV_ACTIONS	インストール後のアプリケーションコンポーネントの駆除およびファイル削除機能を無効にします。 駆除およびファイル削除機能が無効で、脅威が検出された場合、アプリケーションは、脅威が検出されたファイルの駆除または削除を試みず、ファイル内の脅威の検知についてユーザに通知するだけです。 アプリケーションをインストールした後、kesl.ini 設定情報ファイルの DisableFileAvActions パラメータを使用して、ファイルの駆除および削除機能を有効にできます。	yes：インストール後のアプリケーション起動時に、駆除機能とファイル削除機能を無効にします。 no（既定値）：インストール後のアプリケーション起動時に、駆除機能とファイル削除機能を無効にしません。

設定情報ファイル autoinstall.ini の設定を変更する場合は、設定の値を次の形式で指定します：<設定名>=<設定値>（設定名とその値の間のスペースは処理されません）

Kaspersky Security Center の使用の開始

Kaspersky Endpoint Security を Kaspersky Security Center 経由で導入した後は、アプリケーションを動作させるための準備を行う必要があります。実行する操作は、Kaspersky Endpoint Security を使用するモードによって異なります。

標準モード

Kaspersky Endpoint Security を標準モードで使用する場合は、アプリケーションを導入した後、次の操作を実行する必要があります：

- 本製品をアクティベートします。管理コンソールまたは Kaspersky Security Center Web コンソールを使用して、アクティベーションタスクを作成、実行します。また、Kaspersky Endpoint Security のライセンス保管領域から、ライセンスをデバイスへ配信します。

- 管理コンソールまたは Kaspersky Security Center Web コンソールを使用して、定義データベースと機能をアップデートします。アップデートタスクを使用できます。このタスクは、MMC 管理プラグインまたは Kaspersky Endpoint Security Web 管理プラグインのインストール後に、Kaspersky Security Center の初期設定ウィザードによって自動的に作成されます。

- Kaspersky Security Center 管理コンソールまたは Web コンソールを使用して、アプリケーションを集中管理するためのポリシーを設定します。MMC 管理プラグインまたは Kaspersky Endpoint Security Web 管理プラグインのインストール後に、Kaspersky Security Center の初期設定ウィザードによって自動的に作成されたポリシーを使用できます。

  管理コンソールまたは Web コンソールを使用して、本製品の管理タスクを設定することもできます。

Light Agent モード

Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合は、アプリケーションを導入した後、次の操作を実行します：

1. Light Agent の SVM 検出設定を設定します。これを行うには、クライアントデバイスで製品を集中管理するためのポリシーを作成して設定する必要があります。管理コンソールまたは Web コンソールを使用して、ポリシーを操作できます。

   ポリシーのプロパティで次の設定を構成する必要があります：

   - Light Agent を Integration Server に接続するための設定。
   - Light Agent を SVM に接続するための設定。

2. Light Agent、SVM、および Integration Server 間で接続が確立されていることを確認します。

   保護対象の仮想マシン上で Kaspersky Endpoint Security のコマンドを使用すると、接続に関する情報を取得できます：

   - コマンド `kesl-control [-V] --svm-info` を使用すると、SVM への接続に関する情報を表示できます。
   - Integration Server への接続に関する情報は、コマンド `kesl-control [-V] --viis-info` を使用して表示できます。

3. Kaspersky Hybrid Cloud Security for Virtualization Light Agent が有効化されているライセンス情報を、Light Agent として使用する Kaspersky Endpoint Security が受信していることを確認してください。

   SVM でソリューションをアクティベートし、Light Agent を SVM に接続すると、Protection Server コンポーネントから Light Agent にライセンス情報が送信されます。ソリューションの一部として Kaspersky Endpoint Security が使用するライセンス情報は、保護対象の仮想マシン上でコマンド `kesl-control -L --query` を使用して表示できます。

4. Light Agent の動作に必要なデータベースのアップデートが保護対象の仮想マシンにインストールされていることを確認します。

   保護された仮想マシン上のデータベースは、SVM 上のフォルダーがアップデートソースとして指定された特別なアップデートタスクに格納されている必要があります。アップデートタスクは自動的に開始されます。

   コマンド `kesl-control --app-info` を使用すると、Light Agent で保護された仮想マシン上のデータベースがどれだけ最新であるかを確認できます。

   管理コンソールまたは Web コンソールを使用して、本製品の管理タスクを設定することもできます。

Kaspersky Security Center を使用した本製品のアクティベーション

*アクティベーション*とは、ライセンスの有効期限が切れるまで、すべての機能を使用できる製品版のライセンスを有効化するプロセスです。

Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、インストール後にアプリケーションをアクティベートする必要はありません。Kaspersky Hybrid Cloud Security for Virtualization Light Agent をアクティベートする場合、アクティベーションは、Protection Server（Kaspersky Hybrid Cloud Security for Virtualization Light Agent のコンポーネント）の SVM にライセンスを追加することで行います。詳細については、Kaspersky Hybrid Cloud Security for Virtualization Light Agent のヘルプを参照してください。

Kaspersky Endpoint Security を有効化するプロセスは、製品ライセンスの追加を伴います。

次の方法で、Kaspersky Security Center を通じて本製品にライセンスを追加できます。

- Kaspersky Endpoint Security インストールパッケージにライセンスを追加します。

  この方法では、Kaspersky Endpoint Security を展開するときに、インストールパッケージのプロパティにアプリケーションライセンスを追加できます。インストール後、アプリケーションは自動的に有効化されます。

- ライセンスの追加タスクを使用する。

  この方法では、特定のデバイスまたは管理グループに属しているデバイスにライセンスを追加できます。Kaspersky Security Center Web コンソールまたは管理コンソールを使用して、ライセンスの追加タスクを作成して実行できます。

- Kaspersky Security Center 管理サーバーに保管されているライセンスをクライアントデバイスに配信。

  この方法では、Kaspersky Security Center に既に接続されているクライアントデバイスと新しいクライアントデバイスにライセンスを自動的に追加できます。この方法を使用するには、まず Kaspersky Security Center の管理サーバーにライセンスを追加する必要があります。

Kaspersky Security Center 管理コンソールまたは Kaspersky Security Center Web コンソールを使用して、製品にライセンスを追加するタスクの作成、ライセンスの保管領域へのライセンスの追加、クライアントデバイスへのライセンスの配信が可能です。

Kaspersky Endpoint Detection and Response Optimum 機能が含まれていないライセンスでアプリケーションを使用している場合は、アプリケーションを有効化した後、EDR Optimum ラインセンスを追加する必要があります。

Kaspersky Security Center Web コンソールを使用したアクティベーション

［ライセンスの追加］タスクの作成前またはライセンスの配信前に、Kaspersky Security Center 管理サーバーのライセンス保管領域にライセンスを追加します。

Web コンソールを使用して Kaspersky Security Center のライセンス保管領域にライセンスを追加するには：

1. Web コンソールのメインウィンドウで、［**操作**］→［**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. 表示されたウィンドウで、リポジトリにライセンスを追加する方法を選択します：

   - ［**アクティベーションコードを入力**］：アクティベーションコードを使用してライセンスを追加する場合に選択します。
   - ［**ライセンス情報ファイルを追加**］：ライセンス情報ファイルを使用してライセンスを追加する場合に選択します。

4. 前の手順で選択したライセンスの追加方法に応じて、次のいずれかを行います：

   - 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。
   - ［**ライセンス情報ファイルの選択**］をクリックし、表示されたウィンドウで拡張子が key のファイルを選択します。

5. ［**閉じる**］をクリックします。

追加されたライセンスがライセンスのリストに表示されます。

［ライセンスの追加］タスクを使用して Web コンソール経由で本製品にライセンスを追加します：

1. Web コンソールのメインウィンドウで、**アセット（デバイス）→タスク**の順に選択します。
   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。
   タスクウィザードが起動します。
3. タスクの設定を編集します：
   a. ［**アプリケーション**］ドロップダウンリストで、製品名 Kaspersky Endpoint Security を選択します。
   b. ［**タスク種別**］ドロップダウンリストで、［**ライセンスの追加**］を選択します。
   c. ［**タスク名**］フィールドに、簡単な説明を入力します（例：`Kaspersky Endpoint Security for Linux` のアクティベーション）。
   d. ［**タスクを割り当てるデバイス**］セクションで、タスク範囲を選択します。［**次へ**］をクリックします。
4. 選択したタスク範囲オプションに従ってデバイスを選択します。［**次へ**］をクリックします。
   ［**Kaspersky Security Center ライセンス保管領域**］ウィンドウが表示されます。
5. Kaspersky Security Center ライセンス保管領域にライセンスを事前に追加している場合は、リストからライセンスを選択して［**次へ**］をクリックします。
6. 必要なキーがライセンス保管領域にない場合は、［**ライセンスの追加**］をクリックします。
   a. 表示されたウィンドウで、リポジトリにライセンスを追加する方法を選択します：
      - ［**アクティベーションコードを入力**］：アクティベーションコードを使用してライセンスを追加する場合に選択します。
      - ［**ライセンス情報ファイルを追加**］：ライセンス情報ファイルを使用してライセンスを追加する場合に選択します。

b. 前の手順で選択したライセンスの追加方法に応じて、次のいずれかを行います：

- 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。
- ［**ライセンス情報ファイルの選択**］をクリックし、表示されたウィンドウで拡張子が key のファイルを選択します。

c. ライセンスに関する情報を読み、［**閉じる**］をクリックします。

d. 追加されたライセンスがライセンスのリストに表示されます。リストからそのライセンスを選択し、［**次へ**］をクリックします。

7. ライセンスに関する情報を読み、［**次へ**］をクリックします。

8. ウィザードを完了します。

新しいタスクがタスクのリストに表示されます。

9. タスクの横にあるチェックボックスをオンにします。［**開始**］をクリックします。

［*ライセンスの追加*］タスクのプロパティで、デバイスに［*予備のライセンス*］を追加できます。現在のライセンスが期限切れになるか削除されると、予備のライセンスがアクティブになります。予備のライセンスを追加しておくことで、ライセンスの有効期限が切れた時に本製品の機能が制限されるのを防ぐことができます。

予備のライセンスを追加しているが、現在のライセンスが製品にまだ追加されていない場合、タスクはエラーで終了します。

Web コンソールを使用して、管理サーバーからデバイスにライセンスを配信して本製品にライセンスを追加します：

1. Web コンソールのメインウィンドウで、［**操作**］→［**カスペルスキーのライセンス**］の順に選択します。

2. ライセンスの対象となるアプリケーションの名前のリンクを使用して、ライセンスのプロパティを開きます。

3. ［**全般**］タブで、［**管理対象デバイスにライセンスを自動的に配布**］を選択します。

4. ［**保存**］をクリックします。

ライセンスは、該当するクライアントデバイスに自動的に配信されます。現在のライセンスまたは予備のライセンスとしてライセンスを自動配信する際、デバイス数によるライセンスの制限（ライセンスのプロパティで設定）が考慮されます。ライセンスの上限に達すると、このライセンスのデバイスへの配信は自動的に停止されます。［**デバイス**］タブのライセンスのプロパティで、ライセンスが追加されたデバイスの数とその他の情報を表示できます。

Kaspersky Security Center Web コンソールを使用してライセンスの使用状況を管理する方法は次の通りです：

- ライセンスの使用状況レポートを表示します（［**監視とレポート**］→［**レポート**］）。
- 管理対象デバイスのステータスを表示します（［**資産（デバイス）**］→［**管理対象デバイス**］）。製品がアクティベートされていない場合、デバイスには ステータスおよび「**保護が無効されています**」ステータスの説明が表示されます。
- ライセンスのプロパティを表示します（［**操作**］→［**カスペルスキーのライセンス**］）。

Kaspersky Security Center Cloud コンソールでのアクティベーション手順で特に注意すべき事項

Kaspersky Security Center Cloud コンソールには、試用版があります。*試用版*は、ユーザーに Cloud コンソールの機能に慣れていただくために設計された、Kaspersky Security Center Cloud コンソールの特別なバージョンです。このバージョンでは、30 日間ワークスペースで動作します。Kaspersky Endpoint Security を含むすべての管理対象のアプリケーションは、Kaspersky Security Center Cloud コンソールの試用版ライセンスのもとで自動的にアクティベートされます。ただし、Cloud コンソールの試用ライセンスの有効期限が切れると、Kaspersky Endpoint Security 独自の試用ライセンスを使用しても有効化できません。Cloud コンソールの詳細は、Kaspersky Security Center Cloud コンソールのヘルプを参照してください。

Kaspersky Security Center Cloud コンソールの試用版では、その後製品版に切り替えることはできません。30 日間の期限が切れると、試用版ワークスペースはすべてのコンテンツとともに自動的に削除されます。

コマンドラインを使用したネットワークエージェントのインストールと初期設定

本製品のインストール時に、コマンドラインを使用して次の操作を実行できます：

- 製品のインストール（グラフィカルユーザーインターフェイスあり）

  Kaspersky Hybrid Cloud Security for Virtualization Light Agent の一部として、Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、グラフィカルユーザーインターフェイスには対応してません。グラフィカルユーザーインターフェイスを含まない製品パッケージのみをインストールする必要があります。

- グラフィカルユーザーインターフェイスを使用せずに、製品パッケージのみをインストールします。
- アプリケーションがインストールされているデバイスにグラフィカルユーザーインターフェースをインストールします。

  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グラフィカルユーザーインターフェースをインストールすることはできません。

apt パッケージマネージャーのバージョンが 1.1.X より前の場合は、dpkg / rpm パッケージマネージャー（オペレーティングシステムによって異なります）を使用してインストールします。

本製品のインストールが完了したら、対話または自動で初期設定を実行します。

コマンドラインを使用したネットワークエージェントのインストール

製品のインストール（グラフィカルユーザーインターフェイスなし）

Kaspersky Endpoint Security を RPM パッケージから 32 ビットオペレーティングシステムにインストールするには、次のコマンドを実行します：

```
# rpm -i kesl-12.1.0-<ビルド番号>.i386.rpm
```

Kaspersky Endpoint Security を RPM パッケージから 64 ビットオペレーティングシステムにインストールするには、次のコマンドを実行します：

```
# rpm -i kesl-12.1.0-<ビルド番号>.x86_64.rpm
```

Kaspersky Endpoint Security を RPM パッケージから ARM アーキテクチャ用 64 ビットオペレーティングシステムにインストールするには、次のコマンドを実行します：

```
# rpm -i kesl-12.1.0-<ビルド番号>.aarch64.rpm
```

Kaspersky Endpoint Security を DEB パッケージから 32 ビットオペレーティングシステムにインストールするには、次のコマンドを実行します：

```
# apt-get install ./kesl_12.1.0-<ビルド番号>_i386.deb
```

Kaspersky Endpoint Security を DEB パッケージから 64 ビットオペレーティングシステムにインストールするには、次のコマンドを実行します：

```
# apt-get install ./kesl_12.1.0-<ビルド番号>_amd64.deb
```

Kaspersky Endpoint Security を DEB パッケージから ARM アーキテクチャ用 32 ビットオペレーティングシステムにインストールするには、次のコマンドを実行します：

```
# apt-get install ./kesl_12.1.0-<ビルド番号>_arm64.deb
```

グラフィカルユーザーインターフェイスのインストール

グラフィカルユーザーインターフェイスを RPM パッケージから 32 ビットオペレーティングシステムにインストールするには、次のコマンドを実行します：

```
# rpm -i kesl-gui-12.1.0-<ビルド番号>.i386.rpm
```

グラフィカルユーザーインターフェイスを RPM パッケージから 64 ビットオペレーティングシステムにインストールするには、次のコマンドを実行します：

```
# rpm -i kesl-gui-12.1.0-<ビルド番号>.x86_64.rpm
```

グラフィカルユーザーインターフェイスを RPM パッケージから ARM アーキテクチャ用 64 ビットオペレーティングシステムにインストールするには、次のコマンドを実行します：

```
# rpm -i kesl-gui-12.1.0-<ビルド番号>.aarch64.rpm
```

グラフィカルユーザーインターフェイスを DEB パッケージから 32 ビットオペレーティングシステムにインストールするには、次のコマンドを実行します：

```
# apt-get install ./kesl-gui_12.1.0-<ビルド番号>_i386.deb
```

グラフィカルユーザーインターフェイスを DEB パッケージから 64 ビットオペレーティングシステムにインストールするには、次のコマンドを実行します：

```
# apt-get install ./kesl-gui_12.1.0-<ビルド番号>_amd64.deb
```

グラフィカルユーザーインターフェイスを DEB パッケージから ARM アーキテクチャ用 64 ビットオペレーティングシステムにインストールするには、次のコマンドを実行します：

```
# apt-get install ./kesl-gui_12.1.0-<ビルド番号>_arm64.deb
```

対話モードでの製品の初期設定

コマンドラインを使用して Kaspersky Endpoint Security をインストールした後、初期設定スクリプトを実行して、アプリケーションの初期設定を実行します。インストール後の設定スクリプトは、Kaspersky Endpoint Security の配布キットに含まれています。

クライアントデバイスの保護を有効にするためには、コマンドラインを使用して本製品をインストールした後、初期設定を行う必要があります。

Kaspersky Endpoint Security の初期設定スクリプトを実行するには、次のコマンドを実行します：

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl
```

Kaspersky Endpoint Security パッケージのインストール完了後、初期設定スクリプトを root 権限で実行する必要があります。スクリプトにより、Kaspersky Endpoint Security の設定値の段階的な入力が要求されます。スクリプトの実行完了とコンソールの解放は、アプリケーションの初期設定が完了したことを示します。

リターンコードを確認するには、次のコマンドを実行します：

```
echo $?
```

コマンドがコード 0 を返した場合、アプリケーションの初期設定は正常に完了しています。

本製品の使用モードの選択

このステップでは、Kaspersky Endpoint Security の使用モードを有効にします。

- Light Agent モードで Kaspersky Endpoint Security を使用して仮想環境を保護したい場合は、［yes］を入力してください。
- Kaspersky Endpoint Security を標準モードで使用したい場合は、［no］を入力してください。

初期設定が完了した後は、製品の使用モードを変更することはできません。

仮想マシンのロールの定義

このステップは、最初の手順で Kaspersky Endpoint Security を仮想環境の保護に Light Agent モードで使用することを選択した場合のみ表示されます。

このステップでは、Kaspersky Endpoint Security をインストールする仮想マシンのロール（サーバーまたはワークステーション）を指定します：

- 仮想マシンをサーバーとして使用する場合は、［yes］と入力します。
- 仮想マシンをワークステーションとして使用する場合は、［no］と入力します。

VDI保護モードの有効化

このステップは、最初の手順でKaspersky Endpoint Securityを仮想環境の保護に Light Agentモードで使用することを選択した場合のみ表示されます。

このステップでは、VDI 保護モードを有効にすることができます。このモードでは、一時的な仮想マシン上での Kaspersky Endpoint Security の動作を最適化します。VDI 保護モードが有効な場合、仮想マシンの再起動が必要なアップデートはインストールされません。再起動が必要なアップデートを受信すると、仮想マシンにインストールされた Light Agent から Kaspersky Security Center に対して、保護対象仮想マシンテンプレートを更新する必要がある旨のメッセージが送信されます。

VDI 保護モードを有効にする場合は、 yes を指定します。Kaspersky Endpoint Security を一時的な仮想マシンの作成に使用する仮想マシンテンプレートにインストールする場合は、こちらを推奨します。

VDI 保護モードを有効にしない場合は、 no を指定します。Kaspersky Endpoint Security を永続的な仮想マシン、または仮想マシンの作成に使用される仮想マシンテンプレートにインストールする場合は、こちらを推奨します。

ロケールの選択

このステップでは、サポートされているロケール識別子のリストが RFC 3066 形式で表示されます。

このリストで識別される形式でロケールを指定します。このロケールは、Kaspersky Security Center に送信される製品イベント、および使用許諾契約書、プライバシーポリシー、Kaspersky Security Network に関する声明の本文で使用されます。

グラフィカルインターフェイスとアプリケーションコマンドラインのロケールは、 LANG 環境変数の値によって異なります。Kaspersky Endpoint Security でサポートされていないロケールが LANG 環境変数の値として指定されている場合、グラフィカルインターフェイスとコマンドラインは英語で表示されます。

使用許諾契約書とプライバシーポリシーの表示

このステップでは、お客様とカスペルスキーとの間で締結する使用許諾契約書、およびデータの処理と転送について説明しているプライバシーポリシーをお読みください。

使用許諾契約書への同意

このステップでは、使用許諾契約書の条件に同意するかしないかを指定する必要があります。

表示モードの終了後、次の値のいずれかを入力します：

- yes（または y）：使用許諾契約書の条件に同意する場合。
- no（または n）：使用許諾契約書の条件に同意しない場合。

使用許諾契約書の条件に同意しないときは、アプリケーションが、Kaspersky Endpoint Security の設定プロセスを終了させます。

プライバシーポリシーへの同意

このステップでは、プライバシーポリシーの条件に同意するかしないかを指定する必要があります。

表示モードの終了後、次の値のいずれかを入力します：

- yes（または y）：プライバシーポリシーに同意する場合。
- no（または n）：プライバシーポリシーに同意しない場合。

プライバシーポリシーの条件に同意しない場合、アプリケーションは、Kaspersky Endpoint Security の設定プロセスを終了します。

Kaspersky Security Network を使用する

このステップでは、Kaspersky Security Network に関する声明の利用規約に同意するかしないかを指定する必要があります。Kaspersky Security Network に関する声明が記載されているファイル ksn_license.<言語 ID> は、ディレクトリ /opt/kaspersky/kesl/doc/ にあります。

次のいずれかの値を入力します：

- yes（または y）：Kaspersky Security Network に関する声明の条件に同意する場合。［拡張 KSN モード］が有効になります。
- no（または n）：Kaspersky Security Network に関する声明の条件に同意しない場合。

Kaspersky Security Network への参加に同意しなくても、Kaspersky Endpoint Security の初期アプリケーション設定は中断されません。Kaspersky Security Network のモードは、いつでも有効化、無効化、または変更することができます。

Kaspersky Endpoint Security が標準モードで使用されており、Kaspersky Security Network の使用を有効にしている場合、アプリケーションのクラウドモードが自動的に有効になります。このモードでは、Kaspersky Endpoint Security はマルウェア対策データベースの軽量バージョンを使用します。仮想環境を保護するための Light Agent モードでは、軽量マルウェア対策データベースの使用はサポートされていません。

特権グループからのユーザーの削除

このステップは、ユーザーが［kesladmin］グループおよび / または［keslaudit］グループで検出された場合にのみ表示されます。

このステップでは、［kesladmin］および［keslaudit］特権グループからユーザーを削除するかどうかを指定します。［kesladmin］および［keslaudit］グループに含まれるユーザーは、製品機能への特権的なアクセス権を受け取ります。

［yes］入力すると、検出されたすべてのユーザーを［kesladmin］および / または［keslaudit］グループから削除します。プライマリグループが［kesladmin］または［keslaudit］であるユーザーは、［nogroup］グループに移動します。［nogroup］グループがない場合、インストールは失敗し、特権グループからユーザーを手動で削除するよう要求されます。

特権グループからユーザーを削除したくない場合は、［no］と入力してください。

ユーザーへの Administrator ロールの割り当て

このステップでは、管理者ロール（admin）をユーザーに付与できます。

管理者ロールを付与するユーザーの名前を入力します。

ユーザーへの管理者ロールの付与は、後でいつでも実行可能です。

ファイル操作のインターセプターの種別の決定

このステップでは、使用されるオペレーティングシステムのファイル操作のインターセプターの種別が判断されます。fanotify テクノロジーをサポートしないオペレーティングシステムの場合、カーネルモジュールのコンパイルが開始されます。

カーネルモジュールのコンパイルプロセス中に必要なパッケージが検出されない場合、それらのインストールを指示するメッセージが表示されます。パッケージをダウンロードできない場合、エラーメッセージが表示されます。

必要なパッケージがすべて使用可能な場合、ファイル脅威対策タスクの開始時にカーネルモジュールが自動的にコンパイルされます。

Kaspersky Endpoint Security の初期設定の完了後、カーネルモジュールをコンパイルできます。

SELinux の自動設定の有効化

このステップは、オペレーティングシステムに SELinux がインストールされている場合にのみ表示されます。

このステップでは、Kaspersky Endpoint Security と連携するために SELinux の自動設定を有効にできます。

SELinux の自動設定を有効にするには、「yes」を入力します。SELinux を自動的に設定できない場合、エラーメッセージが表示され、SELinux を手動で設定するよう指示されます。

SELinux を自動的に設定しない場合は、「no」を入力します。

既定では、「yes」が指定されます。

Kaspersky Endpoint Security の初期設定が完了した後、必要に応じて、SELinux を本製品と連携するように手動で設定できます。

アップデート元の設定

このステップは、最初の手順として Kaspersky Endpoint Security を標準モードで使用することを選択した場合のみ表示されます。Kaspersky Endpoint Security を Light Agent モードで使用する場合、Kaspersky Endpoint Security は Protection Server から Light Agent 用の定義データベースと製品モジュールのアップデートを受信します。

このステップでは、データベースとアプリケーションモジュールのアップデート元を指定します。

次のいずれかの値を入力します：

- ［KLServers］- アプリケーションが、カスペルスキーのアップデートサーバーのいずれかからアップデートを受信します。
- ［SCServer］- アプリケーションが、組織に設置されている Kaspersky Security Center 管理サーバーからアップデートを保護対象のデバイスにダウンロードします。組織のデバイス保護の集中管理に Kaspersky Security Center を使用する場合は、このアップデート元を選択できます。
- < URL >: アプリケーションは、カスタムソースからアップデートをダウンロードします。ローカルエリアネットワーク、またはインターネットにあるカスタムのアップデート元のアドレスを指定できます。
- < path > – アプリケーションは指定されたディレクトリからアップデートを受け取ります。

プロキシサーバーの設定

このステップは、最初の手順として Kaspersky Endpoint Security を標準モードで使用することを選択した場合のみ表示されます。

このステップでは、プロキシサーバーを使用してインターネットにアクセスしている場合にプロキシサーバー設定を指定する必要があります。アップデートサーバーから定義データベースをダウンロードするには、インターネット接続が必要です。

プロキシサーバーを設定するには、次の操作のいずれかを実行します：

- インターネットへの接続にプロキシサーバーを使用する場合、次の形式のいずれかを使用して、プロキシサーバーのアドレスを指定します：
  - `<`プロキシサーバーの `IP` アドレス`>:<`ポート番号`>`（プロキシサーバー接続で認証が必要ない場合）。
  - `<`ユーザー名`>:<`パスワード`>@<`プロキシサーバーの `IP` アドレス`>:<`ポート番号`>`（プロキシサーバー接続で認証が必要な場合）。

    HTTP プロキシ経由で接続する場合は、他のシステムへのログインに使用しない別のアカウントを使用することを推奨します。HTTP プロキシがセキュアでない接続を使用しているため、アカウントが危険にさらされている可能性があります。
- インターネットへの接続にプロキシサーバーを使用しない場合は、「no」と入力します。

既定では、「no」が指定されます。

プロキシサーバー設定は、後で初期設定スクリプトを使用せずに指定できます。

本製品の定義データベースのアップデートの開始

このステップは、最初の手順として Kaspersky Endpoint Security を標準モードで使用することを選択した場合のみ表示されます。Kaspersky Endpoint Security を Light Agent モードで使用する場合、Kaspersky Endpoint Security は保護サーバーから Light Agent 用のデータベースとアプリケーションモジュールのアップデートを受信します。

このステップでは、クライアントデバイスで定義データベースのアップデートタスクを実行できます。定義データベースには、脅威シグネチャの説明と脅威の対処方法が格納されています。本製品では、脅威を検索して無害化する時にこれらのレコードを使用します。カスペルスキーのウイルスアナリストは、脅威に関する新しいレコードを定期的に追加します。

定義データベースをすぐにダウンロードしない場合は、`no` を入力します。

デバイス上でデータベースのアップデートタスクを開始する場合は、`yes` を入力します。

既定では、「`yes`」が指定されます。

［`yes`］を選択すると、データベースのアップデート後に本製品が自動的に再起動されます。

Kaspersky Endpoint Security では、定義データベースがアップデートされた後にのみ、デバイスが保護されます。

初期設定スクリプトを使用せずに、後でアップデートタスクを開始できます。

定義データベースの自動アップデートの有効化

このステップは、最初の手順として Kaspersky Endpoint Security を標準モードで使用することを選択した場合のみ表示されます。Kaspersky Endpoint Security を Light Agent モードで使用する場合、Kaspersky Endpoint Security は保護サーバーから Light Agent 用の定義データベースとアプリケーションモジュールのアップデートを受信します。

このステップでは、定義データベースの自動アップデートをオンにします。

定義データベースの自動アップデートをオンにするには、「yes」を入力します。既定では、60 分ごとに使用可能な定義データベースのアップデートを確認します。アップデートが使用可能な場合、アップデートされた定義データベースがダウンロードされます。

定義データベースを自動的にダウンロードしない場合は、「no」を入力します。

アップデートタスクのスケジュールを設定することにより、初期設定スクリプトを使用せずに後で定義データベースの自動アップデートを有効にすることができます。

本製品のアクティベーション

このステップは、最初の手順として Kaspersky Endpoint Security を標準モードで使用することを選択した場合のみ表示されます。Kaspersky Endpoint Security を Light Agent モードで使用する場合、Kaspersky Endpoint Security は Protection Server からライセンスに関する情報を受け取るため、Kaspersky Endpoint Security を個別にアクティベートする必要はありません。

このステップでは、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使用して本製品を有効化する必要があります。

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、アクティベーションコードを入力します。

ライセンス情報ファイルを使用して製品をアクティベートするには、ライセンス情報ファイルの絶対パスを指定します。

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が指定されていない場合、試用版ライセンスを使用して 1か月間アクティベートされます。

初期設定スクリプトを使用せずに後で本製品を有効化できます。

自動モードでの製品の初期設定

製品の初期設定を自動モードで実行できます。

製品の自動初期設定を開始するには、次のコマンドを実行します。

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl --autoinstall=<初期設定情報ファイル>
```

<インストール後の設定情報ファイル>は、初期設定情報を含む設定情報ファイルへのパスです。このファイルを作成するか、Kaspersky Security Center を使用して製品のリモートインストールに使用する設定情報ファイル autoinstall.ini から必要な構造をコピーすることができます。

初期設定スクリプトが終了してコンソールが使用できるようになったら、本製品の初期設定は完了しています。

リターンコードを確認するには、次のコマンドを実行します：

```
echo $?
```

コマンドがコード 0 を返した場合、アプリケーションの初期設定は正常に完了しています。

スクリプトの完了後にアプリケーションモジュールを正しくアップデートするには、アプリケーションの再起動が必要になる場合があります。`kesl-control --app-info` コマンドを使用して、アプリケーションのアップデートステータスを確認します。

初期設定情報ファイルの設定

インストール後の設定情報ファイルでは、以下の表に示す設定を指定できます。適用されるアプリケーション設定のセットは、製品の使用モードによって異なります。

初期設定情報ファイルの設定

設定	説明	値
KSVLA_MODE	Kaspersky Endpoint Security の使用モード	［yes］-Kaspersky Endpoint Security は、仮想環境を保護するために Light Agent モードで使用されます（Kaspersky Hybrid Cloud Security for Virtualization Light Agent の一部として）。 ［no］-Kaspersky Endpoint Securityを標準モードで使用します。
SERVER_MODE	保護対象仮想マシンのロール（サーバーまたはワークステーション） この設定は、製品が Light Agent モードで使用されている場合にのみ適用されます。	［yes］- 保護された仮想マシンがサーバーとして使用されます。 ［no］- 保護された仮想マシンはワークステーションとして使用されます。
VDI_MODE	VDI 保護モードを有効にして、一時的な仮想マシン上の製品のパフォーマンスを最適化します。 この設定は、アプリケーションが Light Agent モードで使用されている場合にのみ適用されます。	yes – VDI 保護モードを有効にします。Kaspersky Endpoint Security を一時的な仮想マシンの作成に使用する仮想マシンテンプレートにインストールする場合は、こちらを推奨します。 no – VDI 保護モードを有効にしません。

EULA_AGREED	必須の設定。 使用許諾契約書の条件の同意。	yes – 使用許諾契約書の条項に同意して、製品のインストールを続行する。 no – 使用許諾契約書に同意しない。製品のインストールが中断されます。
PRIVACY_POLICY_AGREED	必須の設定。 プライバシーポリシーの条項の同意。	yes – プライバシーポリシーに同意して、製品のインストールを続行する。 no – プライバシーポリシーに同意しません。製品のインストールが中断されます。
USE_KSN	必須の設定。 Kaspersky Security Network の使用を有効にする：KSN の使用を有効にするには、Kaspersky Security Network に関する声明の条項に同意する必要があります。	yes – Kaspersky Security Network に関する声明の条項に同意し、KSN の使用を有効にします。 no – Kaspersky Security Network に関する声明に同意しない。 Kaspersky Endpoint Security が標準モードで使用されており、KSN の使用を有効にしている場合、アプリケーションのクラウドモードが自動的に有効になります。このモードでは、Kaspersky Endpoint Security はマルウェアデータベースの軽量バージョンを使用します。
GROUP_CLEAN	必須の設定。 ［Kesladmin］および［keslaudit］特権グループからのユーザーの削除。	［yes］- 特権グループからユーザーを削除します。値が yes で［nogroup］グループがない場合、インストールは失敗し、特権グループからユーザーを手動で削除するよう要求されます。 ［no］- 特権グループからユーザーを削除しないでください。
LOCALE	オプション設定。 Kaspersky Security Center に送信される製品イベントに使用されるロケール。	RFC 3066 で指定されている形式のロケール。 Locale 設定が指定されていない場合、オペレーティングシステムのローカリゼーション言語が使用されます。製品がオペレーティングシステムのローカリゼーション言語を判別できなかった場合、またはオペレーティングシステムのローカリゼーションがサポートされていない場合は、既定値の en_US.utf8 が使用されます。 グラフィカルインターフェイスとコマンドラインのロケールは、LANG 環境変数の値によって異なります。Kaspersky Endpoint Security でサポートされていないロケールが LANG 環境変数の値として指定されている場合、グラフィカルインターフェイスとコマンドラインは英語で表示されます。
INSTALL_LICENSE	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。	

	この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。	
UPDATER_SOURCE	アップデート元。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。	SCServer – Kaspersky Security Center 管理サーバーをアップデート元として使用する。 KLServers – カスペルスキーのサーバーをアップデート元として使用する。 アップデート元のアドレス
PROXY_SERVER	インターネットへの接続に使用するプロキシサーバーのアドレス。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。	プロキシサーバーのアドレス
UPDATE_EXECUTE	設定中に製品の定義データベースアップデートタスクを開始する。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。	yes – アップデートタスクを開始する。 no – アップデートタスクを開始しない。
KERNEL_SRCS_INSTALL	カーネルモジュールのコンパイルの自動開始。	yes – カーネルモジュールをコンパイルする。 no – カーネルモジュールをコンパイルしない。
ADMIN_USER	管理者ロール（admin）を割り当てられたユーザー。	
CONFIGURE_SELINUX	Kaspersky Endpoint Security と連携するための SELinux の自動設定。	yes – Kaspersky Endpoint Security と連携するよう SELinux を自動設定する。 no – Kaspersky Endpoint Security と連携するよう SELinux を自動設定しない。
DISABLE_PROTECTION	本製品のインストール後、保護コンポーネントとスキャンタスクを無効にします。	［yes］：インストール後の製品起動時に保護コンポーネントとスキャンタスクを無効にします。 ［no］：インストール後のアプリケーション起動時に保護コンポーネントとスキャンタスクを無効にしません。

	保護コンポーネントを無効にしたインストールは、たとえば、製品の動作における問題を再現し、トレースファイルを作成するのに便利です。 `DISABLE_PROTECTION=yes` パラメータでアプリケーションのインストール後に必要なコンポーネントとタスクを有効にすると、製品の再起動後も有効にされたコンポーネントとタスクが機能し続けます。	
DISABLE_FILEAV_ACTIONS	インストール後のアプリケーションコンポーネントの駆除およびファイル削除機能を無効にします。 駆除およびファイル削除機能が無効で、脅威が検出された場合、アプリケーションは、脅威が検出されたファイルの駆除または削除を試みず、脅威の検出についてユーザに通知するだけです。 アプリケーションをインストールした後、 `kesl.ini` 設定情報ファイルの DisableFileAvActions パラメータを使用して、ファイルの駆除および削除機能を有効にできます。	`yes`：インストール後のアプリケーション起動時に、駆除機能とファイル削除機能を無効にします。 `no`（既定値）：インストール後のアプリケーション起動時に、駆除機能とファイル削除機能を無効にしません。

本製品の初期設定情報ファイルの設定を変更する場合は、設定の値を次の形式で指定します：<設定名>=<設定値>（設定名とその値の間のスペースは処理されません）

SELinux システムの権限の設定

本製品での動作のための SELinux の手動設定

本製品の初期設定時に SELinux の自動設定ができない場合、または自動設定を拒否した場合は、Kaspersky Endpoint Security と連携するように SELinux を手動で設定できます。

本製品で動作するように SELinux を設定します：

1. SELinux を Permissive モードに切り替えます：

   - SELinux がアクティベートされた場合は、次のコマンドを実行します：

     ```
     # setenforce Permissive
     ```

- SELinux が無効になっている場合は、`SELINUX=permissive` 設定を設定情報ファイル /etc/selinux/config で設定し、オペレーティングシステムを再起動します。

2. オペレーティングシステムに semanage 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ます。ユーティリティがインストールされていない場合は、パッケージマネージャに応じて、policycoreutils-python または policycoreutils-python-utils パッケージをインストールします。

3. 既定のターゲットポリシーの代わりにカスタム SELinux ポリシーを使用している場合は、使用している SELinux ポリシーに従って、Kaspersky Endpoint Security の各ソース実行ファイルにラベルを割り当てます。そのためには、次のコマンドを実行します：

   ```
   # semanage fcontext -a -t bin_t <実行ファイル>
   # restorecon -v <実行ファイル>
   ```

   ここでの <実行ファイル> は：

   - /var/opt/kaspersky/kesl/12.1.0.<ビルド番号>_<インストール日時>/opt/kaspersky/kesl/libexec/kesl
   - /var/opt/kaspersky/kesl/12.1.0.<ビルド番号>_<インストール日時>/opt/kaspersky/kesl/bin/kesl-control
   - /var/opt/kaspersky/kesl/12.1.0.<ビルド番号>_<インストール日時>/opt/kaspersky/kesl/libexec/kesl-gui
   - /var/opt/kaspersky/kesl/12.1.0.<ビルド番号>_<インストール日時>/opt/kaspersky/kesl/shared/kesl

4. 次のタスクを実行します：

   - ファイル脅威対策タスク：

     ```
     kesl-control --start-task 1
     ```

   - 簡易スキャンタスク：

     ```
     kesl-control --start-task 4 -W
     ```

   > Kaspersky Endpoint Security の使用中に実行を予定しているすべてのタスクの実行を推奨します。

5. 使用する計画がある場合、グラフィカルユーザーインターフェイスを起動します。

6. audit.log ファイルにエラーがないことを確認します：

   ```
   # grep kesl /var/log/audit/audit.log
   ```

7. audit.log ファイルにエラーがある場合は、そのエラーを修正するためにブロック化レコードに基づいて新しいルールモジュールを作成してダウンロードし、Kaspersky Endpoint Security の使用中に実行する予定のすべてのタスクを再度開始します。そのためには、次のコマンドを実行します：

   ```
   # grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   # semodule -i kesl.pp
   ```

   > Kaspersky Endpoint Security に関する新しい監査メッセージが表示された場合は、ルールモジュールファイルを含むファイルをアップデートする必要があります。

8. SELinux を Blocking モードに切り替えます：

   ```
   # setenforce Enforcing
   ```

カスタム SELinux ポリシーを使用する場合は、製品のアップデートをインストールした後、Kaspersky Endpoint Security のソース実行ファイルに手動でラベルを割り当てる必要があります（手順 1、3〜8 に従ってください）。

詳しくは、お使いのオペレーティングシステムのマニュアルをご覧ください。

「プロセスの開始」タスクの実行のための SELinux の設定

SELinux が `Enforcing` モードでオペレーティングシステムにインストールされている場合、［プロセスの開始］タスクを開始するには、SELinux の追加設定が必要です。

SELinuxを設定して「プロセスの開始」タスクを実行します

1. SELinux を Permissive モードに切り替えます：
   - SELinux がアクティベートされた場合は、次のコマンドを実行します：
     ```
     # setenforce Permissive
     ```
   - SELinux が無効になっている場合は、`SELINUX=permissive` 設定を設定情報ファイル /etc/selinux/config で設定し、オペレーティングシステムを再起動します。
2. オペレーティングシステムに semanage 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ます。ユーティリティがインストールされていない場合は、パッケージマネージャに応じて、policycoreutils-python または policycoreutils-python-utils パッケージをインストールします。
3. 「プロセスの開始」タスクを開始します。
4. audit.log ファイルにエラーがないことを確認します：
   ```
   # grep kesl /var/log/audit/audit.log
   ```
5. audit.log ファイルにエラーが存在する場合は、ブロックルールに基づいて新しいルールモジュールを作成して読み込み、エラーを修正してから、「プロセスの開始」タスクを再度実行します。
   ```
   # grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   # semodule -i kesl.pp
   ```
6. SELinux を Blocking モードに切り替えます：
   ```
   # setenforce Enforcing
   ```

閉鎖ソフトウェア環境モードの Astra Linux OS での本製品の実行

このセクションでは、Astra Linux Special Edition オペレーティングシステムで本製品を起動する方法について説明します。

Astra Linux Special Edition (regular update 1.7)、Astra Linux Special Edition (regular update 1.6) の場合

Astra Linux Special Edition (regular update 1.7)、または Astra Linux Special Edition (regular update 1.6) のオペレーティングシステムで本製品を起動するには、以下の操作を実行します：

1. ファイル /etc/digsig/digsig_initramfs.conf で、次の設定を指定します：

   ```
   DIGSIG_ELF_MODE=1
   ```

2. 互換性パッケージをインストールします：

   ```
   apt install astra-digsig-oldkeys
   ```

3. 本製品のライセンス用のディレクトリを作成します：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. 本製品のライセンス（/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg）を、前のステップで作成したディレクトリで見つけます。

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. initramfs イメージを更新します：

   ```
   update-initramfs -u -k all
   ```

Astra Linux Special Edition (operational update 1.5) の場合

Astra Linux Special Edition (operational update 1.6) オペレーティングシステムで本製品を実行する場合、次を実行します：

1. ファイル /etc/digsig/digsig_initramfs.conf で、次の設定を指定します：

   ```
   DIGSIG_LOAD_KEYS=1
   DIGSIG_ENFORCE=1
   ```

2. 本製品のライセンス用のディレクトリを作成します：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

3. 本製品のライセンス（/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg）を、前のステップで作成したディレクトリで見つけます。

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

4. initramfs イメージを更新します：

   ```
   sudo update-initramfs -u -k all
   ```

本製品のグラフィカルユーザーインターフェイスは、必須のアクセスコントロールのセッションで使用できます。

旧バージョンからの本製品のアップデート

Kaspersky Endpoint Security 12.1 for Linuxにアップデート可能なバージョンは、Kaspersky Endpoint Security 12.0 for Linuxのみです。

Kaspersky Endpoint Security の以前のバージョンからバージョン 12.1 へのアップグレードはサポートされていません。以前のバージョンの Kaspersky Endpoint Security がインストールされている場合は、アンインストールしてから Kaspersky Endpoint Security 12.1 for Linux をインストールする必要があります。

Kaspersky Endpoint Security をインストールする前に、インストールの準備をする必要があります。

アプリケーションのアップデート手順には、次の手順が含まれます。

1. **Kaspersky Security Center ネットワークエージェントのアップデート**

   Kaspersky Security Center を使用して Kaspersky Endpoint Security を管理している場合は、保護対象デバイス上のネットワークエージェントをアップデートする必要があります。アップデートは、ネットワークエージェントの新しいバージョンをインストールすることで実行されます。

   ネットワークエージェントがアップデートされていない場合、本製品を Kaspersky Security Center で管理することはできません。

   > Astra Linux Special Edition オペレーティングシステムのデバイスでは、ネットワークエージェントを Kaspersky Security Center を使用してリモートでアップデートしてください。Kaspersky Security Center 管理コンソールでコマンドラインを使用してアップデートすると、同じ管理対象デバイスの新しいコピーが作成されるため、古いコピーにアクセスできなくなります。

   ネットワークエージェントのアップデート中、本製品は正常に機能し続けます。

2. **Kaspersky Endpoint Security 管理プラグインのアップデート**

   Kaspersky Security Center を使用して Kaspersky Endpoint Security を管理している場合は、 Kaspersky Security Center の管理に使用しているコンソールに応じて、Kaspersky Endpoint Security 管理 Web プラグインまたは MMC プラグインをアップデートする必要があります。

3. **保護対象デバイス上の製品とグラフィカルユーザーインターフェイスの更新**

   保護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をアップデートする必要があります。アップデートされたアプリケーションは、インストール時に選択されたアプリケーション使用モードを保持します。アプリケーションを別のモードで使用する場合は、アプリケーションをアンインストールしてから、アプリケーションのインストールと初期設定を実行する必要があります。

   Kaspersky Endpoint Security を標準モードで使用しており、アプリケーションのグラフィカルユーザー インターフェイスを使用している場合は、グラフィカルユーザー インターフェイスもアップデートする必要があります。

   アプリケーションとアプリケーションのグラフィカルユーザーインターフェースは、次の方法でアップデートできます：

   - Kaspersky Security Center を使用してリモートでアップデートする。
   - コマンドラインを使用してローカルでアップデートする。

製品のアップデート中にエラーが発生した場合、アップデートはロールバックされ、以前のバージョンの製品が起動します。この場合、エラーメッセージが表示されますが、パッケージマネージャー（rpm/dpkg）が新しいバージョンを示します。

Kaspersky Endpoint Security がアップデートプロセスの前に起動しても、アップデートが正常に完了すると、新しい製品バージョンが起動します。

アプリケーションを新しいバージョンにアップデートすると、以前のバージョンのダンプ ファイルは削除されます。

Kaspersky Endpoint Security を標準モードで使用している場合は、アプリケーションをアップデートした後にデータベースアップデートタスクを開始することをお勧めします。

Kaspersky Endpoint Security 管理プラグインのアップデート

Kaspersky Endpoint Security の管理プラグインは、新しいバージョンの管理プラグインをインストールすることで更新されます。使用する Kaspersky Security Center 管理コンソールに応じて、次のプラグインをインストールする必要があります：

- Kaspersky Endpoint Security Web 管理プラグイン
- Kaspersky Endpoint Security MMC 管理プラグイン

Kaspersky Endpoint Security 12.0 for Linux 用に設定されたポリシーとタスクは、本製品の更新バージョンと互換性がありません。Kaspersky Security Center 管理コンソールを使用して本製品を管理する場合は、管理 MMC プラグインを更新した後、Kaspersky Security Center ポリシーとタスクのバッチ変換ウィザードを使用してポリシーとタスクを変換できます（詳細については、Kaspersky Security Center ヘルプ を参照してください）。

ほとんどの設定では、変換されたポリシーとタスクは、本製品の以前のバージョンに対して設定された値を使用します。一部の設定には特別な値が割り当てられています。以前のバージョンのポリシーとタスクで構成されていなかった設定は、変換されたポリシーとタスクでは既定値になります。

ポリシーとタスクを変換する手順は、Kaspersky Security Center Web コンソールでは利用できません。Web コンソールを使用して本製品を管理する場合は、Kaspersky Security Center で本製品の新しいポリシーとタスクを作成する必要があります。設定をエクスポートおよびインポートすることで、ポリシーおよびタスクの設定の一部を、以前のバージョンのポリシーまたはタスクから新しいバージョンに移行できます。

以前のバージョンの管理プラグインは、新しいバージョンの Kaspersky Endpoint Security 管理プラグインをインストールした後も引き続き機能します。これらを使用して、Kaspersky Endpoint Security の以前のバージョンを管理できます。

すべてのクライアントデバイスでアプリケーションを更新した場合は、以前のバージョンの Kaspersky Endpoint Security 管理プラグインをアンインストールできます。

Kaspersky Security Center を使用した本製品のアップデート

アプリケーションとグラフィカルユーザーインターフェースは、保護されたデバイスに新しいバージョンのアプリケーションパッケージとグラフィカルユーザーインターフェースをリモートでインストールすることによって更新されます。

仮想環境の保護に Kaspersky Endpoint Security Light Agent モードを使用している場合、グラフィカルユーザーインターフェイスはサポートされません。

リモートインストールに、Kaspersky Endpoint Security インストールパッケージを使用します。インストールパッケージを作成するには、Kaspersky Security Center Web コンソールまたは管理コンソールを使用します。

Kaspersky Security Center Web コンソールがサポートする主要な導入方法は、次の通りです：

- 保護展開ウィザードを使用してアプリケーションをインストールします。
- リモートインストールタスクを使用したインストール。

Kaspersky Security Center 管理コンソールでは、主に次の導入方法をサポートしています：

- リモートインストールウィザードを使用して製品をインストールします。
- リモートインストールタスクを使用したインストール。

導入手順については、Kaspersky Security Center のヘルプを参照してください。

コマンドラインを使用した本製品のアップデート

コマンドラインを使用したアプリケーションのアップデートは、パッケージ マネージャーの種類に応じて、RPM または DEB 形式のパッケージから新バージョンのアプリ ケーションをデバイスにインストールすることで実行されます。

グラフィカルユーザーインターフェースを使用している場合、更新にはまず `rpm -e --nodeps kesl-gui` というコマンドを使用して以前のバージョンのグラフィカルユーザーインターフェースパッケージをアンインストールしてから、グラフィカルユーザーインターフェースのバージョン12.1用のファイルを含むパッケージをインストールする必要があります。

> 仮想環境の保護に Kaspersky Endpoint Security Light Agent モードを使用している場合、グラフィカルユーザーインターフェイスはサポートされません。

使用許諾契約書およびプライバシーポリシーの条件がアプリケーションの新しいバージョンで変更されている場合は、アップデート中に新しい条件に同意する必要があります。使用許諾契約書およびプライバシーポリシーの新バージョンをお読みください：

- 新バージョンの使用許諾契約書は、ディレクトリ（~/.kesl/<アプリケーションバージョン>/license.<言語 ID>）にあります。
- 新バージョンのプライバシーポリシーは、ディレクトリ（~/.kesl/<アプリケーションバージョン>/license.<言語ID>）にあります。

使用許諾契約書とプライバシーポリシーのいずれかまたは両方の条件に同意しない場合、本製品はアップデートされません。

本製品の新しいバージョンで Kaspersky Security Network に関する声明の条項が変更された場合は、Kaspersky Security Network に参加するための新しい使用条項に同意するかどうかを指定する必要があります。ディレクトリ (~/.kesl/<アプリケーションバージョン>/ksn_license.<言語 ID> にある新しいバージョンの文書をお読みください。Kaspersky Security Network への参加に同意しなくても、Kaspersky Endpoint Security のアップデートプロセスは中断されません。Kaspersky Security Network のモードの有効化、無効化、変更は、後ででも行えます。

本製品の以前のバージョンで KSN を使用し、Kaspersky Security Network に関する声明の条件に同意した場合は、本製品のアップデート時に Kaspersky Security Network に関する声明の条件に同意する必要があります。そうしないと、KSN の使用が無効になります。

アップデート中に新しい契約条件に同意するには、環境変数 `KESL_EULA_AGREED=yes`、`KESL_PRIVACY_POLICY_AGREED=yes`、 `KESL_USE_KSN=yes/no` を使用します。

アプリケーションをアップデートするには：

1. パッケージマネージャーに応じて、次のコマンドを使用してアプリケーションパッケージをインストールします。以前のバージョンのグラフィカルユーザーインターフェイスをインストールしている場合は、グラフィカルユーザーインターフェイスのファイルを含むパッケージも起動する必要があります。

   - RPM パッケージの場合

     `# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] rpm -U --replacefiles --replacepkgs kesl-12.1.0-<ビルド番号>.<arch>.rpm [kesl-gui-12.1.0-<ビルド番号>.<arch>.rpm]`

     `<arch>` はアーキテクチャの種別：

     - i386 – 32 ビットオペレーティングシステム
     - x86_64 – 64 ビットオペレーティングシステム
     - aarch64 – ARM アーキテクチャの 64 ビットオペレーティングシステム

     > rpm ベースのオペレーティングシステムでは、製品パッケージと GUI パッケージの両方がインストールされている場合、一方のパッケージをアップデートせずにもう一方のパッケージをアップデートすることは推奨しません。

   - DEB パッケージの場合

     `# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] apt-get install./kesl_12.1.0-<ビルド番号>_<arch>.deb [./kesl-gui_12.1.0-<ビルド番号>_<arch>.deb]`

     `<arch>` はアーキテクチャの種別：

     - i386 – 32 ビットオペレーティングシステム
     - amd64 – 64 ビットオペレーティングシステム
     - arm64 – ARM アーキテクチャの 64 ビットオペレーティングシステム

     > dpkg ベースのオペレーティングシステムでは、製品パッケージと GUI パッケージの両方がインストールされている場合、どちらか一方のパッケージをアップデートしないと、もう一方のパッケージをアップデートできません。

2. Kaspersky Endpoint Security が自動的に再起動されます。

3. 一部のオペレーティングシステムの再起動が必要になる場合があります。必要な場合、アプリケーションは対応するメッセージを表示します。

コマンドラインを使用して本製品を管理する場合、アップグレード後、ほとんどの製品設定では、製品の以前のバージョンに対して構成された値が使用されます。一部の設定には特別な値が割り当てられています。本製品の以前のバージョンになかった設定は、新しいバージョンでは既定値になります。

アップデートが完了した後、アプリケーションの再起動前にアプリケーションの設定に加えられた変更は保存されません。

本製品の更新時にパラメータ値を設定する際の特別な考慮事項

Kaspersky Security Center 管理コンソールを使用して本製品を管理し、本製品のアップデート後に、以前のバージョン用に Kaspersky Security Center で構成されたポリシーとタスク設定の値を使用する場合は、ポリシーとタスクを変換する必要があります（詳細は、Kaspersky Security Center ヘルプを参照してください）。

ポリシーとタスクを変換する手順は、Kaspersky Security Center Web コンソールでは利用できません。Web コンソールを使用して本製品を管理する場合は、更新されたバージョンに対して新しいポリシーとタスクを作成する必要があります。設定をエクスポートおよびインポートすることで、ポリシーおよびタスクの設定の一部を、以前のバージョンのポリシーまたはタスクから新しいバージョンに移行できます。

コマンドラインでは、ほとんどの設定が製品の以前のバージョンから移行されます。設定をファイルにエクスポートし、そのファイルから設定をインポートすることで、製品設定を移行できます。

製品の以前のバージョンには存在しなかった設定には既定値が割り当てられます。一部の設定には特別な値が割り当てられています。

除外設定

MMC プラグインでタスクが変換されると、スキャン タスク（ODS 種別）およびコンテナースキャンタスクで［**グローバル除外を使用する**］および［**ファイル脅威保護除外を使用する**］チェックボックスがオフになります。タスクの変換は Web プラグインではサポートされていません。

コマンドラインで製品をアップデートすると、`UseOASExclusions` および `UseGlobalExclusions` 設定が `No` に設定されます。

Kaspersky Security Network の設定

MMC プラグインでポリシーを変換したら、ポリシーのプロパティで［**Kaspersky Endpoint Security を使用しない**］オプションが選択されます。ポリシーの変換は Web プラグインではサポートされていません。

コマンドラインで製品をアップグレードした後、アップデート時に `KESL_USE_KSN=No` を設定した場合は UseKSN 設定が `No` に設定され、`KESL_USE_KSN=Yes` を設定した場合は `UseKSN=Extended` が適用されます。それ以外の場合、`UseKSN` 設定の値は更新後も変更されません。

Kaspersky Security Network の使用を開始または再開するには、次の手順を実行する必要があります：

- MMC または Web プラグインを使用する場合は、**基本 KSN モード**または**拡張 KSN モード**を選択します。
- コマンドラインを使用する場合は、`UseKSN` を `Basic` または `Extended` に設定します。

クラウドモード設定

MMC プラグインでポリシーを変換すると、［**クラウドモードを有効にする**］チェックボックスがオフになります。ポリシーの変換は Web プラグインではサポートされていません。

コマンドラインで製品をアップデートすると、`CloudMode` は次のように設定されます：

- アップグレード後に `UseKSN=No` が設定されている場合は `CloudMode=No` になります。
- アップグレード後に `UseKSN=Yes` が設定され、アップグレード前に `CloudMode=Yes` が設定されていた場合は、`CloudMode=Yes` になります。

KSN の使用が有効になっている場合、クラウドモードを使用できます。クラウドモードを有効にします：

- MMC または Web プラグインを使用する場合は、［**拡張 KSN モード**］オプションを選択し、［**クラウドモードを有効にする**］チェック ボックスをオンにします。
- コマンドラインを使用する場合は、`UseKSN` と `CloudMode` を［`Yes`］に設定します。

ファイル操作遮断モード

本製品の以前のバージョンで［**スキャン中にファイルへのアクセスをブロックする**］チェックボックスがオフになっていた場合、MMC プラグインでポリシーを変換すると、ファイル脅威対策タスクの**最初の処理**が［**ブロック**］に設定されます。ポリシーの変換は Web プラグインではサポートされていません。

本製品の新バージョンでは、ファイル操作遮断モードを決定するコマンドラインオプションの名前が、`InterceptorProtectionMode=Block|Notify` から `FileBlockDuringScan=Yes|No` に変更されました。以前のバージョンで `InterceptorProtectionMode` が［`Notice`］に設定されていた場合、コマンドラインを使用して本製品をアップデートすると、`FileBlockDuringScan` は［`No`］に設定され、ファイル脅威対策タスクの `FirstAction` 設定は［`Block`］に設定されます。

本製品のアンインストール

Kaspersky Endpoint Security をアンインストールするには、次の手順を実行します。

1. **アプリケーションとアプリケーションのグラフィカルユーザーインターフェイスのアンインストール**

   保護対象デバイスからアプリケーションのパッケージをアンインストールし、グラフィカルユーザーインターフェイスを使用している場合は、グラフィカルユーザーインターフェイスのパッケージもアンインストールします。

   アプリケーションパッケージとグラフィカルユーザーインターフェイスパッケージの両方をアンインストールすることも、グラフィカルユーザーインターフェイスパッケージのみをアンインストールすることもできます。グラフィカルユーザーインターフェイスパッケージがインストールされている場合、製品パッケージのみをアンインストールすることはできません。

   アプリケーションおよびアプリケーションのグラフィカルユーザーインターフェースは、次の方法でアンインストールできます：

   - Kaspersky Security Center を使用してリモートでアップデートする。
   - コマンドラインを使用してローカルでアップデートする。

   > アプリケーションのアンインストール中は、デバイス上の Kaspersky Endpoint Security のすべてのタスクが停止されます。

2. **ネットワークエージェントの削除**

   Kaspersky Security Center を使用して Kaspersky Endpoint Security を管理していた場合は、保護対象デバイスからネットワークエージェントをアン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をアンインストールするには、次の方法があります：

   - Kaspersky Security Center を使用してリモートでアップデートする。
   - コマンドラインを使用してローカルでアップデートする。

3. **Kaspersky Endpoint Security 管理プラグインのアンインストール**

   Kaspersky Security Center を使用して Kaspersky Endpoint Security を管理していた場合は、 Kaspersky Security Center の管理に使用していたコンソールに応じて、 Kaspersky Endpoint Security 管理 Web プラグインまたは MMC プラグインをアンインストールする必要があります。

> 本製品をアンインストールすると、ライセンス データベースを除く、アプリケーションによって保存されたすべての情報が削除されます。インストール済みのアプリケーション証明書も削除されます。ライセンスデータベースが保存され、それを使用してアプリケーションを再インストールできます。

アプリケーションが systemd にインストールされている場合、systemd の設定は、アプリケーションのアンインストール後に初期状態にリストアされます。

Kaspersky Security Center を使用してアプリケーションとネットワークエージェントをアンインストールします

Kaspersky Endpoint Security および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できます。

アンインストールは、Kaspersky Security Center Web コンソールまたは管理コンソールの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実行します。詳細については、Kaspersky Security Center のヘルプシステムを参照してください。

製品を削除せずにグラフィカルユーザーインターフェイスのみを削除する場合は、設定情報ファイル autoinstall.ini で設定値を `USE_GUI=No` に指定し、リモートでインストールタスクを開始します。

アンインストールはバックグラウンドで実行されます。本製品のアンインストールが完了すると、クライアントデバイスの再起動が求められます。

コマンドラインを使用した本製品のアンインストール

製品パッケージとグラフィカルユーザーインターフェイスパッケージのアンインストール

RPM パッケージからインストールされたアプリケーションおよびグラフィカルユーザーインターフェイスをアンインストールするには、次のコマンドを実行します：

```
# rpm -e kesl kesl-gui
```

DEB パッケージからインストールされたアプリケーションおよびグラフィカルユーザーインターフェイスをアンインストールするには、次のコマンドを実行します：

```
# apt-get purge kesl kesl-gui
```

製品パッケージのアンインストール（グラフィカルユーザーインターフェイスパッケージなし）

RPM パッケージからインストールしたアプリケーションを、グラフィカルユーザーインターフェイスを削除せずにアンインストールする場合は、次のコマンドを実行します：

```
# rpm -e kesl
```

DEB パッケージからインストールしたアプリケーションを、グラフィカルユーザーインターフェイスを削除せずにアンインストールする場合は、次のコマンドを実行します：

```
# apt-get purge kesl
```

グラフィカルユーザーインターフェイスパッケージの削除

RPM パッケージからインストールされたグラフィカルユーザーインターフェイスを削除するには、次のコマンドを実行します：

```
# rpm -e kesl-gui
```

DEB パッケージからインストールされたグラフィカルユーザーインターフェイスを削除するには、次のコマンドを実行します：

```
# apt-get purge kesl-gui
```

アンインストールが完了すると、アンインストールの結果に関するメッセージが表示されます。

コマンドラインを使用したネットワークエージェントの削除

32 ビットオペレーティングシステム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 RPM パッケージからアンインストールするには、次のコマンドを実行します：

```
# rpm -e klnagent
```

64 ビットオペレーティングシステム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 RPM パッケージからアンインストールするには、次のコマンドを実行します：

```
# rpm -e klnagent64
```

32 ビットオペレーティングシステム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 DEB パッケージからアンインストールするには、次のコマンドを実行します：

```
# apt-get purge klnagent
```

64 ビットオペレーティングシステム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 DEB パッケージからアンインストールするには、次のコマンドを実行します：

```
# apt-get purge klnagent64
```

アンインストールが完了すると、アンインストールの結果に関するメッセージが表示されます。

Kaspersky Endpoint Security 管理プラグインのアンインストール

Kaspersky Endpoint Security Web 管理プラグインは、Kaspersky Security Center Web Console のインストール済みプラグイン一覧（**設定 → Web プラグイン**）からアンインストールします。

MMC プラグインをアンインストールするには、オペレーティングシステムのアプリケーションをアンインストールするための標準ツールを使用します。アプリケーションの一覧で、アンインストールする **Kaspersky Endpoint Security <バージョン番号> for Linux** を選択します。

本製品のライセンス管理

このセクションでは、Kaspersky Endpoint Security のライセンスの情報について説明します。

使用許諾契約書の概要

*使用許諾契約書*は、ユーザーと AO Kaspersky Lab との間で締結される契約で、製品を使用できる条件を明記しています。

使用許諾契約書の条項をよくお読みになり、本製品の使用を開始してください。

Kaspersky Endpoint Security ソリューションの使用許諾契約書の条項と、データの処理および転送について規定したプライバシーポリシーは、次の方法で確認できます：

- license.<言語 ID> ファイルの内容の確認。このファイルには本製品の配布キットが含まれています。
- Kaspersky Endpoint Security インストール中。

  本製品のインストールパッケージを作成するとき（Kaspersky Security Center を使用してインストールした場合）、または本製品の初期設定中（コマンドラインを使用してインストールした場合）に、使用許諾契約書とプライバシーポリシーのテキストに同意することを確認することで、使用許諾契約書とプライバシーポリシーの条件に同意したことになります。使用許諾契約書またはプライバシーポリシーの条件に同意しない場合は、本製品のインストールをキャンセルし、本製品を使用してはなりません。

- Kaspersky Endpoint Security のインストール後。

  本製品がインストールされると、Kaspersky Endpoint Security 使用許諾契約書とプライバシーポリシーのテキストを含むファイルが、保護対象デバイスの /opt/kaspersky/kesl/doc/license に保存されます。<language ID> フォルダ。

ライセンスの概要

*ライセンス*とは、Kaspersky Endpoint Security の期間限定の使用権であり、使用許諾契約書に基づいて付与されます。

使用可能な機能のリストと製品の有効期間は、製品が使用されるライセンスによって異なります。

ライセンス種別には、以下があります：

- *試用版* - 製品をお試しいただくための無償ライセンス。

  試用版ライセンスの有効期間は短く設定されています。試用版の有効期間が終了すると、すべての Kaspersky Endpoint Security の機能が無効になります。製品を引き続き使用するには、製品版ライセンスを購入する必要があります。

  トライアルライセンスでアプリケーションを使用できるのは、1回のトライアル期間のみです。

- *コマーシャル*は有料ライセンスです。

製品版ライセンスの有効期限が切れると、本製品の主な機能は動作を停止します。Kaspersky Endpoint Security 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。ライセンスの有効期限が切れると、アプリケーションは使用できなくなり、デバイスからアンインストールする必要があります。

セキュリティの脅威からデバイスを継続的に保護するために、有効期限が切れる前にライセンスをアップデートすることを推奨します。

ライセンス証明書の概要

*ライセンス証明書*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と一緒に提供される文書です。

ライセンス証明書には、提供されるライセンスに関する次の情報が含まれます：

- 識別 ID または注文番号
- ライセンスユーザーに関する情報
- 提供されたライセンスを使用してアクティベーションを実行可能な製品の情報
- ライセンス単位数の制限（このライセンスで本製品を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限または有効期間
- ライセンス種別

ライセンスの概要

*ライセンス*は、製品のアクティベーションに使用される数値列で、使用許諾契約書の条件に応じて製品を使用できるようにします。ライセンスは、カスペルスキーにより生成されます。

製品にライセンスを追加するには、*ライセンス情報ファイル*を適用するか、*アクティベーションコード*を入力します。製品にライセンスを追加すると、一意の英数字の並びとしてライセンスが製品インターフェイスに表示されます。

使用許諾契約書の条項に違反した場合、カスペルスキーによりライセンスがブロックされることがあります。ライセンスがブロックさた場合、製品を適切に操作するには別のライセンスを追加します。

Kaspersky Endpoint Security 製品は、次の*種別*のライセンスに対応しています。

- *製品ライセンス* – Kaspersky Endpoint Security 製品の機能を有効にするためのライセンス。利用可能な製品機能のセットは、製品ライセンスに関連付けられたライセンスによって異なります。
- *EDR Optimum ライセンス* – Kaspersky Endpoint Detection and Response Optimum の機能を有効にするための、Kaspersky Endpoint Detection and Response Optimum アドオンの追加ライセンス。Kaspersky Endpoint Detection and Response Optimum の機能が含まれていないライセンスで本製品を使用している場合は、このライセンスが必要です。

ライセンスには、現在のライセンスと予備のライセンスがあります。

*現在のライセンス*は、本製品の実行のために現在使われているライセンスです。試用版ライセンス、製品版ライセンス、または定期性サービスライセンスを現在のライセンスとして追加できます。本製品に追加できる現在の乱センスは、種別ごとに1つだけです。

*予備のライセンス*は、製品を使用するユーザーに権利を与えるもので、現在使用されていないライセンスです。現在のライセンスの有効期間が終了すると、予備のライセンスが自動的に現在のライセンスとなります。予備のライセンスは、現在と同じ種別のライセンスが既に追加されてい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または定額制サービス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の概要

*アクティベーションコード*は、20 桁の英数字で構成される一意の文字の並びです。Kaspersky Endpoint Security のアクティベートしてライセンスを追加するには、アクティベーションコードを入力する必要があります。Kaspersky Endpoint Security の購入時または試用版の Kaspersky Endpoint Security の要求時に登録したメールアドレスで、アクティベーションコードを受け取ります。

アクティベーションコードを使用して製品のアクティベーションを実行するには、カスペルスキーのアクティベーションサーバーへの接続時にインターネット接続が確立されている必要があります。

製品をアクティベートした後にアクティベーションコードを紛失した場合は、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。

ライセンス情報ファイルの概要

*ライセンス情報ファイル*は、カスペルスキーが提供する、拡張子が「key」のファイルです。ライセンス情報ファイルは、製品をアクティベートするためのライセンスを追加することを目的としています。

Kaspersky Endpoint Security の購入時または試用版の Kaspersky Security の注文時に登録したメールアドレスで、ライセンス情報ファイルを受け取ります。

ライセンス情報ファイルを使って本製品のアクティベーションを実行するために、カスペルスキーのアクティベーションサーバーに接続する必要はありません。

誤ってライセンス情報ファイルを削除してしまった場合は、復元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を登録する際に、ライセンス情報ファイルが必要になる場合があります。

ライセンス情報ファイルを復元する方法は次のいずれかです：

- ご購入元の販売代理店へ問い合わせる。
- アクティベーションコードがある場合、カスペルスキーの Web サイトでライセンス情報ファイルを取得する。

定額制サービスの概要

Kaspersky Endpoint Security の定額制サービスは、特定の設定（定額制サービスの有効期限が切れる日、保護されるデバイスの数）を使用した製品の購入注文です。Kaspersky Endpoint Security の定額制サービスをサービスプロバイダー（インターネットサービスプロバイダーなど）から注文できます。定額制サービスを更新またはキャンセルできます。サービスプロバイダーの Web サイトで定額制サービスを管理できます。

定額制サービスは、制限すること（1年など）も、無制限にすること（有効期限なし）もできます。制限付き定額制サービスの有効期間の終了後も本製品の使用を継続するには、定額制サービスを更新する必要があります。無制限の定額制サービスは、プロバイダーのサービスが期限通りに前払いされた時に、自動的に更新されます。

制限付き定額制サービスの有効期限が切れると、定額制サービスを更新するための猶予期間が提供される場合があります。この期間中は、製品の機能に制限なく使用できます。サービスプロバイダーにより猶予期間が付与されるかどうかが決定され、付与する場合は猶予期間の長さを決定されます。

定額制サービスを管理するための一連のオプションは、サービスプロバイダーによって異なる場合があります。サービスプロバイダーは、製品の機能に制限なく動作している場合、定額制サービスを更新するための猶予期間を提供しない場合があります。

定額制サービスで Kaspersky Endpoint Security を使用するには、サービスプロバイダーから取得したアクティベーションコードを使用する必要があります。アクティベーションコードの適用後、定額制サービスで製品を使用するためのライセンスに対応する現在のライセンスがアプリケーションに追加されます。予備のライセンスは、アクティベーションコードを使用する場合にのみ追加でき、ライセンス情報ファイルまたは定額制サービスには追加できません。

定額制サービスで購入されたアクティベーションコードは、Kaspersky Endpoint Security の以前のバージョンのアクティベートに使用できない場合があります。

異なるライセンス間の製品機能の比較

Kaspersky Endpoint Security で使用可能な製品機能は、ライセンスによって異なります（下の表を参照）。

製品機能の比較は、Intel アーキテクチャプロセッサに基づくソリューションに基づいています。Arm アーキテクチャに基づくソリューションのライセンスと利用可能な機能の詳細については、お住まいの地域のサービスプロバイダーにお問い合わせください。

製品機能の比較

機能	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Endpoint Security for Business Total	Kaspersky Hybrid Cloud Security（Desktop）	Kaspersky Security for Virtualization（Desktop）	Kaspe Securit Ent
ファイル脅威対策	✓	✓	✓	✓	✓	
ウェブ脅威対策	✓	✓	✓	✓	✓	
ネットワーク脅威	✓	✓	✓	✓	✓	

対策						
ファイアウォール管理	✓	✓	✓	✓	✓	
ふるまい検知	✓	✓	✓	✓	✓	
デバイスコントロール	✓	✓	✓	✓	✓	
リムーバブルドライブのスキャン	✓	✓	✓	✓	✓	
アンチクリプター（共有フォルダー用）	✓	✓	✓	–	–	
コンテナースキャン	–	–	–	–	–	
システム変更監視	–	–	–	–	–	
アプリケーションコントロール	–	✓	✓	✓	✓	
ウェブコントロール	✓	✓	✓	✓	✓	
Kaspersky Endpoint Detection and Response Optimum の連携	–	–	–	–	–	

データの提供

このセクションは、Kaspersky Endpoint Security がデバイス上に保存し、操作中にカスペルスキーに自動送信する可能性のある情報について説明しています。

カスペルスキーは、法律と該当するカスペルスキーのルールに従って、受信した情報を保護します。データは暗号化された通信で転送されます。

本製品の使用中に取得した情報の処理、保存、破棄、およびカスペルスキーへ送信される情報についての詳細は、カスペルスキーの Web サイトにある使用許諾契約書、KSN に関する声明、プライバシーポリシーをお読みください。license.<言語 ID> ファイルと ksn_license.<言語 ID> ファイルには使用許諾契約書と Kaspersky Security Network に関する声明が記載されており、製品の配布パッケージに組み込まれています。

アクティベーションコードを使用する時に提供されるデータ

アクティベーションコードを使用して標準モードで Kaspersky Endpoint Security をアクティベートする場合、製品が合法的に使用されているかどうかを確認し、製品の配布と使用に関する統計情報を取得するために、以下の情報を自動的にカスペルスキーに提供することに同意するものとします：

- インストールされているアプリケーションの種別、バージョン、ローカリゼーション
- インストールされている本製品のアップデートのバージョン
- デバイス ID とデバイス上の製品のインストール ID
- 本製品を有効化するために使用されたアクティベーションコード
- 現在のライセンスの ID
- 本製品のライセンスの作成日時
- ユーザーデバイスの日時
- 製品ライセンスの有効期限の日時
- オペレーティングシステムの種別、バージョン、ビットサイズ

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する時に提供されるデータ

Kaspersky Endpoint Security を標準モードで使用し、カスペルスキーのアップデートサーバーを使用してアップデートをダウンロードする場合、アップデート手順の効率を高め、製品の配布と使用に関する統計情報を取得するために、以下の情報を自動的にカスペルスキーに提供することに同意するものとします：

- ライセンスに基づく本製品の識別子
- 本製品の詳細バージョン
- 本製品のライセンスの識別子

- 使用された本製品のライセンスの種別
- 本製品のインストールの識別子（PCID）
- 本ソフトウェアのアップデート開始の識別子
- 処理中の URL

Light Agent モードで本製品を使用する際に転送されるデータ

Kaspersky Security for Virtualization Light Agent の一部として仮想環境を保護するために Kaspersky Endpoint Security を Light Agent モードで使用する場合、アプリケーションは個人データや機密データが含まれる可能性がある次の情報を保存し、アプリケーションの動作中に他のソリューションコンポーネントに送信します。

- アクティベーションの場合、Kaspersky Endpoint Security は、ライセンスのステータス確認の有効期間、保護対象仮想マシンの BIOS ID、Light Agent の動作に必要なライセンスに関する情報などのデータを Protection Server に送信します。
- Light Agent データベースをアップデートするために、Kaspersky Endpoint Security は次のデータを Protection Server に送信します：ライセンスから取得したソフトウェア識別子、ソフトウェアのフルバージョン、ソフトウェアライセンス識別子、ソフトウェアインストール識別子（PCID）、処理された Web アドレス、ライセンスの種類、更新開始の識別子。
- 保護を提供するために、Kaspersky Endpoint Security は、スキャンタスクの実行中にオブジェクトのスキャンに必要な情報を Protection Server に送信します。送信される情報には、ファイルの名前とファイルシステム内のファイルへのパス、ファイルチェックサム、Web アドレス、スキャンされたオブジェクトまたはそのフラグメントが含まれる場合があります。
- VMware vCenter Server および VMware NSX Manager によって管理されるインフラストラクチャでは、Kaspersky Endpoint Security は、ウイルス、マルウェア、またはネットワーク攻撃に典型的なアクティビティの検知時に、保護対象仮想マシンに割り当てられているセキュリティタグに関する情報を Integration Server に送信する場合があります。保護対象仮想マシンの ID も送信されます。
- 接続する SVM を選択する時に使用される情報を取得するために、Kaspersky Endpoint Security は、保護対象仮想マシンの識別子を Integration Server と Protection Server に送信します。
- Kaspersky Security for Virtualization Light Agent ソリューションをマルチテナントモードで使用する場合、テナント保護レポートの生成に必要な情報が Kaspersky Endpoint Security Protection Server から SVM に送信されることがあります。次のデータが送信される場合があります：保護対象仮想マシンの識別子、保護対象仮想マシンにインストールされているゲストオペレーティングシステムの種類とバージョン、Kaspersky Endpoint Security が SVM に接続された時間間隔。
- 統計を取得するために、Kaspersky Endpoint Security は次の情報を Protection Server に送信します：保護対象仮想マシンの OS バージョンに関する情報、Kaspersky Endpoint Security のローカリゼーション、現在の Kaspersky Endpoint Security コンポーネントの名前、保護対象仮想マシンの識別子（BIOS ID）。

指定された情報は、暗号化されたデータチャネルを介して送信されます（オブジェクトのスキャンに必要な情報と、SVM の選択時に使用される情報を除く）。Kaspersky Endpoint Security と Protection Server の接続は、規定では暗号化されません。Kaspersky Endpoint Security 設定で、Light Agent と Protection Server 間のデータチャネルの暗号化を有効にできます。

Kaspersky Security Center に送信されるデータ

Kaspersky Endpoint Security は、動作中に以下の情報を保存して Kaspersky Security Center に送信します。それらの情報には、個人データや機密データが含まれている場合があります：

- 本製品で使用されるデータベースに関する情報：
  - 本製品に必要なデータベースカテゴリのリスト
  - データベースが公開され、本製品にロードされた日時
  - ダウンロードした本製品の定義データベースのアップデートがリリースされた日付
  - 本製品の定義データベースの最新アップデートの日時
  - 現在使用されている定義データベースのレコード数
- 本ソフトウェアのライセンス情報：
  - ライセンスのシリアル番号と種別
  - ライセンスの有効期間（日数）
  - ライセンスの対象となるデバイスの数
  - ライセンスの有効期間の開始日と終了日
  - ライセンスのステータス
  - 本製品がアクティベーションコードを使用してアクティベートされた場合、アクティベーションサーバーとの同期が成功した最新の日時
  - ライセンスとなる本製品の識別子
  - そのライセンスで使用可能な機能
  - ライセンスが提供されている組織の名前
  - 本製品が定額制サービスで使用されている場合の詳細情報（定額制サービスのフラグ、定額制サービスの有効期限と定額制サービスの更新が可能な日数、定額制サービスのプロバイダーの URL、現在の定額制サービスのステータスとそのステータスの理由）、本ソフトウェアがデバイスでアクティベートされた日時
  - デバイス上の本製品のライセンスの有効期限の日時
- 製品アップデートに関する情報：
  - インストールまたはアンインストールするアップデートのリスト
  - アップデートの公開日と［*緊急*］ステータスのサイン
  - アップデートの名前、バージョン、簡単な説明
  - アップデートの詳細な説明へのリンク
  - 本製品のアップデートに関する使用許諾契約書とプライバシーポリシーの識別子と本文
  - 本製品のアップデートに関する Kaspersky Security Network 声明の識別子と本文

- アップデートを削除できるかどうかを示すインジケーター
- 本製品のポリシーと管理プラグインのバージョン
- 本製品の管理プラグインをダウンロードする URL
- インストールされたソ製品アップデートの名前、バージョン、インストール日
- アップデートのインストールまたはアンインストールがエラーになった場合のエラーコードと説明
- 製品アップデートによるデバイスまたは本製品の再起動の必要性のサインと理由

- Kaspersky Security Network に関する声明、使用許諾契約書、プライバシーポリシーの条件に対するユーザーの同意または不同意。
- デバイスに割り当てられているタグのリスト
- デバイスのステータスおよび割り当てられた理由。
- 本製品の全体的なステータスとそのすべてのコンポーネントのステータス、ポリシーのコンプライアンスに関する情報、デバイスのリアルタイム保護ステータス、本製品の安定性ステータス、本製品の停止に関する情報。
- 最新のデバイススキャンの日時、スキャンされたオブジェクトの数、検知された悪意のあるオブジェクトの数、ブロック / 削除 / 駆除されたオブジェクトの数、駆除できないオブジェクトの数、スキャンエラーの数、検知されたネットワーク攻撃の数。
- 現在適用されている製品設定の値に関するデータ。
- グループタスクとローカルタスクの現在のステータスと実行結果、およびそれらの設定の値
- クライアントデバイスに接続されている外部デバイスに関する情報（ID、名前、種別、製造元、説明、シリアル番号、VID/PID）
- バックアップ保管領域のバックアップファイルコピーに関する情報（名前、パス、オブジェクトのサイズと種別、オブジェクトの説明、検知された脅威の名前、脅威の検知に使用される定義データベースのバージョン、オブジェクトがバックアップ保管領域に移動された日時）、バックアップ保管領域にあるオブジェクトの処理（削除、復元）、管理者の要求によるファイル。
- 各ソフトウェアコンポーネントの動作およびイベントとして表される各タスクの実行に関する情報：
  - イベントの日時
  - イベントの名前と種別
  - イベントの緊急度
  - イベントの発生時に実行されていたタスクまたはアプリケーション コンポーネントの名前
  - イベントのきっかけとなったアプリケーションに関する情報：アプリケーション名、ディスク上のファイルへのパス、プロセス識別子、設定値（アプリケーションの起動や設定変更のイベントが発生した場合）
  - ユーザー ID
  - イベントのきっかけとなった動作の原因（タスクスケジューラー、アプリケーション、Kaspersky Security Center、ユーザーなど）の名前

- ファイルへのアクセスを開始したユーザーの名前と識別子
- オブジェクトまたは動作の処理結果（説明、種別、名前、脅威のレベルと精度、デバイスでのファイル名と動作の種別、動作に関するアプリケーションの決定）
- オブジェクトに関する情報（オブジェクトの名前と種別、ディスク上のオブジェクトへのパス、オブジェクトのバージョン、サイズ、実行された処理に関する情報、イベントの原因の説明、オブジェクトを処理せずスキップする理由の説明）
- デバイス情報（メーカー名、デバイス名、パス、デバイスタイプ、バスタイプ、識別子、VID/PID、システムデバイスフラグ、デバイスアクセスルールスケジュール名）
- デバイスのブロックとブロック解除に関する情報、ブロックされた接続に関する情報（名前、説明、デバイス名、プロトコル、リモートアドレスとポート、ローカルアドレスとポート、パケットルール、処理）
- 要求された URL に関する情報
- 検知されたオブジェクトに関する情報
- 検知の種別、方法、ID
- 実行された処理に関する情報
- 定義データベースに関する情報（ダウンロードした定義データベースのアップデートが公開された日付、定義データベースの使用に関する情報、定義データベースの使用エラー、インストールされた定義データベースのアップデートのキャンセルに関する情報）
- 暗号化検知に関する情報（ランサムウェア名、暗号化が検知されたデバイスの名前、デバイスのブロックとブロック解除に関する情報）
- アプリケーション設定とネットワーク設定
- きっかけとなったアプリケーションコントロールルール（名前と種別）とそのアプリケーションの結果に関する情報
- コンテナとコンテナイメージの情報（コンテナまたはコンテナイメージの名前、コンテナまたはコンテナイメージへのパス、リポジトリ URL）
- 有効な接続とブロックされた接続に関する情報（名前、説明、種別）
- 信頼されないデバイスへのアクセスのブロックとブロック解除に関する情報
- KSN の使用に関する情報（KSN 接続状況、KSN インフラストラクチャ、拡張モードでの KSN に関する声明の識別子、拡張モードでの KSN に関する声明への同意、KSN に関する声明の識別子、KSN に関する声明への同意）
- 証明書に関する情報（ドメイン名、主体名、発行者の名前、有効期限、証明書のステータス、証明書の種別、証明書が追加された日付、証明書発行日、シリアル番号、SHA256 サムプリント）
- 会社のソフトウェアソリューションの一部である外部システムに関する情報（Integration Server のアドレス）
- デバイスのネットワーク分離の有効化と無効化に関する情報
- Light Agent モードでの作業に関する情報：仮想マシンテンプレートの名前、Integration Server のアドレス

- ネットワーク分離が有効または無効になっているデバイスの名前
- スキャンタスクの統計：スキャンされたオブジェクトの数、見つかった脅威の数、感染したオブジェクトの数、感染の可能性があるオブジェクトの数、駆除されたオブジェクトの数、バックアップに追加されたオブジェクトの数、削除されたオブジェクトの数、駆除されていないオブジェクトの数、スキャンエラーの数、パスワードで保護されたオブジェクトの数、スキップされたオブジェクトの数、スキャンされたコンテナとイメージの数
- 本製品で使用される EDR Optimum コンポーネントのバージョンに関する情報
- 脅威開発チェーンに関する情報：脅威開発チェーンのオンラインリストの名前、脅威開発チェーンの ID

- システム変更スキャンタスクの動作に関する情報（名前、種別、パス）およびシステムのベースラインに関する情報
- ネットワーク活動、パケットルール、およびネットワーク攻撃に関する情報
- ユーザーロールの情報：
  - ユーザーロールの変更を開始したユーザーの名前と識別子
  - ユーザーロール
  - ロールが割り当てられた、またはロールが取り消されたユーザーの名前
- クライアントデバイス上で検出されたアプリケーションの実行ファイルに関する情報（名前、パス、種別とハッシュ、アプリケーションが属するカテゴリのリスト、アプリケーションが属する KL カテゴリ、アプリケーションが属する信頼グループ、ファイルの初回起動時刻、アプリケーションの名前とバージョン、アプリケーションの開発者名、アプリケーションに署名するために使用された証明書に関する情報、シリアル番号、指紋、発行元、主体、リリース日、有効期限、公開鍵、HIPS グループ名、KSN グループ名）。
- 脅威開発チェーンのオンラインリストに関する情報：脅威開発チェーン ID、脅威開発チェーンの作成タイムスタンプ、脅威開発チェーンの形式（テキストまたはアーカイブ）、脅威開発チェーンの本文サイズ（バイト単位）。

本製品のインターフェイスでリンクをたどった時に提供されるデータ

Kaspersky Endpoint Security インターフェイスのリンクをクリックすると、以下の情報をカスペルスキーに自動で提供することに同意したことになります：

- 本製品の詳細バージョン
- 本製品の言語版
- 本製品の識別子（PID）
- リンク名

Kaspersky Security Network を使用する時に提供されるデータ

拡張モードで Kaspersky Security Network を使用する場合、Kaspersky Security Network に関する声明に記載されているすべてのデータを自動的にカスペルスキーに提出することに同意するものとします。また、侵入者がデバイスに損害を与えるために使用する可能性のある特定のファイル（またはファイルの一部）およびオペレーティングシステムにあるデータをスキャンするためにカスペルスキーへ送信することもできます。

Kaspersky Security Network に関する声明が記載されている ksn_license.<言語 ID> ファイルは、製品の配布キットに含まれています。

Kaspersky Anti Targeted Attack Platform の使用時に提供される情報

Kaspersky Endpoint Security を Kaspersky Anti Targeted Attack Platform ソリューションのコンポーネントである Kaspersky Endpoint Detection and Response (KATA) と連携すると、Kaspersky Endpoint Security は個人情報および機密データを含む次の内部情報を保存します：

- KATA サーバーのアドレス
- Kaspersky Endpoint Detection and Response (KATA) と連携するためのサーバーの証明書の公開鍵
- Kaspersky Endpoint Detection and Response (KATA) と連携するためのクライアント証明書を含む Cryptocontainer
- プロキシサーバー上の認証用資格情報
- KATA サーバーとの同期頻度の設定およびデータを KATA サーバーに送信するための設定
- KATA サーバーとの接続のステータス、およびクライアント証明書とサーバー証明書のエラーに関する情報
- KATA サーバーから受信したタスクの設定：
  - タスクの開始スケジュール設定
  - タスクの開始に使用するのに必要なアカウントの名前およびパスワード
  - 設定のバージョン
  - サービス開始の種類
  - サービスの名前
  - タスクの起動に使用されるコマンドライン（引数を含む）
  - オブジェクトの MD5 および SHA256 ハッシュ
  - オブジェクトへのパス
  - IOC ファイル
- 除外に指定されたデバイス以外のデバイスへの接続をブロックする分離設定

Kaspersky Endpoint Security を Kaspersky Endpoint Detection and Response (KATA) と連携すると、Kaspersky Endpoint Security は次の情報を保存し、KATA サーバーに送信する場合があります：

- EDR (KATA) コンポーネントへの同期リクエスト用情報
  - 一意の識別子

- サーバーアドレスの基部
- デバイス名
- デバイスの IP アドレス
- デバイスの MAC アドレス
- デバイスの現地時間
- デバイス上にインストールされたオペレーティングシステムの名前およびバージョン
- Kaspersky Endpoint Security のバージョン
- 使用されている製品データベースの公開日
- ライセンスステータス

- リクエストからタスク実行レポートの EDR（KATA）コンポーネントへの情報：
  - デバイスの IP アドレス
  - 一意の識別子
  - サーバーアドレスの基部
  - デバイスの MAC アドレス
  - タスク実行エラーおよび戻りコード
  - タスク完了ステータス
  - タスク完了時間
  - 使用されたタスク設定のバージョン
  - サーバーリクエストでデバイス上で開始または停止されたプロセスに関する情報：PID および UniquePID、エラーコード、プロジェクトの MD5 および SHA256 チェックサム
  - サーバーにリクエストされたファイル
  - オブジェクトに関する情報を取得中に発生したエラーに関する情報：エラーが発生したオブジェクトの完全な名前、エラーコード
  - ネットワーク分離のステータス
  - IOC の場合、スキャン結果（各インジケーターが検出されたかどうか、見つかったオブジェクト、およびインジケーターのどのブランチが検出されたかに関する情報）が表示されます。
  - IOC が検出されたオブジェクトの場合、インジケーターの種別に応じて異なる値が表示されます：
    - ArpEntry：ARP テーブルからの IP アドレス （ipv6 を含む）、ARP テーブルからの物理アドレス。
    - File：ファイルの MD5 ハッシュ、ファイルの SHA256 ハッシュ、完全なファイル名（パスを含む）、ファイルサイズ。

- Port：スキャン中に接続を確立するために使用されるリモート IP アドレスとポート、ローカルアダプターの IP アドレスとポート、プロトコルの種類（TCP、UDP、IP、RAWIP）。
- Process：プロセス名、プロセス引数、プロセスファイルへのパス、プロセスのシステム PID、親プロセスのシステム PID、プロセスを開始したユーザー名、プロセスが開始された日時。
- SystemInfo：OS 名、OS のバージョン、ドメインのないデバイスのネットワーク名、ドメインまたはワークグループ。
- User：ユーザー名。

- テレメトリパケット内のデータ：
  - ファイルに関する情報：
    - 端末の一意な ID
    - ファイルパス
    - ファイル名
    - ファイルサイズ
    - ファイルの属性
    - ファイルの作成日時
    - ファイルの最終変更日時
    - オブジェクトの MD5 および SHA256 ハッシュ
    - ファイルを所有するユーザーとグループに関する情報（名前と ID）
  - 実行中のプロセスに関する情報：
    - プロセスファイルの一意の ID
    - プロセスの開始時に使用されたコマンドラインオプション
    - プロセス ID
    - セッション ID
    - プロセスが開始された日時
    - プロセスを開始したユーザーとグループに関する情報（名前とID）
  - 検知および処理された脅威に関する情報：
    - 検知された脅威の名前と、 カスペルスキーの分類に従った脅威を検知したテクノロジー。
    - 製品データベースのバージョン
    - 感染したオブジェクトがダウンロードされた URL。
    - 脅威の処理ステータス。

- 脅威を排除できない理由。
- 脅威ファイルの一意の ID

- ファイル変更データ：
  - 変更ファイルの一意の ID
  - 変更をしたプロセスの一意の ID
  - 変更に関する情報
- システムの変更に関するデータ：
  - 変更をしたプロセスの一意の ID
  - 発生した変更に関する情報
- ユーザーログオン情報：
  - セッション ID
  - ユーザー情報（名前とID）
  - セッションが確立されたデバイスの IP アドレス
- 終了するプロセスに関するデータ：プロセスの一意の ID。

ここにリストされている情報は、トレースファイルやダンプに保存することもできます。

Kaspersky Kaspersky Endpoint Detection and Response Optimum 使用時に提供されるデータ

IOC スキャンタスクの結果とともに送信されるデータ

Kaspersky Endpoint Security は、*IOC* スキャンタスクの結果に関するデータをKaspersky Security Center に自動的に送信します。

IOC スキャンタスクの結果データには、次の情報が含まれる場合があります：

- ネットワーク情報：
  - アドレス解決プロトコル（ARP）の表からの IP アドレス
  - アドレス解決プロトコルの表からの MAC アドレス
  - DNS レコードの種別と名前
  - 保護対象デバイスの IP アドレス

    - 保護対象デバイスの MAC アドレス
    - リモート接続の IP アドレスとポート
    - ローカルネットワークアダプタの IP アドレス
    - ローカルアダプタの開いているポートの番号
    - Internet Assigned Numbers Authority (IANA) 標準に従ったプロトコル番号
- プロセスに関する情報：
    - プロセス名
    - プロセスの引数
    - プロセスの実行ファイルへのパス
    - プロセス ID（PID）
    - 親プロセス ID
    - プロセスを開始したユーザーの名前
    - プロセスが開始された日時
- サービスに関する情報：
    - サービス名
    - サービスの説明
    - サービス実行ファイルのパスと名前
    - サービス ID
    - サービス種別（カーネルドライバー、アダプターなど）
    - サービスステータス
    - サービス開始モード
    - サービスを開始したユーザーの名前
- ファイルシステムに関する情報：
    - ボリューム名
    - ボリューム文字
    - ボリューム種別
- オペレーティングシステムに関する情報：
    - OS の名前とバージョン

- 保護対象デバイスのネットワーク名
- デバイスが属するドメインまたはグループ

- ウェブアクティビティに関する情報：
  - ブラウザ名
  - ブラウザバージョン
  - ウェブリソースへの最終アクセス時刻
  - HTTP リクエストの URL
  - HTTP リクエストを行ったユーザーの名前
  - HTTP リクエストを作成したプロセスの名前
  - HTTP リクエストを行ったプロセスの実行ファイルへのパス
  - HTTP リクエストを作成したプロセスの ID
  - HTTP リファラー（HTTP リクエストの送信元の URL）
  - 要求されたリソースの URL
  - 処理された Web リクエストのユーザーエージェント（HTTP ユーザーエージェント）
  - HTTP リクエスト実行時刻
  - HTTP リクエストを作成したプロセスの一意な ID

脅威開発チェーンを作成するためのデータ

脅威開発チェーンを作成するためのデータには、次の情報が含まれる場合があります。

- アラートの詳細：
  - アラート発生日時
  - オブジェクト名
  - スキャンモード
  - アラートに関連する最後の処理のステータス
  - アラート処理が失敗した理由
- 処理されたオブジェクトに関する情報：
  - プロセスの識別子
  - 親プロセス ID
  - プロセスファイル ID

- プロセスのコマンドライン
- プロセスを開始したユーザーの名前
- プロセスが開始されたセッションの ID
- プロセスが開始されたセッションの種別
- 処理されたオブジェクトの整合性レベル
- ユーザーが特権グループに属しているかどうか
- 処理されたオブジェクトの ID
- 処理されたオブジェクトのフルネーム
- 保護対象デバイスの ID
- オブジェクトのフルネーム（ローカルファイルまたは URL）
- 処理されたオブジェクトの MD5 および SHA256 チェックサム
- 処理されたオブジェクトの種別
- オブジェクトが作成された日付と最後に変更された日付
- 処理されたオブジェクトのサイズ
- 処理されたオブジェクトの属性
- オブジェクトに署名した組織に関する情報
- オブジェクトのデジタル証明書の検証結果
- オブジェクトのセキュリティ識別子（SID）
- オブジェクトのタイムゾーン ID
- オブジェクトをダウンロードした URL（ファイルのみ）
- ファイルをダウンロードしたアプリケーションの名前
- ファイルをダウンロードしたアプリケーションの MD5 および SHA256 チェックサム
- ファイルを最後に変更したアプリケーションの名前
- ファイルを最後に変更したアプリケーションの MD5 および SHA256 チェックサム
- 処理されたオブジェクトが開始された回数
- 処理されたオブジェクトの最初の開始日時
- 端末の一意な ID
- ファイルのフルネーム（ローカルファイルまたは URL）

- 処理された Web リクエストの URL
- 処理された Web リクエストのリンクのソース（HTTP リファラー）
- 処理されたウェブリクエストのユーザーエージェント
- 処理された Web リクエストの種別（GET または POST）
- 処理された Web リクエストのローカル IP ポート
- 処理された Web リクエストのリモート IP ポート
- 処理された Web リクエストの接続方向（受信または送信）
- 悪意のあるコードが挿入されたプロセスの ID

アプリケーション管理概念

Kaspersky Endpoint Security を管理するのに使用できるのは次のとおりです：

- Kaspersky Security Center
- コマンドライン
- グラフィカルユーザーインターフェイス

> Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、Kaspersky Security Center Cloud コンソールおよびグラフィカルユーザーインターフェースを使用して製品を管理することはできません。

Kaspersky Endpoint Security のグラフィカルユーザーインターフェイスを使用して実行できる一連の処理は制限されています。

このセクションでは、Kaspersky Security Center およびコマンドラインを介したアプリケーション管理の詳細について説明し、Kaspersky Security Center 管理コンソールおよびコマンドラインでの主な作業方法について説明します。

Kaspersky Security Center を使用した製品の管理

Kaspersky Security Center を使用すると、クライアントデバイス上の Kaspersky Endpoint Security の操作をリモートおよび一元管理できます。Kaspersky Endpoint Security のインストールとアンインストール、起動、停止をリモートで実行できます。アプリケーションだけでなく、アプリケーションの個々のコンポーネントやタスクの設定を構成できます。管理対象デバイス上でタスクを開始および停止できます。

次の Kaspersky Security Center 管理コンソールを使用して、Kaspersky Security Center 経由で Kaspersky Endpoint Security を管理できます：

- Kaspersky Security Center 管理コンソール（以後「管理コンソール」とも表記）。これは、管理者のワークステーションにインストールされる Microsoft 管理コンソール (MMC) スナップインで、管理サーバーおよびネットワークエージェント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 管理コンソールを介して Kaspersky Endpoint Security を管理するためのインターフェイスは、MMC ベースの管理コンソール用の MMC 管理プラグイン（以後「MMC プラグイン」とも表記）によって提供されます。

  > このヘルプでは、Kaspersky Security Center 14.2 Windows の管理コンソールを管理する方法について説明します。

- Kaspersky Security Center Web コンソール（以後「Web コンソール」とも表記）。これは、カスペルスキーのアプリケーションに基づいた保護システムを管理するための Web インターフェイスです。管理サーバーにアクセスできるデバイスであれば、ブラウザーを使用して Kaspersky Security Center Web コンソールで作業ができます。

  Kaspersky Security Center Web コンソールを介して Kaspersky Endpoint Security を管理するためのインターフェイスは、Web 管理プラグイン（以後、単に 「Web プラグイン」とも表記）によって提供されます。

このヘルプでは、Kaspersky Security Center 15.1 Linux の Web コンソールを管理する方法について説明します。

- Kaspersky Security Center Cloud コンソール：これは、Kaspersky Security Center のクラウドバージョン内のクラウドベースの管理コンソールであり、Kaspersky Security Center Cloud コンソールとも呼ばれます。Could コンソールのインターフェイスは、Kaspersky Security Center Web コンソールと同様です。Kaspersky Security Center Cloud コンソール経由で Kaspersky Endpoint Security を管理するためのインターフェイスも、Web プラグインによって提供されます。

  Kaspersky Security Center クラウドコンソールでは、Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response（KATA）との連携のための設定管理をサポートしていません。

  Kaspersky Endpoint Security が仮想環境の保護に Light Agent モードで使用されている場合、Kaspersky Security Center Cloud コンソールを使用してアプリケーションを管理することはできません。

MMC プラグインと Web プラグインを使用すると、Kaspersky Endpoint Security の動作を管理するためのポリシーとタスクを Kaspersky Security Center に作成できます。

- *ポリシー*は、管理グループ内のすべてのデバイスに適用される一連の設定です。ポリシーを使用すると、管理グループ内のすべてのクライアントデバイスに同一の製品設定を適用できます。

  Kaspersky Endpoint Security ポリシーは、Kaspersky Endpoint Security の動作に関する全般設定と、ポリシーが適用されるデバイス上のアプリケーションの個々の機能コンポーネントの動作に関する設定を定義します。

- Kaspersky Security Center で作成された Kaspersky Endpoint Security の*タスク*は、保護対象デバイス上で実行され、オンデマンドスキャン、アプリケーションのアクティベーション、定義データベースと機能のアップデートなどの Kaspersky Endpoint Security 機能を実装します。

  Kaspersky Security Center では、個々のデバイスで実行するタスク（ローカルタスク）、管理グループ内のすべてのデバイスのタスク（グループタスク）、またはランダムに選択したデバイスのタスク（デバイスのタスク一式）を作成できます。

使用する Kaspersky Security Center 管理コンソールに関係なく、Kaspersky Security Center を使用してこれらのデバイス上の Kaspersky Endpoint Security を管理するには、Kaspersky Endpoint Security がインストールされているデバイスを管理グループに割り当てる必要があります。Kaspersky Endpoint Security のインストール前に、Kaspersky Security Center の管理グループを作成し、管理グループへデバイスを自動的に移動するルールを設定することができます。Kaspersky Endpoint Security のインストール後に、管理グループにデバイスを手動で移動することも可能です（詳細は、Kaspersky Security Center のヘルプを参照してください）。

Kaspersky Endpoint Security 管理プラグイン

Kaspersky Security Center を使用した Kaspersky Endpoint Security の管理に必要な管理プラグインは、次のとおりです：

- Kaspersky Endpoint Security Web 管理プラグイン（以降、「*Web プラグイン*」とも表記）は、Kaspersky Endpoint Security と、Kaspersky Security Center Web コンソール、Kaspersky Security Center Cloud コンソールを使用する Kaspersky Security Center との対話を仲介します。

  Kaspersky Security Center Web コンソールがインストールされたデバイスに Web プラグインをインストールする必要があります。Web プラグインを使用した Kaspersky Endpoint Security の管理は、ブラウザーで Kaspersky Security Center Web コンソールにアクセスできるすべての管理者が使用可能です。

- Kaspersky Endpoint Security MMC 管理プラグイン（以降、「*MMC プラグイン*」とも表記）は、Kaspersky Endpoint Security と Kaspersky Security Center の対話を、管理コンソールを使用して仲介します。

  MMC プラグインは、Kaspersky Security Center 管理コンソールがインストールされているデバイスにインストールする必要があります。

Kaspersky Endpoint Security 管理プラグインにより、ポリシーとタスクを使用して Kaspersky Endpoint Security を管理できます。

ポリシーの設定の詳細は、Kaspersky Security Center のヘルプを参照してください。

Kaspersky Security Center ポリシー

*ポリシー*は、管理グループに含まれるすべてのクライアントデバイスに対して適用される Kaspersky Endpoint Security の一連の設定です。

1つのアプリケーションに対して、異なる設定値を持つ複数のポリシーを定義することができます。ただし、任意のアプリケーションに対して1つの管理グループ内で一度に使用できるのは、アクティブなポリシー1つだけです。新しいポリシーを作成すると、管理グループ内の他のすべてのポリシーが非アクティブになります。ポリシーのステータスは後で変更できます。

ポリシーには、管理グループと同様に階層があります。既定では、親ポリシーから子ポリシーへ設定を継承します。*子ポリシー*は、ネストされた階層レベルのポリシー、つまり、ネストされた管理グループとセカンダリ管理サーバーのポリシーです。親ポリシーから設定の継承を有効にすることができます。

これらの設定の変更がポリシーで禁止されていない場合、管理グループ内の個々のデバイスのポリシーで指定された設定の値をローカルで変更できます。

ポリシープロファイルを使用すると、製品の動作設定を柔軟に設定できます。*ポリシープロファイル*には、「基本」ポリシーの設定とは異なる設定が含まれている場合があり、設定された条件（アクティベーションルール）を満たす時にクライアントデバイスに適用されます。ポリシープロファイルを使用すると、様々なデバイスの動作設定を柔軟に設定できます。プロファイルは、ポリシーのプロパティの［**ポリシープロファイル**］セクションで作成および設定できます。

各ポリシー設定には、子ポリシー設定とローカル製品設定を変更できるかどうかを示す「ロック」属性があります。ポリシーのプロパティ内の設定の「ロック」ステータスにより、クライアントデバイスの製品設定が編集可能かどうか確定されます：

- 設定が「ロック」されている場合（🔒）、その値をローカルまたはネストされた階層レベルのポリシーで編集できません。ポリシーによって指定される設定の値は、管理グループおよびネストされたグループ内のすべてのクライアントデバイスに対して使用されます。

- 設定が「ロック解除」されている場合（🔓）、その値をローカルまたはネストされた階層レベルのポリシーで編集できます。設定値がローカルに指定されている場合、または管理グループ内のクライアントデバイスのネストされた階層レベルのポリシーのプロパティで指定されている場合、ポリシーのプロパティに指定されている設定値は適用されません。

Web プラグインと MMC プラグインでは、「ロック」のパラメータの数が異なります。Web プラグインには、MMC プラグインには存在しない「ロック」が含まれています。

ポリシーが初めて適用される際に、製品設定はポリシーの設定に従って変更されます。

ポリシーとポリシープロファイルの詳細については、Kaspersky Security Center のヘルプを参照してください。

Kaspersky Security Center で作成された Kaspersky Endpoint Security のタスク

Kaspersky Security Center の Kaspersky Endpoint Security では、次の種類のタスクを作成できます：

- 個々のデバイスで実行するローカルタスク
- 管理グループ内のデバイスで実行するグループタスク
- 管理グループに含まれているかどうかに関係なく、複数のデバイスで実行する複数デバイス一式のタスク

> これらの一連のデバイスに対するタスクは、タスクの設定で指定されたデバイスでのみ実行されます。タスクが作成された特定のデバイスに新しいデバイスが追加された場合、このタスクはこれらの新しいデバイスに適用されません。タスクをこれらのコンピューターに適用するには、新しいタスクを作成するか、既存のタスクの設定を編集する必要があります。

任意の数のグループタスク、複数デバイス一式に対するタスク、またはローカルタスクを作成できます。

> このタスクは、Kaspersky Endpoint Security がデバイスで稼働している場合にのみ実行されます。

Kaspersky Security Center で作成されたタスクに関する全般的な情報は、Kaspersky Security Center のヘルプを参照してください。

Kaspersky Endpoint Security を Kaspersky Security Center で管理するためのタスクは次のとおりです：

- **マルウェアのスキャン**。タスクの実行中に、ウイルスやその他のマルウェアを検知するためにタスクの設定で指定したデバイスの領域をスキャンします。
- **簡易スキャン**：タスクの実行中に、ブートセクター、スタートアップオブジェクト、プロセスメモリ、カーネルメモリをスキャンします。
- **コンテナースキャン**：タスクの実行中に、ウイルスやその他のマルウェアを検知するため、コンテナとイメージをスキャンします。
- **インベントリ**：タスクの実行中に、デバイスに保存されているすべての実行ファイルに関する情報を受け取ります。
- **システム整合性チェック**：タスクの実行中に、各オブジェクトの変更は、監視対象オブジェクトの現在の状態と、以前ベースラインとして確立された元の状態を比較することで決定されます。
- **ライセンスの追加**：タスクの実行中に、本製品をアクティベートするために、ライセンス（予備のライセンスを含む）を追加します。
- **アップデート**：タスクの実行中に、設定されたアップデート設定に従い、定義データベースをアップデートします。
- **ロールバック**：タスクの実行中に、前回の定義データベースのアップデートをロールバックします。

ポリシー設定のセットとタスク設定のデフォルト値は、ライセンスの種別によって異なります。アプリケーションが仮想環境を保護するために Light Agent モードで使用されている場合は、ライセンスの追加、アップデート、ロールバックのタスクは適用されません。さらに、一部のアプリケーション機能は KESL コンテナではサポートされていません。

Web コンソール、Cloud コンソールへのログインとログアウト

Kaspersky Security Center Web コンソール

Web コンソールにログインするには、Web コンソールのインストール時に指定した管理サーバーの URL とポート番号が必要です（ポート 8080 が既定で使用されます）。ブラウザーで JavaScript を有効にしておくことも必要です。

Web コンソールにログインするには：

1. ブラウザーで、「<管理サーバーのアドレス>:<ポート番号>」にアクセスします。
   ログインページが表示されます。
2. アカウントのユーザー名とパスワードを入力します。

   パスワードの複雑性とブルートフォース攻撃防止メカニズムにより、6か月以内にパスワードが推測できないようにすることを推奨します。

3. ［**ログイン**］をクリックします。
   管理サーバーが応答しないか不正確な認証情報を入力した場合、エラーメッセージが表示されます。

ログインすると、前回使用した言語とテーマを適用したダッシュボードが表示されます。

Web コンソールのインターフェイスの詳細は、Kaspersky Security Center のヘルプを参照してください。

Web コンソールからログアウトするには：

画面の左下隅で、［**<アカウント名>**］→［**終了**］の順に選択します。

Web コンソールが終了し、ログインページが表示されます。

Kaspersky Security Center Cloud コンソール

Kaspersky Security Center Cloud コンソールの場合、Web トークンを使用して Cloud コンソールのポータルでアカウントにログインします。

Kaspersky Security Center Cloud コンソールの詳細は、Kaspersky Security Center Cloud コンソールのヘルプを参照してください。

Web コンソールでのポリシーの管理

Web コンソールのポリシーを使用して次の処理実行できます：

- ポリシーを作成します。
- ポリシーの設定を編集する。

  管理サーバーにアクセスするのに使用したユーザーアカウントが、特定の機能範囲の設定を編集する権限を持たない場合、これらの機能範囲の設定は編集できません。一部の設定は、KESL コンテナではサポートされていません。

- ポリシー設定をエクスポートおよびインポートします。
- ポリシーをコピーして移動します。
- ポリシーを削除します。
- ポリシーのステータスを変更します。
- ポリシープロファイルを作成します。

ポリシーの操作に関する一般的な情報については、Kaspersky Security Center のヘルプを参照してください。

Web コンソールでのポリシーの作成

Web コンソールでポリシーを作成します：

1. Web コンソールのメインウィンドウで、**アセット（デバイス）** → **ポリシーとポリシープロファイル**タブを順に選択します。

   ポリシーとポリシープロファイルのリストが開きます。

2. ポリシーを適用するデバイスを含む管理グループを選択します。そのためには、ポリシーおよびポリシープロファイルのリストの上にある**現在のパス**フィールドのリンクをクリックし、開いたウィンドウで管理グループを選択します。
3. ［**追加**］をクリックします。

   ポリシーウィザードが起動します。

4. ドロップダウンリストで、**Kaspersky Endpoint Security 12.1 for Linux** を選択します。

   ウィザードの次のステップに進みます。

5. Kaspersky Endpoint Security の使用モードを指定します：

   - **ワークステーションとサーバーを保護する標準モード** – Linux オペレーティングシステムを実行しているデバイスを保護するために使用されます。
   - **仮想環境保護用 Light Agent モード**– Linux ゲストオペレーティングシステムを実行している仮想マシンを保護するための、Kaspersky Security for Virtualization Light Agent ソリューションの一部としての Light Agent モード。

6. アプリケーションを Light Agent モードで使用して仮想環境を保護している場合は、SVM 検出設定を構成します：

a. Light Agent が接続可能な SVM を検出するために使用する方法を選択します。

- **Integration Server を使用する**

  このオプションがオンにされている場合、Light Agent は Integration Server に接続し、接続可能な SVM のリストとそれらに関する情報を取得します。

- **SVM アドレスのカスタムリストを使用する**

  このオプションを選択する場合は、このポリシーによって管理される Light Agent が接続できる SVM のリストを指定できます。Light Agent は、リストで指定された SVM にのみ接続します。

SVM アドレスのリストを使用するを選択した場合、Light Agent は高度な SVM 選択アルゴリズムを使用し、SVM で大規模インフラストラクチャ保護モードが有効になります（詳細については、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください）。この場合、SVM パスが無視された場合にのみ、Light Agent をこの SVM に接続できます。［**SVM 選択アルゴリズム**］セクションで、［**SVM パス**］設定を［**SVM パスを無視**］に設定する必要があります。それ以外の値に設定した場合、Light Agent は SVM に接続できなくなります。

b. Integration Server を選択した場合、このウィザードには、Light Agent を Integration Server に接続するための現在の設定（接続用のアドレスとポート）が表示されます。必要に応じて、新しい接続設定を指定します：

a. ［**設定**］をクリックし、開いたウィンドウで新しい接続設定を指定します：

- **アドレス**

  Integration Server がインストールされているデバイスの IPv4 形式の IP アドレスまたは完全修飾ドメイン名（FQDN）。

  アドレスとして NetBIOS 名、「localhost」、または 127.0.0.1 が指定されている場合、Integration Server への接続はエラーが発生して失敗します。

- **Port**

  Integration Server に接続するためのポート。

  ポート 7271 が既定で使用されます。

b. ［**確認**］をクリックします。

c. Web プラグインは Integration Server から受信した SSL 証明書をチェックします。証明書にエラーが含まれている場合、または信頼できない場合は、［**Integration Server への接続**］ウィンドウに対応するメッセージが表示されます。

［**受信済みの証明書を見る**］行をクリックすると、Integration Server から受信した証明書に関する情報を表示できます。SSL 証明書で問題が発生した場合は、使用しているデータ伝送チャネルがセキュアであることを確認することを推奨します。

受信した証明書を保存し、Integration Server への接続を続行するには、［**処理の選択**］ブロックで［**無視**］をオンにします。

d. Integration Server の管理者パスワード（`admin` アカウントのパスワード）を指定し、［**テスト**］をクリックします。

新しいポリシーウィザードは Integration Server に接続します。接続に失敗すると、ウィンドウにエラーメッセージが表示されます。接続が成功すると、［**Integration Server への接続**］ウィンドウが閉じ、［新規ポリシーウィザード］ウィンドウの［**Integration Server への接続**］フィールドに［**接続済み**］ステータスが表示されます。

c. 手動で定義された SVM アドレスのリストを選択すると、このポリシーで管理されている Light Agent が接続できる SVM のリストがウィンドウに表示されます。リストに SVM を追加するには、**追加**をクリックして開いたウィンドウで、IPv4 形式の IP アドレスまたは SVM の完全修飾ドメイン名（FQDN）を指定します。SVM の複数の IP アドレスまたは FQDN を新しい行に入力できます。

> 単一の IP アドレスにマップされる完全修飾ドメイン名（FQDN）のみを指定します。複数の IP アドレスに対応する完全修飾ドメイン名を使用すると、アプリケーションでエラーが発生する可能性があります。

［**削除**］をクリックすると、リストで選択したアドレスを削除できます。

ウィザードの次のステップに進みます。

7. Kaspersky Security Network を使用するかどうかを決定します。Kaspersky Security Network に関する声明を読んで内容を確認したら、次のいずれかを行います：

- 声明のすべての条件に同意し、本製品で Kaspersky Security Network を使用する場合は、［**Kaspersky Security Network に関する声明をすべて確認し、理解した上で条項に同意する**］をオンにします。
- Kaspersky Security Network を使用しない場合は、［**Kaspersky Security Network に関する声明の条項に同意しない**］をオンにして、表示されるウィンドウで決定内容を確認します。

Kaspersky Security Network の使用に同意しなくても、ポリシーの作成プロセスは中断されません。ポリシー設定でいつでも、Kaspersky Security Network の使用を有効または無効にしたり、管理対象デバイスの KSN モードを変更したりできます。

ウィザードの次のステップに進みます。

8. 新しいポリシー設定ウィンドウの［**全般**］タブが表示されます。新しいポリシーの名前を指定します。

次のポリシー設定を構成することもできます：

- ポリシーのステータス：
  - **アクティブ**：現在デバイスに適用されているポリシーです。このオプションを選択すると、このポリシーは、デバイスと管理サーバーとが次に同期する時に、デバイス上でオンになります。既定では、このオプションがオンです。
  - **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です。このオプションを選択すると、ポリシーは非アクティブになりますが、［**ポリシー**］フォルダーには残ります。非アクティブなポリシーは、後でアクティブにすることができます。
- ポリシー設定の継承：
  - ［**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。この切り替えボタンは既定でオンになっています。

- ［**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、子ポリシーの設定値はロックされます。この切り替えボタンは既定でオフになっています。

ポリシーの設定の詳細は、Kaspersky Security Center のヘルプセクションを参照してください。

9. 他のポリシー設定を構成する場合は、**アプリケーション設定**タブに移動して必要な変更を加えます。
ポリシーの設定は後で変更できます。

10. ［**保存**］をクリックします。

作成したポリシーが、ポリシーのリストに表示されます。

ポリシーの管理に関する一般的な情報については、Kaspersky Security Center のヘルプを参照してください。

Web コンソールでのポリシーの変更

Web コンソールでポリシーの設定を編集します：

1. Web コンソールのメインウィンドウで、**アセット（デバイス）→ポリシーとポリシープロファイル**タブを順に選択します。
ポリシーのリストが表示されます。

2. ポリシーを適用するデバイスを含む管理グループを選択します。そのためには、ウィンドウ上部の**現在のパス**フィールドのリンクをクリックし、開いたウィンドウで管理グループを選択します。
リストには、選択した管理グループに設定されているポリシーが表示されます。

3. リスト内の必要な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が表示されます。

4. アプリケーション設定タブで**ポリシー設定**を編集します。

5. **保存**をクリックして、変更内容を保存します。

更新された設定でポリシーが保存されます。

Web コンソールでのポリシーの設定

ポリシー設定の既定一式および既定値は、アプリケーションの有効化に使用されたライセンスによって異なります。一部のポリシー設定がアプリケーションに適用されるかどうかは、アプリケーションライセンスの種別によって異なります。さらに、一部のアプリケーション機能は KESL コンテナではサポートされていません。

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**タブでポリシー設定を構成できます。

ポリシーの設定

セクション	サブセクション
脅威対策	**ファイル脅威対策** **ファイル脅威対策の除外**

	ファイアウォール管理 ウェブ脅威対策 ネットワーク脅威対策
先進の脅威対策	Kaspersky Security Network アンチクリプター ふるまい検知
Detection and Response	Managed Detection and Response Endpoint Detection and Response Optimum Endpoint Detection and Response (KATA)
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 デバイスコントロール システム変更監視 Web コントロール
ローカルタスク	タスク管理 リムーバブルドライブのスキャン
全般設定	プロキシサーバー設定 アプリケーション設定 コンテナースキャン設定 ネットワーク設定 グローバル除外リスト 保管領域の設定
Light Agent モード	SVM 検出設定 Integration Server 接続設定 SVM 接続タグ SVM 選択アルゴリズム 接続の保護

管理コンソールでのポリシーの管理

Kaspersky Security Center 管理コンソールのポリシーで、次の操作を実行できます：

- ポリシーを作成します。
- ポリシーの設定を編集する。

  管理サーバーにアクセスするのに使用したユーザーアカウントが、特定の機能範囲の設定を編集する権限を持たない場合、これらの機能範囲の設定は編集できません。一部の設定は、KESL コンテナではサポートされていません。

- ポリシー設定をエクスポートおよびインポートします。
- ポリシーを削除します。

- ポリシーのステータスを変更します。
- ポリシープロファイルを作成します。

ポリシーの操作に関する一般的な情報については、Kaspersky Security Center のヘルプを参照してください。

管理コンソールでのポリシーの作成

管理コンソールでポリシーを作成します：

1. 管理コンソールツリーの**管理対象デバイス**フォルダで、ポリシーを適用するデバイスを含む管理グループを選択します。

   この管理グループの名前が付いたフォルダーの**デバイス**タブで、管理グループに属しているデバイスのリストを表示できます。

2. 作業領域で、［**ポリシー**］タブを選択します。
3. **新しいポリシー**ボタンをクリックして、新しいポリシーウィザードを開始します。

   ポリシーのリストのコンテキストメニューで**作成 → ポリシー**項目をクリックしてウィザードを開始することもできます。

4. ウィザードの最初のステップで、リストから **Kaspersky Endpoint Security 12.1 for Linux** を選択します。

   ウィザードの次のステップに進みます。

5. 新しいポリシーの名前を入力します。
6. 作成中のポリシーで以前のバージョンの Kaspersky Endpoint Security ポリシーの設定を使用するには、［**旧バージョンのアプリケーションのポリシー設定を使用する**］をオンにします。

   ウィザードの次のステップに進みます。

7. Kaspersky Security Network を使用するかどうかを決定します。Kaspersky Security Network に関する声明を読んで内容を確認したら、次のいずれかを行います：

   - 声明のすべての条件に同意し、本製品で Kaspersky Security Network を使用する場合は、［**Kaspersky Security Network に関する声明をすべて確認し、理解した上で条項に同意する**］をオンにします。
   - Kaspersky Security Network を使用しない場合は、［**Kaspersky Security Network に関する声明の条項に同意しない**］をオンにして、表示されるウィンドウで決定内容を確認します。

   Kaspersky Security Network の使用に同意しなくても、ポリシーの作成プロセスは中断されません。ポリシー設定でいつでも、Kaspersky Security Network の使用を有効または無効にしたり、管理対象デバイスの KSN モードを変更したりできます。

   ウィザードの次のステップに進みます。

8. Kaspersky Endpoint Security の使用モードを指定します：

   - **ワークステーションとサーバーを保護する標準モード** – Linux オペレーティングシステムを実行しているデバイスを保護するために使用されます。
   - **仮想環境保護用 Light Agent モード**– Linux ゲストオペレーティングシステムを実行している仮想マシンを保護するための、Kaspersky Security for Virtualization Light Agent ソリューションの一部としての Light Agent モード。

ウィザードの次のステップに進みます。

9. アプリケーションを Light Agent モードで使用して仮想環境を保護している場合は、SVM 検出設定を構成します：

a. Light Agent が接続可能な SVM を検出するために使用する方法を選択します。

- **Integration Server を使用する**

  このオプションがオンにされている場合、Light Agent は Integration Server に接続し、接続可能な SVM のリストとそれらに関する情報を取得します。

- **SVM アドレスのカスタムリストを使用する**

  このオプションを選択する場合は、このポリシーによって管理される Light Agent が接続できる SVM のリストを指定できます。Light Agent は、リストで指定された SVM にのみ接続します。

SVM アドレスのリストを使用するを選択した場合、Light Agent は高度な SVM 選択アルゴリズムを使用し、SVM で大規模インフラストラクチャ保護モードが有効になります（詳細については、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください）。この場合、SVM パスが無視された場合にのみ、Light Agent をこの SVM に接続できます。［**SVM 選択アルゴリズム**］セクションで、［**SVM パス**］設定を［**SVM パスを無視**］に設定する必要があります。それ以外の値に設定した場合、Light Agent は SVM に接続できなくなります。

b. Integration Server を選択した場合、このウィザードには、Light Agent を Integration Server に接続するための現在の設定（接続用のアドレスとポート）が表示されます。必要に応じて、新しい接続設定を指定します：

a. ［**編集**］をクリックし、開いたウィンドウで新しい接続設定を指定します：

- **アドレス**

  Integration Server がインストールされているデバイスの IPv4 形式の IP アドレスまたは完全修飾ドメイン名（FQDN）。

  Kaspersky Security Center 管理コンソールがインストールされているデバイスがドメインの一部である場合、既定ではフィールドにこのデバイスのドメイン名が表示されます。

  Kaspersky Security Center 管理コンソールがインストールされているデバイスがドメインの一部ではない場合、または Integration Server が別のデバイスにインストールされている場合は、フィールドに手動で入力する必要があります。

  アドレスとして NetBIOS 名、「localhost」、または 127.0.0.1 が指定されている場合、Integration Server への接続はエラーが発生して失敗します。

- **Port**

  Integration Server に接続するためのポート。

  ポート 7271 が既定で使用されます。

b. ［**OK**］をクリックします。

c. Kaspersky Security Center 管理コンソールをホストしているデバイスがドメインに属していない場合、またはアカウントが KLAdmins ローカルグループまたはドメイングループまたはローカル管理者グループに属していない場合は、Integration Server の管理者アカウントが Integration Server での認証に使用されます。

開いたウィンドウで、Integration Server の管理者のパスワード（`admin` アカウントのパスワード）を入力し、［**OK**］をクリックします。

d. MMC プラグインは、Integration Server から受信した SSL 証明書をチェックします。証明書にエラーが含まれている場合、または証明書が信頼されていない場合は、［**Integration Server の証明書を検証してください**］ウィンドウが開きます。ウィンドウ内のリンクをクリックすると、受信した証明書の詳細を表示できます。

SSL 証明書で問題が発生した場合は、使用しているデータ伝送チャネルがセキュアであることを確認することを推奨します。

Integration Server への接続を続行するには、［**無視する**］をクリックします。受信した証明書は、Kaspersky Security Center 管理コンソールがインストールされているデバイスに信頼できる証明書としてインストールされます。

c. 手動で定義された SVM アドレスのリストを選択すると、このポリシーで管理されている Light Agent が接続できる SVM のリストがウィンドウに表示されます。リストに SVM を追加するには、**追加**をクリックして開いたウィンドウで、IPv4 形式の IP アドレスまたは SVM の完全修飾ドメイン名（FQDN）を指定します。SVM の複数の IP アドレスまたは FQDN を新しい行に入力できます。

単一の IP アドレスにマップされる完全修飾ドメイン名（FQDN）のみを指定します。複数の IP アドレスに対応する完全修飾ドメイン名を使用すると、アプリケーションでエラーが発生する可能性があります。

［**削除**］をクリックすると、リストで選択したアドレスを削除できます。

ウィザードの次のステップに進みます。

10. 必要に応じて、ファイル脅威対策の全般設定を構成します。
ウィザードの次のステップに進みます。

11. 必要に応じて、既定で構成されているファイル脅威対策設定を編集します。
ウィザードの次のステップに進みます。

12. 必要に応じて、ファイル脅威対策の除外リストを構成します。
ウィザードの次のステップに進みます。

13. 必要に応じて、感染したオブジェクトに対する既定の処理を変更します。
ウィザードの次のステップに進みます。

14. 新規ポリシーウィザードを完了します。

作成されたポリシーは、**ポリシー**タブの管理グループのポリシーのリストと、コンソールツリーの**ポリシー**フォルダに表示されます。

ポリシーの設定は後で変更できます。ポリシーの管理に関する一般的な情報については、Kaspersky Security Center のヘルプを参照してください。

Kaspersky Security Center 管理コンソールでのポリシー設定の変更

管理コンソールでポリシーの設定を編集します：

1. Kaspersky Security Center 管理コンソールツリーの**管理対象デバイス**フォルダーで、必要なデバイスを含む管理グループの名前が付いているフォルダーを開きます。
2. 作業領域で、［**ポリシー**］タブを選択します。
3. ポリシーのリストで必要なポリシーを選択し、ダブルクリックして**プロパティの <ポリシー名>** ウィンドウが開きます。

   ポリシーのコンテキストメニューの**プロパティ**項目を使用するか、ポリシー設定のセクションでポリシーのリストの右側にある**ポリシー設定の構成**リンクをクリックして、ポリシーのプロパティウィンドウを開くこともできます。
4. ポリシーの設定を編集します。
5. ポリシーのプロパティウィンドウで、［OK］をクリックして変更内容を保存します。

管理コンソールでのポリシーの設定

ポリシー設定の既定一式および既定値は、アプリケーションの有効化に使用されたライセンスによって異なります。一部のポリシー設定がアプリケーションに適用されるかどうかは、アプリケーションライセンスの種別によって異なります。さらに、一部のアプリケーション機能は KESL コンテナではサポートされていません。

ポリシーのプロパティウィンドウのセクションおよびサブセクションでポリシー設定を構成できます。全般的なポリシー設定とイベント設定に関する情報は、Kaspersky Security Center のヘルプを参照してください。

ポリシーの設定

セクション	サブセクション
脅威対策	**ファイル脅威対策** **ファイル脅威対策の除外** **ファイアウォール管理** **ウェブ脅威対策** **ネットワーク脅威対策**
先進の脅威対策	Kaspersky Security Network **アンチクリプター** **ふるまい検知**
Detection and Response	Managed Detection and Response Endpoint Detection and Response (KATA)
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** **デバイスコントロール** **システム変更監視**

	Web コントロール
ローカルタスク	**タスク管理** **リムーバブルドライブのスキャン**
全般設定	**プロキシサーバー設定** **アプリケーション設定** **コンテナースキャン設定** **ネットワーク設定** **グローバル除外リスト** **プロセスメモリを除外** **保管領域の設定**
Light Agent モード	**Integration Server への接続** **SVM 検出設定** **SVM 接続タグ** **SVM 選択アルゴリズム** **接続の保護**

Web コンソールでのタスクの管理

Web コンソールの Kaspersky Endpoint Security のタスクを使用して、次のアクションを実行できます：

- 新しいタスクを作成します。
- タスクの設定を編集します。

  管理サーバーにアクセスするのに使用したユーザーアカウントが、特定の機能範囲の設定を編集する権限を持たない場合、これらの機能範囲の設定は編集できません。一部の設定は、KESL コンテナではサポートされていません。

- タスクの開始、停止、一時停止、再開。

  アップデートタスクを一時停止または再開することはできません。開始または停止のみが可能です。

- タスクのエクスポートとインポート。
- タスクの削除。

タスクのリストでは、タスクのステータスとデバイスでのタスクパフォーマンスの統計情報を含むタスク実行結果を監視できます。イベントの抽出を作成して、タスクの実行を監視することもできます（［**監視とレポート**］→［**イベントの抽出**］）。イベントの抽出の詳細は、Kaspersky Security Center のヘルプを参照してください。

タスクの実行結果は、デバイス上のローカルと Kaspersky Security Center のレポートに保存されます。

タスク管理に関する一般的な情報については、Kaspersky Security Center のヘルプを参照してください。

デバイスがポリシーによって管理されている場合、コマンドラインまたはデバイス上のローカルユーザーインターフェイスを使用して、Kaspersky Security Center で作成されたタスクを表示および管理できない場合があります。

Web コンソールでのタスクの作成

Web コンソールでタスクを作成します：

1. Web コンソールのメインウィンドウで、**アセット（デバイス）→タスク**の順に選択します。
   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。
   タスクウィザードが起動します。
3. ウィザードの最初のステップでは、次の処理を実行します。
   a. ［**アプリケーション**］ドロップダウンリストで、［**Kaspersky Endpoint Security 12.1 for Linux**］を選択します。
   b. **タスクの種別**ドロップダウンリストで、作成したいタスクの種別を選択します。
   c. **タスク名**フィールドに、新しいタスクの名前を入力します。
   d. **タスクを割り当てるデバイス**セクションで、タスク範囲の定義方法を選択します。タスク範囲は、タスクが実行されるデバイスで構成されます：
      - 特定の管理グループに含まれるすべてのデバイスでタスクを実行する場合は、**タスクを管理グループに割り当てる**オプションを選択します。
      - タスクを指定したデバイスで実行する場合は、**デバイス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**オプションを選択します。
      - 事前に定義済みの基準に従ってデバイス選択に含まれるデバイス上でタスクを実行する場合は、**タスクをデバイス選択に割り当てる**オプションを選択します。デバイス選択の作成方法については、Kaspersky Security Center のヘルプを参照してください。

   ウィザードの次のステップに進みます。
4. タスク範囲を定義するために選択した方法に応じて、次のいずれかの処理を実行します：
   - 管理グループツリーで、必要な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。
   - デバイスのリストで、必要なデバイスの横にあるチェックボックスをオンにします。必要なデバイスがリストにない場合は、次の方法でデバイスを追加できます：
     - **デバイスの追加**ボタンを使用します。名前または IP アドレスでデバイスを追加したり、指定した IP 範囲からデバイスを追加したり、企業 LAN のポーリング時に管理サーバーによって検知されたデバイスのリストからデバイスを選択したりできます。
     - **ファイルからデバイスをインポート**ボタンを使用します。インポートには、デバイスアドレスのリストを含む TXT ファイルが使用されます。各アドレスは別の行に入力する必要があります。

- リストから、必要なデバイスを含む選択の名前を選択します。

ウィザードの次のステップに進みます。

5. 作成直後にタスク設定を構成するには、ウィザードの最後のステップで、**作成後にタスクのプロパティウィンドウを開く**チェックボックスをオンにします。タスクは既定で作成されます。

6. ウィザードを完了します。

新しいタスクがタスクのリストに表示されます。

Web コンソールでのポリシー設定の変更

Web コンソールでタスクの設定を編集します：

1. Web コンソールのメインウィンドウで、**アセット（デバイス）→タスク**の順に選択します。
タスクのリストが表示されます。

2. 次のいずれかの操作を実行します：

- 特定の管理グループに含まれるすべてのデバイスで実行されているタスクの設定を編集するには、ウィンドウの上部にある**現在のパス**フィールドのリンクをクリックし、開いたウィンドウで管理グループを選択します。
リストには、選択した管理グループのために設定されたタスクのみが表示されます。

- 1つ以上のデバイスで実行されているタスク（一連のデバイスに対するタスク）の設定を編集するには、ウィンドウの上部にある**現在のパス**フィールドのリンクをクリックし、開いたウィンドウの管理サーバー名の最上位のノードを選択します。
リストには、管理サーバーで作成されたすべてのタスクが表示されます。

3. タスクのリストで、必要なタスクを選択し、タスク名のリンクをクリックしてタスクのプロパティウィンドウを開きます。

4. タスクの設定を編集します：

- **全般**タブでは、タスクの名前を編集できます。

- ［**製品設定**］タブで、特定のポリシー設定を編集できます。構成可能な設定が利用できるかどうかは、タスクのタイプによって異なります。

- **スケジュール**タブでは、タスクの実行スケジュールと、タスクの開始と停止に関する追加の設定を構成できます。

タスクのプロパティウィンドウの**全般**、**結果**、**設定**、**スケジュール**、および**改訂履歴**タブは、Kaspersky Security Center の標準仕様です。詳細については、Kaspersky Security Center のヘルプを参照してください。

5. **保存**をクリックして、変更内容を保存します。

Web コンソールでのタスクの開始、停止、一時停止、および再開

Web コンソールでタスクを開始、停止、一時停止、再開します：

1. Kaspersky Security Center Web コンソールのメインウィンドウで、**アセット（デバイス）** → **タスク**タブを順に選択します。

   タスクのリストが表示されます。

2. 次のいずれかの操作を実行します：

   - 特定の管理グループに含まれるすべてのデバイスで実行されているタスクを開始または停止するには、ウィンドウの上部にある**現在のパス**フィールドのリンクをクリックし、開いたウィンドウで管理グループを選択します。

     リストには、選択した管理グループのために作成されたタスクのみが表示されます。

   - 1つ以上のデバイスで実行されているタスク（一連のデバイスに対するタスク）を開始または停止するには、ウィンドウの上部にある**現在のパス**フィールドのリンクをクリックし、開いたウィンドウの管理サーバー名の最上位のノードを選択します。

     リストには、管理サーバーで作成されたすべてのタスクが表示されます。

3. タスクのリストで、必要なタスクの名前の横のボックスをチェックし、タスクのリストの上のアクションボタンをクリックします。

管理コンソールでのタスクの管理

管理コンソールの Kaspersky Endpoint Security のタスクを使用して、次のアクションを実行できます：

- 新しいタスクを作成します。
- タスクの設定を編集します。

  > 管理サーバーにアクセスするのに使用したユーザーアカウントが、特定の機能範囲の設定を編集する権限を持たない場合、これらの機能範囲の設定は編集できません。一部の設定は、KESL コンテナには対応していません。

- タスクの開始、停止、一時停止、再開。

  > *アップデートタスクを一時停止または再開することはできません。開始または停止のみが可能です。*

- タスクのエクスポートとインポート。
- タスクの削除。

タスクのリストでは、タスクのステータスとデバイスでのタスクパフォーマンスの統計情報を含むタスク実行結果を監視できます。

タスクの実行の進行状況と結果に関する情報は、Kaspersky Endpoint Security が Kaspersky Security Center 管理サーバーに送信するイベントのリスト（**管理サーバー <サーバー名>** ノードのワークスペースの**イベント**タブ上）で確認できます。タスクの実行を監視するイベントの選択を作成することもできます。イベントの抽出の詳細は、Kaspersky Security Center のヘルプを参照してください。

タスクの実行結果は、デバイス上のローカルと Kaspersky Security Center のレポートに保存されます。

タスク管理に関する一般的な情報については、Kaspersky Security Center のヘルプを参照してください。

デバイスがポリシーによって管理されている場合、コマンドラインまたはデバイス上のローカルユーザーインターフェイスを使用して、Kaspersky Security Center で作成されたタスクを表示および管理できない場合があります。

管理コンソールでのタスクの作成

管理コンソールでタスクを作成します：

1. 管理コンソールで、次のいずれかの処理を実行します。

   - 選択した管理グループに含まれるデバイス上で実行されるタスクを作成するには、**管理対象デバイスフォルダー**のコンソールツリーでこの管理グループを選択し、ワークスペースで**タスク**タブを選択して、**新しいタスク**ボタンをクリックします。

     選択した管理グループのデバイスに対して新しいタスクウィザードが開始されます。

   - 1つまたは複数のデバイスで実行されるタスク（一連のデバイスに対するタスク）を作成するには、コンソールツリーで**タスク**フォルダーを選択し、ワークスペースで**新しいタスク**ボタンをクリックします。

     一連のデバイスに対して新しいタスクウィザードが起動します。

2. ウィザードの最初のステップで、**Kaspersky Endpoint Security 12.1 for Linux** とタスクのタイプを選択します。

   ウィザードの次のステップに進みます。

3. 一連のデバイスのタスクを作成している場合、ウィザードはタスクの範囲を定義するように要求します。タスク範囲は、タスクが実行されるデバイスで構成されます。

   a. タスクの範囲を定義する方法を指定します。管理サーバーによって検知されたデバイスのリストからデバイスを選択します。デバイスアドレスを手動で設定します。ファイルからデバイスのリストをインポートするか、以前に構成したデバイスの選択を指定します（詳細については、Kaspersky Security Center のヘルプを参照してください）。

   b. タスクの範囲を定義するために指定した方法に応じて、開いたウィンドウで次のいずれかの処理を実行します。

      - 検知されたデバイスのリストから、タスクを実行するデバイスを指定します。このためには、デバイス名の左側にあるリストのチェックボックスをオンにします。

      - **追加**または **IP 範囲の追加**ボタンをクリックして、デバイスアドレスを手動で入力します。

      - **インポート**ボタンをクリックし、開いたウィンドウでデバイスアドレスのリストを含む TXT ファイルを選択します。

      - **参照**ボタンをクリックし、開いたウィンドウで、タスクを実行するデバイスを含む選択の名前を指定します。

   ウィザードの次のステップに進みます。

4. ウィザードの指示に従って、利用可能なタスク設定を構成します。

5. 新しいタスクの名前を入力して、ウィザードの次のステップに進みます。

6. ウィザードの終了後すぐにタスクを開始するには、最後のステップで、**ウィザードの終了後にタスクを実行する**チェックボックスをオンにします。

7. ウィザードを完了します。

   新しいタスクがタスクのリストに表示されます。

管理コンソールでのポリシー設定の変更

管理コンソールでタスクの設定を編集します：

1. 管理コンソールで、次のいずれかの処理を実行します。

   - 指定した管理グループに含まれるデバイスで実行されるタスクの設定を編集するには、コンソールツリーでこの管理グループを選択し、ワークスペースで**タスク**タブを選択します。

   - 1つ以上のデバイスで実行されるタスク（一連のデバイスのタスク）の設定を編集するには、コンソール ツリーで**タスク**フォルダーを選択します。

2. タスクのリストから必要なタスクを選択し、ダブルクリックして**プロパティの <タスク名>** ウィンドウが開きます。

   タスクのコンテキストメニューの**プロパティ**項目を使用して、タスクのプロパティウィンドウを開くこともできます。

3. タスクの設定を編集します。構成可能な設定が利用できるかどうかは、タスクのタイプによって異なります。

   タスクのプロパティウィンドウの**全般**、**通知**、**スケジュール**、および**改訂履歴**タブは、Kaspersky Security Center の標準仕様です。詳細については、Kaspersky Security Center のヘルプを参照してください。

4. **プロパティ：<タスク名>** ウィンドウで**適用**または**OK**をクリックして、加えた変更を保存します。

管理コンソールでのタスクの開始、停止、一時停止、および再開

管理コンソールでタスクを開始、停止、一時停止、再開します：

1. 管理コンソールで、次のいずれかの処理を実行します。

   - 指定した管理グループに含まれるデバイスで実行されるタスクを開始または停止するには、コンソールツリーでこの管理グループを選択し、ワークスペースで**タスク**タブを選択します。

     選択した管理グループに対して作成されたタスクのリストが開きます。

   - 1つ以上のデバイスで実行されるタスク（一連のデバイスのタスク）を開始または停止するには、コンソール ツリーで**タスク**フォルダーを選択します。

     管理サーバーで作成されたすべてのタスクのリストが開きます。

2. タスクのリストで必要なタスクを選択し、タスクのコンテキストメニューを開いて、実行するアクションを選択します。

コマンドラインを使用した本製品の管理

コマンドラインを使用して、Kaspersky Endpoint Security をデバイスにインストール、アンインストール、起動、停止したり、本製品をローカルで管理することができます。

本製品の機能コンポーネントは、オペレーティングシステムで実行される *Kaspersky Endpoint Security のローカルタスク*によってサポートされます。コマンドラインで Kaspersky Endpoint Security のタスクを開始または停止することで、デバイス上の本製品の機能コンポーネントを有効または無効にできます。Kaspersky Endpoint Security のタスクを開始することで、1 回限りのデバイス スキャンも実行できます。Kaspersky Endpoint Security の *タスク設定*を行うことで、デバイス上の機能コンポーネントの設定やデバイスのスキャン設定を定義することができます。

タスク設定に加えて、本製品を構成するために次の設定を用意しています：

- コンテナースキャンの全般設定。
- 暗号化された接続のスキャン設定。
- アプリケーションの全般設定で、アプリケーション全体の動作や個々の機能の動作を定義します。

コマンドラインでは、*Kaspersky Endpoint Security 管理コマンド*を使用して、Kaspersky Endpoint Security を管理します。

kesl-control コマンドの自動追加の有効化（bash completion）

bash シェルでは、kesl-control コマンドの自動追加をオフにできます。

現在の bash セッションで kesl-control コマンドの自動追加をオンにするには、次のコマンドを実行します。

```
source /opt/kaspersky/kesl/shared/bash_completion.sh
```

すべての新しい bash シェルセッションで自動追加をオンにするには、次のコマンドを実行します。

```
echo "source /opt/kaspersky/kesl/shared/bash_completion.sh" >> ~.bashrc
```

コマンドラインでのタスク管理

コマンドラインを使用して Kaspersky Endpoint Security を管理するために、次のアプリケーション タスクが提供されています。

- *ファイル脅威対策*。このタスクを使用すると、ファイル脅威対策をリアルタイムで有効または無効にし、ファイル脅威対策コンポーネントの設定を定義できます。アプリケーションの起動時にタスクが自動的に開始されます。
- *マルウェアのスキャン*このタスクを使用すると、オンデマンドでマルウェアのファイルシステムオブジェクトをスキャンし、スキャンの設定を定義できます。このタスクを使用して、デバイス全体のスキャンまたはオブジェクトスキャンを実行できます。

- *簡易スキャン*。このタスクを使用すると、オペレーティングシステムの簡易スキャンをオンデマンドで実行し、スキャンの設定を定義できます。

- *ファイルのカスタムスキャン*。このタスクは、`kesl-control --scan-file` コマンドを使用して指定されたファイルとディレクトリをスキャンするときに使用される設定を構成および保存するように設計されています。コマンドの実行の結果、アプリケーションは一時ファイルスキャンタスクを作成して開始します。

- *コンテナのスキャン*：このタスクを使用すると、オンデマンドでコンテナとイメージをスキャンし、スキャンの設定を定義できます。

- *コンテナのカスタムスキャン*このタスクは、`kesl-control [-T] --scan-container` コマンドを使用して指定されたコンテナとイメージをスキャンするときに使用される設定を構成および保存するように設計されています。コマンドの実行の結果、アプリケーションは一時コンテナキャンタスクを作成して開始します。

- *リムーバブルドライブのスキャン*。このタスクを使用すると、リムーバブルドライブのデバイスへの接続をリアルタイムで監視し、マルウェアの存在に対するリムーバブルドライブのスキャンとブートセクタのスキャンの設定を定義できます。

- *ウェブ脅威対策*。このタスクを使用すると、Web 脅威対策を有効または無効にし、Web 脅威対策コンポーネントの設定を定義できます。

- *ネットワーク脅威対策*。このタスクを使用すると、ネットワーク脅威対策を有効または無効にし、ネットワーク脅威対策コンポーネントの設定を定義できます。

- *アンチクリプター*。このタスクでは、リモートの悪意のある暗号化からのファイルの保護を有効または無効にし、アンチクリプターコンポーネントの設定を定義できます。

- *ファイアウォール管理*。このタスクでは、ファイアウォール管理を有効または無効にし、デバイスのネットワーク接続コントロール設定を定義できます。

- *アプリケーションコントロール*。このタスクでは、アプリケーションコントロールを有効または無効にし、アプリケーションコントロールコンポーネントの設定を定義できます。

- *インベントリ*：このタスクを使用すると、デバイスに保存されているすべてのアプリケーション実行ファイルに関する情報を取得できます。

- *デバイスコントロール*。このタスクでは、デバイスコントロールを有効または無効にし、デバイスコントロールコンポーネントの設定を定義できます。このタスクは、Kaspersky Endpoint Security が起動すると自動的に開始されます。

- *ウェブコントロール*。このタスクでは、ウェブコントロールを有効または無効にし、ウェブコントロールコンポーネントの設定を定義できます。

- *ふるまい検知*。このタスクでは、オペレーティングシステム内のアプリケーションからの悪意のあるアクティビティを監視できます。このタスクは、Kaspersky Endpoint Security が起動すると自動的に開始されます。

- *システム変更監視*。このタスクを使用すると、システム変更監視コンポーネント設定で指定された監視範囲のオブジェクトに対して実行される処理のリアルタイム監視を実行できます。

- *システム整合性チェック*。このタスクを使用すると、監視対象オブジェクトの現在の状態を以前に記録された状態と比較することにより、監視範囲に含めたファイルおよびディレクトリの変更を確認できます。

- *バックアップ管理*。このタスクは、ファイルのバックアップコピーをデバイス上のバックアップに保存する機能を提供します。タスクはアプリケーションの起動時に自動的に開始され、デバイスのオペレーティ

ングメモリに常駐します。タスクは開始、停止、削除できません。

- *ライセンス*。このタスクは、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有効化する機能を提供します。タスクはアプリケーションの起動時に自動的に開始され、デバイスのオペレーティングメモリに常駐します。タスクには設定がありません。ライセンスは、特別な管理コマンドを使用して管理されます。タスクは開始、停止、削除できません。

- *アップデート*このタスクを使用すると、スケジュールされたオンデマンドの定義データベースとモジュールのアップデートを実行し、アップデート設定を編集できます。

- *ロールバック*このタスクを使用すると、定義データベースと機能の最後のアップデートをロールバックできます。

- *Kaspersky Endpoint Detection and Response (KATA) との連携*。このタスクでは、Kaspersky Endpoint Detection and Response (KATA) との連携を有効または無効にし、連携設定を定義できます。

各アプリケーションタスクには、コマンドラインで使用される名前、ID、およびタイプがあります（以下の表を参照）。

ID は、削除されたタスクを含むすべてのタスクに対して一意です。削除されたタスクの ID は再利用されません。新しいタスクの ID は、最後に作成されたタスクの ID から連続する次の番号です。

タスク名の大文字と小文字は区別されません。

アプリケーションのインストール中に、*事前定義済みタスク*が作成されます。これらのタスクは削除できません。各事前定義済みタスクには名前と ID があります。

アプリケーションの操作中に作成するタスクは、*ユーザータスク*といいます。タスクを作成するときに、その名前を指定します。ユーザータスクの ID は、タスクの作成時にアプリケーションによって定義され、割り当てられます。ユーザータスクの ID は 100 から始まります。

動作中に、アプリケーションは一時スキャンタスクを作成します。一時タスクの名前と ID はアプリケーションによって割り当てられます。一時タスクは完了すると自動的に削除されます。

アプリケーションタスク

タスク	コマンドラインのタスク名	タスク ID	タスクの種別
ファイル脅威対策	File_Threat_Protection	1	OAS
マルウェアのスキャン	Scan_My_Computer	2	ODS
マルウェアのスキャン（ユーザータスク）	ユーザーによって定義	100 以上	ODS
ファイルのカスタムスキャン	Scan_File	3	ODS
簡易スキャン	Critical_Areas_Scan	4	ODS
アップデート	Update	6	Update
アップデート（ユーザータスク）	ユーザーによって定義	100 以上	Update
ロールバック	Rollback	7	Rollback
ロールバック（ユーザータスク）	ユーザーによって定義	100 以上	Rollback
ライセンス	License	9	License
バックアップ管理	Backup	10	Backup

システム変更監視	System_Integrity_Monitoring	11	OAFIM
システム変更監視（ユーザータスク）	ユーザーによって定義	100以上	ODFIM
ファイアウォール管理	Firewall_Management	12	Firewall
アンチクリプター	Anti_Cryptor	13	AntiCryptor
ウェブ脅威対策	Web_Threat_Protection	14	WTP
デバイスコントロール	Device_Control	15	DeviceControl
リムーバブルドライブのスキャン	Removable_Drives_Scan	16	RDS
ネットワーク脅威対策	Network_Threat_Protection	17	NTP
コンテナースキャン	Container_Scan	18	ContainerScan
コンテナースキャン（ユーザータスク）	ユーザーによって定義	100以上	ContainerScan
コンテナのカスタムスキャン	Custom_Container_Scan	19	ContainerScan
ふるまい検知	Behavior_Detection	20	BehaviorDetection
アプリケーションコントロール	Application_Control	21	AppControl
インベントリ	Inventory_Scan	22	InventoryScan
インベントリ（ユーザータスク）	ユーザーによって定義	100以上	InventoryScan
Kaspersky Endpoint Detection and Response（KATA）統合	KATAEDR	24	KATAEDR
ウェブコントロール	Web_Control	26	WebControl

タスクに対して、次の処理を実行できます：

- バックアップと *ライセンス*のタスクを除く、すべての事前定義済みタスクとユーザータスクを*開始および停止*します。
- ODS、*ODFIM*、および *InventoryScan* タスクを*一時停止および再開*します。
- ユーザータスクの作成および削除します。アプリケーションの使用モードに応じて、次のタイプのタスクを作成できます：
  - 標準モード：*ODS*、*アップデート*、*ロールバック*、*ODFIM*、*ContainerScan*、および *InventoryScan*
  - 仮想環境を保護する Light Agent モード：*ODS*、*ODFIM*、*ContainerScan*、および *InventoryScan*
- ロールバックと *ライセンス*のタスクを除く、すべてのユーザータスクとすべての事前定義済みタスクの*設定を変更*します。

  アプリケーションが仮想環境を保護する Light Agent モードで使用されている場合、事前定義済みの *アップデート*タスクの設定も編集できません。

- タスクの開始スケジュールを設定します。

コマンドラインでのタスクリストの表示

製品のタスクのリストを表示するには、次のコマンドを実行します：

```
kesl-control --get-task-list [--json]
```

説明：

`--json` - 製品タスクのリストの出力形式。ファイル形式が指定されない場合、出力は INI ファイルになります。

Kaspersky Endpoint Security のタスクのリストが表示されます。

タスクごとに次の情報が表示されます：

- 名前：タスク名
- `ID`：タスク ID
- 種別：タスク種別
- 状態：タスクの現在の状態

Kaspersky Security Center のポリシーにより、ユーザーがローカルでタスクを表示および編集することが禁止されている場合、*Scan_File*、*Backup*、*License*、*File_Threat_Protection*、*System_Integrity_Monitoring*、および *Anti_Cryptor* タスクに関する情報のみが表示されます。その他のタスクの情報は使用できません。

コマンドラインでのタスクステータスの表示

タスクのステータスを表示するには、次のコマンドを実行します：

```
kesl-control --get-task-state <タスク ID / 名> [--json]
```

説明：

- `<タスク ID / 名>` は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。
- `--json` を指定すると、設定はJSON形式で出力されます。

アプリケーションタスクは主に次の状態を示します：

- `Started` – タスクを実行中です。
- `Starting` – タスクを起動中です。

- `Stopped` – タスクを停止しました。
- `Stopping` – タスクを停止しています。

ODS、*ODFIM*、*InventoryScan* の各タスクは、以下のいずれかの状態になることも可能です：

- `Pausing` – タスクは一時停止中です。
- `Suspended` – タスクは中断されています。
- `Resuming` – タスクを再開しています。

コマンドラインでのタスクの作成

標準モードでアプリケーションを使用する場合、次のタイプのタスクを作成できます：*ODS*、*アップデート*、*ロールバック*、*ODFIM*、*ContainerScan*、および *InventoryScan*。

アプリケーションを Light Agent モードで使用して仮想環境を保護する場合、次のタイプのタスクを作成できます：*ODS*、*ODFIM*、*ContainerScan*、および *InventoryScan*。

既定の設定、または設定情報ファイルで指定された設定でタスクを作成できます。

既定の設定でタスクを作成するには、次のコマンドを実行します：

```
kesl-control -create-task <タスク名> --type <タスクの種別>
```

説明：

- `<タスク名>`は、新しいタスクに指定する名前です。
- `<task type>` は、作成されたタスクタイプの識別子です。

設定情報ファイルで指定された設定でタスクを作成するには、次のコマンドを実行します：

```
kesl-control --create-task <タスク名> --type <タスクの種別> --file <設定情報ファイルへのパス> [--json]
```

説明：

- `<タスク名>`は、新しいタスクに指定する名前です。
- `<task type>` は、作成されたタスクタイプの識別子です。
- `<path to file>` は、タスクの作成に使用される設定が含まれる設定情報ファイルへの絶対パスです。
- `--json` を指定すると、設定情報ファイルの設定を JSON 形式でインポートします。`--jason` のライセンスが指定されていない場合、設定は INI ファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

コマンドラインでのタスクの開始、停止、一時停止、および再開

*バックアップ*と *ライセンス*のタイプのタスクを除き、事前定義済みタスクとユーザータスクを開始および停止できます。

ODS、*ODFIM*、および *InventoryScan* タイプのタスクを一時停止および再開できます。

タスクを開始するには、次のコマンドを実行します：

```
kesl-control --start-task <タスク ID / 名> [-W] [--progress]
```

説明：

- `<タスク ID / 名>` は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。
- `[-W]` は、タスク開始コマンドと組み合わせて使用され、このタスクに関連付けられた現在のイベントの表示を有効にするコマンドです。
- `[--progress]` は、タスクの進捗状況を表示する場合に指定する必要があるキーです。

例：
ID 1 でタスクを開始し、タスクに関連付けられた現在のイベントの表示を有効にします。

```
kesl-control --start-task 1 -W
```

タスクを停止するには、次のコマンドを実行します：

```
kesl-control --stop-task <タスク ID / 名> [-W]
```

説明：

- `<タスク ID / 名>` は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。
- `[-W]` は、停止タスクコマンドと組み合わせて使用され、このタスクに関連付けられた現在のイベントの表示を有効にするコマンドです。

タスクを一時停止するには、次のコマンドを実行します：

```
kesl-control --suspend-task <タスク ID / 名>
```

タスクを再開するには、次のコマンドを実行します：

```
kesl-control --resume-task <タスク ID / 名>
```

コマンドラインでのタスクの削除

ユーザータスクのみを削除できます。事前設定済みのタスクは削除できません。

タスクを削除するには、次のコマンドを実行します：

```
kesl-control --delete-task <タスク ID / 名>
```

<タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

コマンドラインでのタスク設定の表示

*ロールバック*と *ライセンス*のタスクを除くすべてのユーザータスクとすべての事前定義済みタスクの設定の現在の値を表示できます（これらのタスクには設定がありません）。

タスク設定の現在の値をコンソール、またはタスク設定の変更に使用できる設定方法ファイルに出力できます。

タスク設定の現在の値をコンソールに出力するには、次のコマンドを実行します：

```
kesl-control --get-settings <タスク ID / 名> [--json]
```

説明：

- <タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。
- `--json` を指定すると、設定はJSON形式で出力されます。もし `--json` キーが指定されなければ、設定はINI形式でインポートされます。

タスク設定の現在の値を設定情報ファイルに出力するには、次のコマンドを実行します：

```
kesl-control --get-settings <タスク ID / 名> --file <設定情報ファイルへのパス> [--json]
```

説明：

- <タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。
- `--file` <設定情報ファイルのパス> - タスク設定を書き込む設定情報ファイルへのパス。パスなしでファイルの名前を指定した場合、そのファイルは現在のディレクトリに作成されます。ファイルが指定されたパスに既に存在する場合は、上書きされます。指定されたディレクトリが存在しない場合、設定情報ファイルは作成されません。
- `--json` を指定すると、設定はJSON形式で出力されます。もし `--json` キーが指定されなければ、設定はINI形式でインポートされます。

コマンドラインでのタスク設定の編集

*ロールバック*と *ライセンス*のタスクを除く、すべてのユーザータスクとすべての事前定義済みタスクの設定を編集できます。

アプリケーションが仮想環境を保護する Light Agent モードで使用されている場合、事前定義済みの *アップデート*タスクの設定を編集することはできません。

コマンドラインで、**kesl-control --set-settings** コマンドを使用してタスクの設定を編集できます。

- タスク設定を含む設定情報ファイルを使用して、タスク設定をすべて編集できます。タスク設定を表示するコマンドを使用して、設定情報ファイルを取得できます。
- コマンドラインキーを使用して、< 設定名 >=< 設定値 > の形式で個々のタスク設定を編集できます。タスク設定を表示するコマンドを使ってタスク設定の現在の値を得ることができます。
- タスク設定をデフォルト値に復元できます。

タスク設定またはコマンドラインキーを含む設定情報ファイルを使用して、スキャン範囲と除外範囲を追加または削除できます。スキャン範囲と除外範囲の設定は、*OAS*、*ODS*、*OAFIM*、*ODFIM*、および*AntiCryptor*タイプのタスクで構成できます。

スキャンタスクの操作を最適化するために、システムによって読み取り専用モードでマウントされたスナップショットを含むパスを、btrfs ファイルシステムを採用し、アクティブなスナップショットが有効になっているシステムの除外に追加することを推奨します。たとえば、SUSE / OpenSUSE をベースとするシステムの場合、パスに次の除外を追加できます：**/.snapshots/*/snapshot/**。

一部のタスクについては、タスク設定を編集できる別の管理コマンドも提供されています。

設定情報ファイルを使用したタスク設定の編集

設定情報ファイルを使ってタスク設定の値を編集します：

1. コマンド **kesl-control --get-settings** を使用して、タスクの設定を設定情報ファイルに出力します。
2. 設定情報ファイルを開き、必要な設定の値を編集します。

   OAS、*ODS*、*OAFIM*、*ODFIM*、および *AntiCryptor* タイプのタスクでは、スキャン範囲および除外範囲を追加または削除できます。

   スキャン範囲を追加したい場合は、ファイルに次の設定の **[ScanScope.item_ #]** セクションを追加します：

   - **AreaDesc** はスキャン範囲の説明で、その範囲に関する詳細情報が含まれます。
   - **UseScanArea** は指定された範囲のスキャンを有効にします。
   - **Path** は、スキャンするオブジェクトのあるディレクトリへのパスです。ローカルディレクトリへのパスを指定することも、クライアントデバイスにマウントされたリモートディレクトリのスキャンを有効にすることもできます。
   - **AreaMask.item_#** はスキャン範囲の制限です。スキャンするファイル名のマスクを指定できます。スキャンは既定で、スキャン範囲内のすべてのオブジェクトに対して有効です。複数の **AreaMask.item_#** 項目を指定できます。

   除外範囲を追加する場合は、ファイルに次の設定の **[ExcludedFromScanScope.item_#]** セクションを追加します：

   - **AreaDesc** – 除外範囲の説明。除外範囲に関する詳細情報が含まれます。
   - **UseScanArea** は指定された範囲の除外を有効にします。

- `Path`は、除外するオブジェクトのあるディレクトリへのパスです。ローカルディレクトリへのパスを指定することも、クライアントデバイスにマウントされたリモートディレクトリの除外を有効にすることもできます。設定可能な値はタスクのタイプによって異なります。

- `AreaMask.item_#` は除外範囲の制限です。スキャン範囲から除外したいファイル名のマスクを指定できます。既定では、範囲内のすべてのオブジェクトが除外されます。

  例：

  ```
  [ExcludedFromScanScope.item_0000]
  AreaDesc=
  UseScanArea=Yes
  Path=/tmp/notchecked
  AreaMask.item_0000=*
  ```

`[ScanScope.item_#]` セクションと `[ExcludedFromScanScope.item_#]` セクションは複数指定できます。範囲はインデックスの昇順で処理されます。

3. 設定情報ファイルを保存します。

4. コマンドを実行します：

   `kesl-control --set-settings <タスク ID / 名> --file <設定情報ファイルへのパス> [--json]`

   説明：

   - `<タスク ID / 名>` は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

   - `--file <設定情報ファイルのパス>` – タスク設定をインポートする設定情報ファイルの絶対パス。

   - `--json`：JSON形式の設定情報ファイルから設定をインポートする場合は、このライセンスを指定します。`--jason` のライセンスが指定されていない場合、設定は INI ファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

   ファイルで定義されたタスク設定のすべての値がアプリケーションにインポートされます。

許可リストを変更する場合や、すべてのアプリケーションの起動を禁止する場合、またはアプリケーションコントロールタスクの設定で Kaspersky Endpoint Security の動作に影響を与えるアプリケーションの起動を禁止する場合は、`--accept` キーで `--set-settings` コマンドを実行します。

コマンドラインキーを使用したタスク設定の編集

`kesl-control --set-settings` コマンドキーを使用すると、タスク設定の個々の値を編集したり、*OAS*、*ODS*、*OAFIM*、*ODFIM*、および *AntiCryptor* タイプのタスクのスキャン範囲や除外範囲を追加または削除したりできます。

個々のタスク設定

コマンドラインキーを使ってタスク設定の個々の値を編集するには、次のコマンドを実行します：

`kesl-control --set-settings <タスク ID / 名> <設定名>=<設定値> [<設定名>=<設定値>]`

説明：

- < タスク ID / 名 > は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。
- < 設定名 >=< 設定値 > はタスク設定の名前と値です。タスク設定を表示するコマンドを使ってタスク設定の現在の値を得ることができます。

  指定されたタスク設定の値が変更されます。

許可リストを変更する場合や、すべてのアプリケーションの起動を禁止する場合、またはアプリケーションコントロールタスクの設定で Kaspersky Endpoint Security の動作に影響を与えるアプリケーションの起動を禁止する場合は、 `--accept` キーで `--set-settings` コマンドを実行します。

スキャン範囲の追加および削除

コマンドラインキーでスキャン範囲を追加するには、次のコマンドを実行します：

```
kesl-control --set-settings < タスク ID / 名 > --add-path < パス >
```

説明：

- `< task ID/name >` は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。
- `--add-path < path >` は、スキャンするオブジェクトのあるディレクトリへのパスを追加します。

  新しい `[ScanScope.item_#]` セクションがタスク設定に追加されます。`Path` 設定で指定されているディレクトリのオブジェクトがスキャンされます。スキャン範囲の残りの設定は既定値を適用します。

  パス設定に指定された値を持つ `[ScanScope.item_ #]` セクションが既にタスク設定に含まれている場合、重複するセクションは追加されません。

  `UseScanArea` 設定が `No` に設定されている場合、このコマンドの実行後に値は `Yes` に変更され、このディレクトリにあるオブジェクトがスキャンされます。

例：
ID=100 のタスクにスキャン範囲を追加します：

```
kesl-control --set-settings 100 ScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/home
```

タスクに次のスキャン範囲設定が追加されます：

```
[ScanScope.item_0001]

AreaDesc=

UseScanArea=Yes

Path=/home

AreaMask.item_0000=*
```

コマンドラインキーを使用してスキャン範囲を削除するには、次のコマンドを実行します：

```
kesl-control --set-settings <タスク ID / 名> --del-path <パス>
```

説明：

- **<タスク ID / 名>** は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。
- **--del-path <path>** は、スキャンするオブジェクトのあるディレクトリへのパスを削除します。

  指定したパスを含む **[ScanScope.item_#]** セクションがタスク設定から削除されます。アプリケーションは、指定されたディレクトリ内のオブジェクトをスキャンしません。

除外範囲の追加および削除

コマンドラインキーで除外範囲を追加するには、次のコマンドを実行します：

```
kesl-control --set-settings <タスク ID / 名> --add-exclusion <パス>
```

説明：

- **<タスク ID / 名>** は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。
- **--add-exclusion <path>** は、スキャンから除外したいオブジェクトのあるディレクトリへのパスを追加します。

  新しい **[ExcludedFromScanScope.item_#]** セクションが設定情報ファイルに追加されます。**Path** 設定で指定されているディレクトリのオブジェクトがスキャンから除外されます。除外範囲の残りの設定は既定値を適用します。

  パス設定に指定された値の **[ExcludedFromScanScope.item_#]** セクションがタスク設定に既に含まれている場合、重複したセクションは追加されません。

  UseScanArea 設定が **No** に設定されている場合、このコマンドの実行後に値は **Yes** に変更され、このディレクトリにあるオブジェクトがスキャンから除外されます。

コマンドラインキーで除外範囲を削除するには、次のコマンドを実行します：

```
kesl-control --set-settings <タスク ID / 名> --del-exclusion <パス>
```

説明：

- **<タスク ID / 名>** は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。
- **--del-exclusion <path>** は、スキャンするオブジェクトのあるディレクトリへのパスを除外します。

  指定したパスを含む **[ExcludedFromScanScope.item_#]** セクションがタスク設定情報ファイルから削除されます。アプリケーションは、指定されたディレクトリ内のオブジェクトをスキャンから除外しません。

コマンドラインでのタスク設定の既定の復元

*ロールバックと ライセンス*タイプのタスクを除くすべてのユーザータスクとすべての事前定義済みタスクの設定の規定を復元できます（これらのタスクには設定がありません）。

次のコマンドを実行してタスク設定を既定値へリセットします：

```
kesl-control --set-settings <タスク ID / 名> --set-to-default
```

<タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

設定が既定値に変更されます。

コマンドラインでのタスクスケジュールの設定

標準モードでアプリケーションを使用する場合、次のタイプのタスクの実行スケジュールを設定できます：*ODS*、*アップデート*、*ロールバック*、*ODFIM*、*ContainerScan*、および *InventoryScan*。

アプリケーションが仮想環境を保護するために Light Agent モードで使用されている場合、次のタイプのタスクの実行スケジュールを設定できます：*ODS*、*ODFIM*、*ContainerScan*、および *InventoryScan*。

タスク実行スケジュールの設定の現在の値をコンソールまたは設定情報ファイルに出力できます。

タスク実行スケジュールの現在の設定をコンソールに出力するには、次のコマンドを実行します：

```
kesl-control --get-schedule <タスク ID / 名> [--json]
```

説明：

- <タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。
- `--json` を指定すると、設定はJSON形式で出力されます。もし `--json` キーが指定されなければ、設定は INI 形式でインポートされます。

タスク実行スケジュールの現在の設定を設定情報ファイルに出力するには、次のコマンドを実行します：

```
kesl-control --get-schedule <タスク ID / 名> --file <設定情報ファイルへのパス> [--json]
```

説明：

- <タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。
- `--file` <設定情報ファイルへのパス> は、タスク実行スケジュールの設定が出力される設定情報ファイルへのパスです。パスなしでファイルの名前を指定した場合、そのファイルは現在のディレクトリに作成されます。ファイルが指定されたパスに既に存在する場合は、上書きされます。指定されたディレクトリが存在しない場合、設定情報ファイルは作成されません。

- `--json` を指定すると、設定はJSON形式で出力されます。もし `--json` キーが指定されなければ、設定はINI形式でインポートされます。

  例：
  アップデートタスクの設定を update_schedule.ini という名前のファイルに保存し、作成したファイルを現在のディレクトリに保存します：

  ```
  kesl-control --get-schedule 6 --file update_schedule.ini
  ```

  コンソールにアップデートタスクのスケジュールを表示します：

  ```
  kesl-control --get-schedule 6
  ```

次の方法でタスク実行スケジュールの設定を編集できます：

- すべてのスケジュール設定を含む構成ファイルから設定をインポートします。
- コマンドラインを使用して、タスク実行スケジュールの個々の設定を < 設定名 >=< 設定値 > の形式で指定します。

設定情報ファイルを使用してタスク実行スケジュールの設定値を編集するには、次の処理を実行します：

1. コマンド `kesl-control --get-schedule` を使用して、タスクの設定を設定情報ファイルに出力します。
2. ファイル内の必要な設定の値を編集し、変更を保存します。
3. コマンドを実行します：

   `kesl-control --set-schedule <タスク ID / 名> --file <設定情報ファイルへのパス> [--json]`

   説明：

   `<タスク ID / 名>` は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

   `--file <設定情報ファイルのパス>` – タスクスケジュール設定をインポートする設定情報ファイルの絶対パス。

   `--json`：JSON形式の設定情報ファイルから設定をインポートする場合は、このライセンスを指定します。`--jason` のライセンスが指定されていない場合、設定はINIファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

   ファイル内で定義されているタスク実行スケジュール設定のすべての値がアプリケーションにインポートされます。

例：
/home/test/on_demand_schedule.ini という名前の設定情報ファイルのスケジュール設定を ID=2 のタスクに読み込みます：

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

コマンドラインを使用してタスク実行スケジュール設定の個々の値を編集するには、次のコマンドを実行します：

`kesl-control --set-schedule <タスク ID / 名> <設定名 >=< 設定値 > [<設定名 >=< 設定値 >]`

説明：

- `<タスク ID / 名>` は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

- < 設定名 >=< 設定値 > は、タスクスケジュールの設定の 1 つの名前と値です。

タスク実行スケジュールに指定された設定値が変更されています。

例：

タスクを 10 時間ごとに開始するようにスケジュールするには、次の設定を指定します：

```
RuleType=Hourly

RunMissedStartRules=No

StartTime=2021/May/30 23:05:00;10

RandomInterval=0
```

タスクを 10 分ごとに開始するようにスケジュールするには、次の設定を指定します：

```
RuleType=Minutely

RunMissedStartRules=No

StartTime=23:10:00;10

RandomInterval=0
```

タスクを毎月 15 日に開始するようにスケジュールするには、次の設定を指定します：

```
RuleType=Monthly

RunMissedStartRules=No

StartTime=23:25:00;15

RandomInterval=0
```

タスクを毎週火曜日に開始するようにスケジュールするには、次の設定を指定します：

```
RuleType=Weekly

StartTime=18:01:30;Tue

RandomInterval=99

RunMissedStartRules=No
```

タスクを 10 時間ごとに開始するようにスケジュールするには、次の設定を指定します：

```
RuleType=Daily

RunMissedStartRules=No

StartTime=23:15:00;11

RandomInterval=0
```

コマンドラインでのアプリケーションの全般設定の管理

アプリケーションの全般設定で、アプリケーション全体の動作や個々の機能の動作を定義します。

特別な管理コマンドを使用して、アプリケーションの全般設定を管理できます。

- アプリケーションの全般設定の現在の値をコンソールまたは設定情報ファイルに出力します。
- 全般設定をすべて含む設定情報ファイルを使用するか、 < 設定名 >=< 設定値 > の形式のコマンドラインキーを使用して、アプリケーションの全般設定を編集します。

全般設定を使用すると、次の操作ができます。

- アプリケーションで Kaspersky Security Network とマルウェア対策データベースの軽量バージョンの使用を設定。
- アプリケーションでプロキシサーバーの使用を設定。
- ファイル操作遮断モード（スキャン中にファイルをブロックする / ブロックしない）を選択。
- マウントポイントスキャンからの除外を設定（グローバル除外）。
- プロセスメモリスキャンからの除外を設定。
- リアルタイムでのコンテナースキャンを有効化または無効化。
- 侵入者がデバイスやデータを侵害するために使用できる正規の製品の検知の有効化または無効化。
- Kaspersky Managed Detection and Response との連携を有効化または無効化。
- イベントログの使用を設定。
- スキャン タスク（ODS タイプ）による CPU リソース使用量の制限を設定します。
- 非特権ユーザーが同時に開始できるオブジェクトスキャンタスク数を制限。

アプリケーションの全般設定の表示

アプリケーションの全般設定の現在の値をコンソール、またはタスク設定の編集に使用できる設定方法ファイルに出力できます。

アプリケーションの全般設定の現在の値をコンソールに出力するには、次のコマンドを実行します：

```
kesl-control --get-app-settings [--json]
```

`--json` を指定すると、設定はJSON形式で出力されます。もし `--json` キーが指定されなければ、設定はINI形式でインポートされます。

アプリケーションの全般設定の現在の値を設定情報ファイルに出力するには、次のコマンドを実行します：

```
kesl-control --get-app-settings --file <設定情報ファイルのパス> [--json]
```

説明：

- `--file <設定情報ファイルパス>` – 本製品の全般設定が書き込まれる設定情報ファイルへのパス。パスなしでファイルの名前を指定した場合、そのファイルは現在のディレクトリに作成されます。ファイルが指定されたパスに既に存在する場合は、上書きされます。指定されたディレクトリが存在しない場合、設定情報ファイルは作成されません。
- `--json` を指定すると、設定はJSON形式で出力されます。もし `--json` キーが指定されなければ、設定はINI形式でインポートされます。

  例：
  製品の全般設定を kesl_config.ini という名前のファイルに表示します。作成されたファイルを現在のディレクトリに保存します：
  `kesl-control --get-app-settings --file kesl_config.ini`

製品の全般設定の編集

コマンドラインで、コマンド `kesl-control --set-app-settings` を使用して、アプリケーションの全般設定を編集できます。

- アプリケーションの全般設定を含む設定情報ファイルを使用して、全般設定をすべて編集できます。全般設定を表示するコマンドを使用して、設定情報ファイルを取得できます。
- コマンドラインキーを使用して、`<設定名>=<設定値>` の形式で個々の設定を編集できます。全般設定を表示するコマンドを使ってアプリケーションの全般設定の現在の値を得ることができます。

設定情報ファイルを使ってアプリケーションの全般設定の値を編集します：

1. アプリケーションの全般設定を設定情報ファイルに出力します。
2. ファイル内の必要なパラメータの値を編集し、変更を保存します。
3. コマンドを実行します：

   ```
   kesl-control --set-app-settings --file <設定情報ファイルのパス> [--json]
   ```

   説明：

   - `--file <設定情報ファイルへのパス>` は、アプリケーションの全般設定が含まれる設定情報ファイルへの絶対パスです。
   - `--json`：JSON形式の設定情報ファイルから設定をインポートする場合は、このライセンスを指定します。`--jason` のライセンスが指定されていない場合、設定はINIファイルからインポートされます。イ

ンポートが失敗すると、エラーが表示されます。

ファイルで定義された全般設定のすべての値がアプリケーションにインポートされます。

コマンドラインキーを使って全般設定の値を編集するには、次のコマンドを実行します：

```
kesl-control --set-app-settings <設定名>=<設定値> [<設定名>=<設定値>]
```

<設定名>=<設定値>は、アプリケーションの全般設定の1つの名前と値です。

指定された全般設定の値が変更されます。

例：

全般的な設定を、設定情報ファイル /home/test/kesl_config.ini から本製品へインポートします：

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

トレースファイルに記録する情報の詳細度を低く設定します：

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

ファイル操作の遮断から除外するマウントポイントを追加します：

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/data"
```

クエリの結果を制限するフィルターの使用

フィルターを使用すると、アプリケーション管理コマンドの実行時にクエリ結果を制限できます。

フィルター条件は1つ以上の*論理式*を使用して指定され、論理演算子を使用して結合され。フィルター条件は引用符で囲む必要があります：

"<フィールド> <比較演算子> '<値>'"

"<フィールド> <比較演算子> '<値>' and <フィールド> <比較演算子> '<値>'"

説明：

- <フィールド>はデータベースのフィールドの名前です。
- <比較演算子>は、次の比較演算子のいずれかです：
  - > は "対象より大きい"
  - < は "対象より小さい"
  - `like` は、指定された値と一致します。値を指定する場合、% マスクを使用できます。たとえば、論理式「FileName like '%etc%'」は、「FileName フィールドにテキスト "etc" が含まれる」という制限を設定します
  - == は "対象に等しい"
  - != は "対象に等しくない"

- >= は "対象以上"
- <= は "対象以下"

- < 値 > はフィールドの値です。値は一重引用符 (') で囲む必要があります。

  日付の値は、UNIX 時間（1970 年 1 月 1 日 00 時 00 分 00 秒（UTC）から経過した秒数）または YYYY-MM-DD hh:mm:ss 形式で指定することができます。ユーザーは、ユーザーのローカルタイムゾーンで日付と時刻を指定し、アプリケーションは同じタイムゾーンでそれらを表示します。

次のアプリケーション管理コマンドでフィルターを使用できます。

- 特定のアプリケーションの現在のイベントに関する情報を表示します：

  `kesl-control -W --query "< フィルター条件 >"`

- イベントログ内の特定のアプリケーションイベントに関する情報を表示します。

  `kesl-control -E --query "< フィルター条件 >"`

- バックアップ内の特定のオブジェクトに関する情報の表示：

  `kesl-control -B --query "< フィルター条件 >"`

- バックアップから特定のオブジェクトを削除します：

  `kesl-control -B --mass-remove --query "< フィルター条件 >"`

  例：
  FileName フィールドに「etc」というテキストを含むイベントに関する情報を取得します：
  `kesl-control -E --query "FileName like '%etc%'"`
  ThreatDetected タイプのイベントに関する情報を表示します：
  `kesl-control -E--query "EventType == 'ThreatDetected'"`
  ODS タイプのタスクによって作成された、ThreatDetected タイプのイベントに関する情報を表示します：
  `kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"`
  UNIX™ タイムスタンプシステム（1970 年 1 月 1 日 00:00:00（UTC）から経過した秒数）で指定された日付の後に生成されたイベントに関する情報を取得します：
  `kesl-control -E --query "Date > '1583425000'"`
  YYYY-MM-DD hh:mm:ss 形式で指定された日付後に発生したイベントに関する情報を取得します：
  `kesl-control -E --query "Date > '2022-12-22 18:52:45'"`
  緊急度が高のバックアップ保管領域内のファイルに関する情報を取得します：
  `kesl-control -B --query "DangerLevel == 'High'"`

製品設定のエクスポートとインポート

Kaspersky Security Center を使用して Kaspersky Endpoint Security を管理している場合、設定のインポートは使用できません。

Kaspersky Endpoint Security が仮想環境を保護する Light Agent モードで使用されている場合、アップデートタイプの事前定義済みタスクの設定はエクスポートおよびインポートできません。

Kaspersky Endpoint Security では、トラブルシューティング、設定の確認、および他のデバイスのアプリケーション設定を簡素化するために、製品のすべての設定をエクスポートとインポートできます。設定をエクスポートすると、すべてのアプリケーション設定（コンテナースキャンの全般設定、暗号化された接続スキャン設定、アプリケーションの全般設定、およびタスク設定を含む）が設定情報ファイルに保存されます。この設定情報ファイルを使用して、設定をアプリケーションにインポートできます。

設定のインポートまたはエクスポート時には、本製品を起動する必要があります。設定のインポート後には本製品を再起動する必要があります。

本製品の旧バージョンから設定をインポートまたはエクスポートする場合、新しい設定項目には既定値が設定されます。旧バージョンに設定をインポートすることはできません。

アプリケーション設定をエクスポートするには、次のコマンドを実行します：

```
kesl-control --export-settings --file <設定情報ファイルのパス> [--json]
```

説明：

- `--file <設定情報ファイルのパス>` - アプリケーション設定を保存する設定情報ファイルの絶対パス。
- `--json` を指定すると、設定情報ファイルへ JSON 形式で設定をエクスポートします。`--json` キーが指定されない場合、設定は INI ファイルへエクスポートされます。

製品の設定をファイルからインポートするには、次のコマンドを実行します：

```
kesl-control --import-settings --file <設定情報ファイルのパス> [--json]
```

説明：

- `--file <設定情報ファイルのパス>` - 本製品へ設定をインポートする設定情報ファイルの絶対パス。
- `--json` を指定すると、設定情報ファイルの設定を JSON 形式でインポートします。`--jason` のライセンスが指定されていない場合、設定は INI ファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

ファイルからアプリケーション設定をインポートすると、`UseKSN` および `CloudMode` 設定は `No` に設定されます。Kaspersky Security Network の使用を開始または再開するには、`UseKSN` 設定の値を `Basic` または `Extended` に設定します。クラウドモードを有効にするには、`CloudMode` 設定を `Yes` に設定する必要があります。KSN の使用が有効になっている場合、クラウドモードを使用できます。

アプリケーション設定がインポートされた後、内部タスク ID が変更される場合があります。タスクの管理にはタスク名を使用してください。

コマンドラインを使用したユーザーロールの管理

コマンドライン経由のKaspersky Endpoint Security 機能へのアクセスは、ユーザーのロールに応じて提供されます。*ロール*は、製品の管理に使用する一連の権限や特権です。

システムユーザーの 4 つのグループ（*kesladmin*、*kesluser*、*keslaudit*、*nokesl*）がオペレーティングシステムに作成されます。システムユーザーに製品のロールを割り当てると、ユーザーは対応するロールのグループに追加されます（下の*ロール*の表を参照してください）。ユーザーのロールを取り消すと、対応するロールのグループからそのユーザーが削除されます。

Kaspersky Endpoint Security のロールがシステムユーザーに割り当てられていない場合、そのユーザーは*権限のないユーザー*という別のグループに所属することになります。

このように、ロールはオペレーティングシステムのユーザーの、4 つのグループに対応します：

- kesladmin - Administrator のロール。
- kesluser - ユーザーのロール。
- keslaudit - Auditor のロール。
- nokesl - 他のロールが割り当てられていない場合に割り当てられます。この場合、ユーザーは*権限のない別のユーザーグループ*に属します。

ユーザーロール

ロール名	製品内のロール	OS のユーザー	権限
Administrator	admin	kesladmin	本製品とタスクの設定の管理。 製品のライセンスの管理。 ユーザーへのロールの割り当て。 ユーザーロールを取り消す（管理者には、自分から管理者のロールを取り消す権利はありません）。 ユーザーの保管領域の表示と管理。
User	user	kesluser	ユーザーファイルスキャンタスクのみを管理します。 アップデートタスクの開始と停止。 このユーザーが作成したタスクのレポートを表示します。 製品の全ユーザーに共通である特定のイベントの表示。
Auditor	audit	keslaudit	製品設定の表示 製品のステータスの表示。 全タスク、その設定、および開始スケジュールの表示。 全イベントの表示。 バックアップ内の全オブジェクトの表示。
-	-	nokesl	アプリケーションにロールが割り当てられていません。権限がありません。

ユーザーとロールのリストの表示

ユーザーとそのロールのリストを表示するには、次のコマンドを実行します：

```
kesl-control [-U] --get-user-list
```

ユーザーへのロールの割り当て

特定のユーザーにロールを割り当てるには、次のコマンドを実行します：

```
kesl-control [-U] --grant-role <ロール> <ユーザー>
```

例：
ロール audit をユーザー test15 に割り当てるには：

```
kesl-control --grant-role audit test15
```

ユーザーロールの取り消し

特定のユーザーのロールを取り消すには、次のコマンドを実行します：

```
kesl-control [-U] --revoke-role <ロール> <ユーザー>
```

例：
ユーザー test15 のロール audit を取り消すには：

```
kesl-control --revoke-role audit test15
```

本製品の起動および停止

Kaspersky Endpoint Security をデバイスにインストールすると、自動的に起動します。既定では、本製品は、オペレーティングシステムの起動時に（各オペレーティングシステムの既定の実行レベルで）自動的に起動します。

既定では、Kaspersky Endpoint Security を起動すると、アプリケーションの次の機能コンポーネントが自動的に起動します：

- ファイル脅威対策。
- デバイスコントロール。
- ふるまい検知。
- ウェブ脅威対策 – 対応しているいずれかのブラウザがシステムで検出され、デバイスでウェブ脅威対策設定のローカル管理が許可されている場合（ポリシーが適用されていないか、ポリシーのプロパティで「ロック」に設定されていない場合）のみに自動的に開始されます。
- ネットワーク脅威対策 – デバイス上のネットワーク脅威対策設定がポリシーで定義されている場合のみ。ネットワーク脅威対策は、既定のポリシーのプロパティで有効になっています。ローカルで構成された設定がデバイスに適用されている場合、ネットワーク脅威対策は既定で無効になります。

本製品が起動すると、本製品の追加機能であるアプリケーション起動機能とバックアップ機能の動作を保証するために、デバイス上でサービスタスクが自動的に開始されます。

既定では、アプリケーションはコマンドラインで設定されたユーザータスクも開始します。このタスクには、「アプリケーションの起動後」実行モード（PS 実行モード）が設定されています。

本製品を停止すると、デバイス上で実行中のすべてのタスクが中断されます。本製品の再起動後、中断されたユーザータスクは自動的に再開されません。

Web コンソールを使用したアプリケーションの起動と停止

本製品をリモートで起動または停止するには：

1. Web コンソールのメインウィンドウで、**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. リストで、アプリケーションを起動または停止するデバイスを選択し、デバイス名のリンクをクリックすると、デバイスのプロパティウィンドウが表示されます。
3. ［**アプリケーション**］タブを選択します。
4. ［**Kaspersky Endpoint Security 12.1 for Linux**］をオンにします。
5. 次のいずれかの操作を実行します：
   - 本製品を起動するには、**起動**ボタンをクリックします。
   - 本製品を終了するには、**停止**ボタンをクリックします。

［**監視とレポート / ダッシュボード**］ウィンドウの［**保護ステータス**］Web ウィジェットを使用して、本製品の動作状態を監視できます。

管理コンソールを使用したアプリケーションの起動と停止

クライアントデバイス上で本製品を起動または停止するには：

1. 管理コンソールのツリーの**管理対象デバイス**フォルダで、必要なデバイスを含む管理グループを選択します。
2. 作業領域で、［**デバイス**］タブを選択します。
3. 管理対象デバイスのリストで、本製品を開始または停止するデバイスを選択します。デバイスのコンテキストメニューで、［**プロパティ**］を選択します。
4. ［**<デバイス名>のプロパティ**］ウィンドウで、［**アプリケーション**］セクションを選択します。
   ウィンドウの右側には、デバイスにインストールされているカスペルスキーのアプリケーションのリストが表示されます。
5. **Kaspersky Endpoint Security 12.1 for Linux** を選択します。
6. 次のいずれかの操作を実行します：
   - アプリケーションを実行するには、カスペルスキーのアプリケーションリストの右側にある［  ］をクリックするか、アプリケーションのコンテキストメニューから［**開始**］を選択します。
   - アプリケーションを停止するには、カスペルスキーのアプリケーションリストの右側にある［  ］をクリックするか、アプリケーションのコンテキストメニューから［**停止**］を選択します。

コマンドラインを使用したアプリケーションの起動と停止

本製品を実行するには、root アカウントが次のディレクトリの所有者であり、所有者のみが書き込みアクセス権を持つ必要があります：/var、/var/opt、/var/opt/kaspersky、/var/log/kaspersky、/opt、/opt/kaspersky、/usr/bin、/usr/lib、/us

Kaspersky Endpoint Security の起動、再起動、停止

本製品を起動するには、次のコマンドを実行します：

```
systemctl start kesl
```

本製品を停止するには、次のコマンドを実行します：

```
systemctl stop kesl
```

本製品を再起動するには、次のコマンドを実行します：

```
systemctl restart kesl
```

Kaspersky Endpoint Security のステータスの監視

Kaspersky Endpoint Security の状態は、ウォッチドッグサービスにより監視されます。ウォッチドッグサービスは、製品の起動時に自動的に開始します。

製品がクラッシュした場合、ダンプファイルが生成され、製品は自動的に再起動されます。

製品設定をエクスポートするには、次のコマンドを実行します：

```
systemctl status kesl
```

デバイスとアプリケーション設定の保護ステータスを表示する

デバイスの保護ステータス、デバイス上の Kaspersky Endpoint Security とそのコンポーネントのステータスに関する情報を表示できます。

デバイスの保護ステータスに関する情報は、次の方法で取得できます：

- Web コンソールまたは管理コンソールで、クライアントデバイスのステータス（*OK*、*重大*、*警告*）を使用します。Kaspersky Security Center 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は、Kaspersky Security Center のクライアントデバイスです。クライアントデバイスのステータスは、次の理由で*重大*または*警告*に変更されることがあります：

  - Kaspersky Security Center で定義されたルールに従います。たとえば、デバイスにセキュリティアプリケーションがインストールされていない場合、ウイルススキャンが長期間実行されていない場合、アプリケーションデータベースが古い場合、ライセンスの有効期限が切れている場合、またはアプリケーションが不安定な場合、ステータスは変わります。ステータスを変更する理由とステータスを割り当てるための条件の設定の詳細については、Kaspersky Security Center ヘルプ システムを参照してください。

  - Kaspersky Security Center は、管理対象アプリケーション、つまり Kaspersky Endpoint Security からデバイスのステータスを受信します。

    > Kaspersky Security Center の、*重大*および*警告*ステータスを割り当てる条件のリストで、管理対象アプリケーションからのデバイスステータスの受信を有効にする必要があります。デバイスのステータスを割り当てる条件は、管理グループのプロパティ画面で設定します。

  クライアントデバイスのステータスの詳細については、Kaspersky Security Center ヘルプを参照してください。

- Web コンソールまたは管理コンソールで、デバイス上の Kaspersky Endpoint Security の機能コンポーネントのステータスを使用します。デバイスにインストールされている Kaspersky Endpoint Security のプロパティに、アプリケーションの機能コンポーネントのリストが表示されます。コンポーネントごとに、そのステータスが表示されます。

- コマンドラインで、コマンド `kesl-control --app-info` を使用します。このコマンドは、アプリケーションの動作と、アプリケーションの機能コンポーネントおよびタスクのステータスに関する情報を表示します。

Web コンソールでのデバイスの保護ステータスの表示

Web コンソールでデバイスの保護ステータスを表示します：

1. Web コンソールのメインウィンドウで、**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. 必要なデバイスを含む管理グループを選択します。そのためには、管理対象デバイス上部の**現在のパス**フィールドのリンクをクリックし、開いたウィンドウで管理グループを選択します。

   リストには、選択した管理グループに管理対象デバイスのみが表示されます。

3. リストで、情報を表示したいデバイスを探し、デバイス名をクリックします。

4. 開いた管理対象デバイスのプロパティウィンドウの **全般**タブで、**保護**セクションを選択します。

プロテクションセクションに、デバイスに関する以下の情報が表示されます：

- **ネットワーク上での可視性** - ネットワーク内の選択されたデバイスの可視性：［*はい*］または［*いいえ*］。
- **デバイスステータス**は、選択したデバイスに対して管理者が設定した保護ステータス基準と、ネットワーク内のデバイスアクティビティ（*OK*、*重大*、または*警告*）に基づいて生成されるクライアントデバイスのステータスです。
- **ステータスの説明** - 選択したデバイスのステータスが「*緊急*」または「*警告*」に変更された理由。
- **保護ステータス**は、選択したデバイス上のファイル脅威対策の現在のステータス（*実行中*、*停止中*、または*一時停止中*）を表します。
- **前回の完全チェック** - 選択したデバイスで前回実行された完全スキャンタスクが完了した日時。
- **ウイルスの検知** - Kaspersky Endpoint Security がインストールされてから、選択されたデバイスで検知された悪意のあるオブジェクトの総数（検知された脅威のカウンター）。
- **駆除に失敗したオブジェクト** - Kaspersky Endpoint Security が駆除できなかった感染オブジェクトの数。

管理コンソールでのデバイスの保護ステータスの表示

管理コンソールでデバイスの保護ステータスを表示します：

1. 管理コンソールのツリーの**管理対象デバイス**フォルダで、必要なデバイスを含む管理グループを選択します。
2. 作業領域で、［**デバイス**］タブを選択します。
3. 管理対象デバイスのリストで必要なデバイスを選択し、ダブルクリックして**プロパティの <タスク名>** ウィンドウが開きます。
4. 管理対象デバイスのプロパティが表示されたウィンドウで、**保護**セクションを選択します。

プロテクションセクションに、デバイスに関する以下の情報が表示されます：

- **デバイスステータス**：管理者が設定した指定デバイスの保護ステータスに関する基準およびネットワークにおけるデバイスの活動に基づいて生成されたクライアントデバイスのステータス。
- **すべての問題**：指定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で検知された問題がすべてリスト表示されます。各問題にはステータスがあり、アプリケーションがデバイスにステータスを割り当てるよう促します。
- **リアルタイム保護のステータス**：指定デバイスに対するファイル脅威対策の現在のステータス（*実行中*、*停止*など）。保護ステータスが変更されると、新しいステータスがデバイスのプロパティウィンドウに表示されますが、表示されるのは管理サーバーとの同期後です。
- **前回のオンデマンドスキャン**：指定デバイスで前回のマルウェアのスキャンが実行された日時。
- **検知した脅威の合計**：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、指定デバイスで検知された脅威の合計数。

  カウンターをリセットするには、**リセット**をクリックします。

- **アクティブな脅威**：指定デバイスの未処理ファイル数。

Web コンソールでのアプリケーションの操作に関する情報の表示

アプリケーションの操作に関する情報を Web コンソールで表示するには、次の手順に従います：

1. Web コンソールのメインウィンドウで、**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. 必要なデバイスを含む管理グループを選択します。そのためには、管理対象デバイス上部の**現在のパス**フィールドのリンクをクリックし、開いたウィンドウで管理グループを選択します。
   リストには、選択した管理グループに管理対象デバイスのみが表示されます。
3. リストで、情報を表示したいデバイスを探し、デバイス名をクリックします。
4. これにより、管理対象デバイスの［プロパティ］ウィンドウが開きます。そのウィンドウで、［**アプリケーション**］タブに移動します。
5. デバイスにインストールされているカスペルスキーのアプリケーションの一覧で、**Kaspersky Endpoint Security 12.1 for Linux** のアプリケーション名をクリックします。
   アプリケーションのプロパティウィンドウが表示されます。

［**Kaspersky Endpoint Security 12.1 for Linux**］ウィンドウに、Kaspersky Endpoint Security に関する次の情報が表示されます：

- ［**情報**］セクションの［**全般**］タブには、インストールされているアプリケーションに関する全般情報が表示されます。
  - **名前** - 製品の名前。
  - **バージョン** - 製品のバージョン番号。
  - **インストール** - 製品がデバイスにインストールされた日時。
  - **前回の製品アップデート**は、Kaspersky Endpoint Security のソフトウェアモジュールが前回アップデートされた日時です。
  - **前回の同期**は、デバイスが Kaspersky Security Center 管理サーバーに最後に接続した日時です。
  - **現在のステータス**：デバイスのファイル脅威対策ステータス（*実行中*、*一時停止*など）。
  - ［**インストール済みのアップデート**］では、製品モジュールのアップデートに関する情報が表示されます。
  - ［**製品データベース**］では、製品データベースのアップデートリリースの日時と前回のアップデートの日時に関する情報が表示されます。
- ［**全般**］タブの［**ライセンス**］セクションには、製品に追加されたライセンスと、これらのライセンスに対応するライセンスに関する情報が含まれています。
- ［**全般**］タブの［**コンポーネント**］セクションには、製品の機能的コンポーネントのリストが含まれています。各コンポーネントのステータス（たとえば、*停止*、*一時停止*、*インストールされていません*など）およびバージョンが表示されます。

仮想環境保護用 Light Agent モード行では、アプリケーションの使用モードに関する情報を確認できます：

- *実行中*ステータスは、本製品が Light Agent モードで使用されていることを意味します。
- *インストールされていない*ステータスは、本製品が標準モードで使用されていることを意味します。

- ［**イベント**］タブには、デバイス上の製品イベントのリストが表示されます。
- ［**イベント設定**］セクションは、本製品がイベントの保管領域に保管するイベントの種別と、その保管期間を表示します。
- ［**製品設定**］タブの［**検知と応答**］セクションでは、デバイスのネットワーク分離を管理できます。

管理コンソールでのアプリケーションの操作に関する情報の表示

アプリケーションの操作に関する情報を Kaspersky Security Center 管理コンソールで表示するには、次の手順に従います：

1. Kaspersky Security Center 管理コンソールのツリーの**管理対象デバイス**フォルダで、必要なデバイスを含む管理グループを選択します。
2. 作業領域で、［**デバイス**］タブを選択します。
3. 管理対象デバイスのリストで必要なデバイスを選択し、ダブルクリックして**プロパティの <タスク名>** ウィンドウが開きます。
4. 管理対象デバイスのプロパティが表示されたウィンドウで、［**製品**］セクションを選択します。
   ウィンドウの右側には、デバイスにインストールされているカスペルスキーのアプリケーションのリストが表示されます。
5. **Kaspersky Endpoint Security 12.1 for Linux** を選択し、ダブルクリックしてアプリケーションのプロパティウィンドウを開きます。あるいは、ウィンドウの下部にある **Properties** ボタンを使用することもできます。
   ［**Kaspersky Endpoint Security 12.1 for Linux の設定**］ウィンドウが表示されます。

［**Kaspersky Endpoint Security 12.1 for Linux の設定**］ウィンドウに、Kaspersky Endpoint Security に関する次の情報が表示されます：

- ［**全般**］セクションには、インストールされたアプリケーションの一般的な情報が表示されます：
  - **バージョン番号**：製品のバージョン番号。
  - **インストール**：本製品がデバイスにインストールされた日時。
  - **現在のステータス**：デバイスのファイル脅威対策ステータス（*実行中*、*一時停止*など）。
  - **前回の製品アップデート**：Kaspersky Endpoint Security のソフトウェアモジュールが前回アップデートされた日時。
  - **インストール済みのアップデート**：アップデートがインストールされたソフトウェアモジュールのリスト。
  - **定義データベース**：定義データベースのアップデートがリリースされた日時。

- ［**コンポーネント**］セクションには、標準製品コンポーネントのリストが表示されます。各コンポーネントのステータス（たとえば、*停止*、*一時停止*、*インストールされていません*など）およびバージョンが表示されます。

  仮想環境保護用 Light Agent モード行では、アプリケーションの使用モードに関する情報を確認できます：

  - *実行中*ステータスは、本製品が Light Agent モードで使用されていることを意味します。
  - *インストールされていない*ステータスは、本製品が標準モードで使用されていることを意味します。

- **ライセンス**セクションには、現在のライセンスと予備のライセンスの情報が表示されます：
  - **シリアル番号** - 一意の英数字の配列。
  - **ステータス** – ライセンスのステータス（たとえば、現在または保留など）。
  - **種別**：ライセンスの種別（「製品版」または「試用版」）。
  - **ライセンス有効期間** – このライセンスでアクティベートした本製品を使用できる日数。
  - **ライセンス上限** - ライセンスを使用できるデバイスの数。
  - **アクティベーション日**（このフィールドは、現在のライセンスでのみ表示されます）：現在のライセンスが追加された日。
  - **ライセンスの有効期限**（現在のラインセンスのみで使用可能）：現在のライセンスで本製品を使用できなくなる日付。
- ［**イベント設定**］セクションは、本製品がイベントの保管領域に保管するイベントの種別と、その保管期間を表示します。
- ［**詳細**］セクションには、アプリケーション管理プラグインの情報が表示されます。

コマンドラインでのアプリケーションの操作に関する情報の表示

アプリケーションに関する情報を表示するには、次のコマンドを実行します：

```
kesl-control --app-info [--json]
```

`--json` はJSON形式でデータを出力します。もし `--json` キーが指定されなければ、設定は INI 形式でインポートされます。

コマンドを実行すると、次の情報がコンソールに表示されます：

- **Name**。製品名。
- **バージョン**。現在の製品バージョン。
- **ポリシー**。Kaspersky Security Center ポリシーがデバイスに適用されているかどうかに関する情報。
- **製品ライセンス情報** 製品ライセンスの情報または製品ライセンスのステータス。
- **アプリケーションのライセンスの有効期限日**。製品ライセンスの有効期限日時（UTC）。

- **EDR Optimum のライセンス情報**。Kaspersky Endpoint Detection and Response Optimum 機能が使用されるライセンスに関する情報、または EDR Optimum ライセンスのステータス。
- **EDR Optimum ライセンスの有効期限日**。Kaspersky Endpoint Detection and Response Optimum 機能を使用するためのライセンスの有効期限日時（UTC）。
- **定額制サービスのステータス**。定額制サービスのステータス。このフィールドは、定額制で製品を起動している場合に表示されます。
- **MDR BLOB ファイルのステータス**。Kaspersky Managed Detection and Response との連携のための BLOB 設定情報ファイルのステータス。
- **MDR BLOB ライセンスの有効期限**。Kaspersky Managed Detection and Response ライセンスの有効期限日時（UTC）。
- **バックアップのステータス**。バックアップのステータス。
- **バックアップの使用量**。バックアップサイズ。
- **「Scan_My_Computer」タスクを前回実行した日付**。前回のマルウェアのスキャンタスクの時間。
- **定義データベースの前回の公開日時**。定義データベースが前回公開された日時。
- **定義データベース**。定義データベースがダウンロードされているかに関する情報。
- **Kaspersky Security Network の使用**。Kaspersky Security Network の使用に関する情報：拡張 KSN モード、標準 KSN モード、または無効。
- **バーチャル環境を保護する Light Agent モード**。本製品が仮想環境保護のために Light Agent モードで使用されていることを示す情報。本製品が標準モードで使用されている場合、その行は表示されません。
- **Kaspersky Security Network のインフラストラクチャ**。カスペルスキーのレピュテーションデータベースと連携するために使用されるインフラストラクチャソリューションに関する情報：Kaspersky Security Network または Kaspersky Private Security Network。
- **ファイルの駆除と削除が無効になっています**。ポリシープロパティで構成された設定に関係なく、ディスク上のファイルが駆除および削除されないアプリケーション動作モードが有効になっているという事実に関する情報。
- **Kaspersky Managed Detection and Response との連携**。Managed Detection and Response との連携のステータス：有効、無効。
- **Kaspersky Endpoint Detection and Response Optimum の連携**。Kaspersky Endpoint Detection and Response Optimum との連携のステータス。
- **ファイル脅威対策**：リアルタイムのファイル脅威対策ステータス。
- **コンテナの監視**：リアルタイムのコンテナースキャンステータス。
- **システム変更監視**：システム変更監視コンポーネントのステータス。
- **ファイアウォール管理**。ファイアウォール管理コンポーネントのステータス。
- **アンチクリプター**。アンチクリプターコンポーネントのステータス。
- **ウェブ脅威対策**。ウェブ脅威対策コンポーネントのステータス。

- **デバイスコントロール**：デバイスコントロールコンポーネントのステータス。
- **リムーバブルドライブのスキャン**。リムーバブルドライブのスキャンコンポーネントのステータス。
- **ネットワーク脅威対策**。ネットワーク脅威対策コンポーネントのステータス。
- **ふるまい検知**。ふるまい検知の設定コンポーネントのステータス。
- **アプリケーションコントロール**：アプリケーションコントロールコンポーネントのステータス。
- **ウェブコントロール**。ウェブコントロールコンポーネントのステータス。
- **Kaspersky Endpoint Detection and Response (KATA) との連携**。Kaspersky Endpoint Detection and Response（KATA）連携のステータス。
- **アップデート後の処理**。製品のアップデートの動作とユーザーが実行した動作。
- **不安定な製品動作**。製品の障害とダンプファイルの作成に関する情報。このフィールドは、本製品の前回の起動時に障害が発生した場合に表示されます。

アプリケーションのアクティベーションとライセンスの管理

*アクティベーション*とは、ライセンスの有効期限が切れるまで、すべての機能を使用できる製品版のライセンスを有効化するプロセスです。

Kaspersky Endpoint Security を有効化するプロセスは、デバイスへ現在のアプリケーションライセンスの追加を伴います。

Kaspersky Endpoint Detection and Response Optimum 機能が含まれていないライセンスで本製品を使用している場合、この機能を有効にするには、デバイスへ追加の Kaspersky Endpoint Detection and Response Optimum アドオンライセンス（「EDR Optimum ライセンス」）を追加する必要があります。

Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、製品を個別にアクティベートする必要はありません。Kaspersky Hybrid Cloud Security for Virtualization Light Agent を有効化します。有効化は、Protection Server（Kaspersky Hybrid Cloud Security for Virtualization Light Agent のコンポーネント）で、SVM にライセンスを追加することによって実行されます。Kaspersky Kaspersky Endpoint Detection and Response Optimum の機能を有効化するには、EDR Optimum ライセンスも SVM に追加する必要があります。

アプリケーションを有効化するには、次のいずれかの方法があります：

- Kaspersky Security Center を使用してリモートでアップデートする：
  - Kaspersky Endpoint Security のインストール中。インストールパッケージにアプリケーションライセンスを追加できます。インストール後、アプリケーションは自動的に有効化されます。
  - Kaspersky Endpoint Security をインストールして、アプリケーション有効化タスクを使用します。
  - Kaspersky Endpoint Security をインストールして、管理サーバーからクライアントデバイスにライセンスを配布します。
- 次のコマンドラインを使用してください：
  - Kaspersky Endpoint Security の初期設定時。
  - Kaspersky Endpoint Security をインストールして、管理コマンドを使用します。

デバイスに EDR Optimum ライセンスを追加するには、ライセンスの追加タスクまたはクライアントデバイスへのキー配布の手順を使用できます。ライセンスの種別を指定する必要はありません。

アプリケーションライセンスを追加した後にのみ、EDR Optimum ライセンスを追加できます。

予備のアプリケーションライセンスと予備 EDR Optimum ライセンスをデバイスに追加することもできます。現在のライセンスが期限切れになるか削除されると、予備のライセンスがアクティブになります。予備のライセンスを追加しておくことで、ライセンスの有効期限が切れた時に本製品の機能が制限されるのを防ぐことができます。

予備のライセンスは、現在のライセンスを追加した後にのみ追加できます。

デバイスに追加されたライセンス情報を表示できます：

- Web コンソールまたは管理コンソールでリモート操作可能。クライアントデバイス上のアプリケーションのプロパティには、**ライセンス**セクションに有効なライセンスと予備のライセンスに関する情報が含まれています。

- コマンドラインで管理コマンドを使用する。

コマンドラインでのライセンスに関する情報の表示

コマンド ラインで `-L --query` コマンドを使用すると、アプリケーションに追加された有効なライセンスと予備のライセンスに関する情報、およびアプリケーションが有効化されたライセンスに関する情報を表示できます。Kaspersky Endpoint Detection and Response Optimum の機能を有効化するための別のライセンスが本製品に追加されている場合は、EDR Optimum の現在および予備のライセンス キーと EDR Optimum ライセンスに関する情報も表示されます。

デバイス上のライセンスに関する情報を表示するには、次のコマンドを実行します：

```
kesl-control -L --query [--json]
```

`--json` はJSON形式でデータを出力します。もし `--json` キーが指定されなければ、設定は INI 形式でインポートされます。

コマンドを実行すると、次の情報がコンソールに表示されます：

- ライセンスが追加された場合の現在の製品ライセンスに関する情報：
  - 本製品を使用するライセンスの有効期限日時。
  - ライセンス期間が終了するまでの日数。
  - 保護機能の制限に関する情報。
  - 定義データベースのアップデートの制限に関する情報。
  - ライセンスのステータスに関する情報。
  - キーに関連付けられたライセンス種別。
  - キーのライセンス制限（ライセンスの個数）。
  - ライセンスを有効化するアプリケーションの名前。
  - 有効なライセンス（一意の英数字文字列）。
  - 有効化された日。
- 本製品の予備ライセンスの情報。本製品が標準モードで使用されており、予備のライセンスが追加されている場合に表示されます。アプリケーションが仮想環境を保護するために Light Agent モードで使用されている場合、予備のライセンスに関する情報は表示されません。予備のライセンスは SVM に追加されます。
  - 本製品を使用するライセンスの有効期限日時。
  - ライセンス期間が終了するまでの日数。

- 保護機能の制限に関する情報。
- 定義データベースのアップデートの制限に関する情報。
- ライセンスのステータスに関する情報。
- キーに関連付けられたライセンス種別。
- キーのライセンス制限（ライセンスの個数）。
- ライセンスを有効化するアプリケーションの名前。
- 有効化された日。

- ライセンスが追加された場合の現在の EDR Optimum ライセンスに関する情報：
  - Kaspersky Endpoint Detection and Response Optimum 機能を使用するためのライセンスの有効期限日時。
  - 定義データベースのアップデートの制限に関する情報。
  - ライセンスのステータスに関する情報。
  - キーに関連付けられたライセンス種別。
  - キーのライセンス制限（ライセンスの個数）。
  - ライセンスを有効化するアプリケーションの名前。
  - 有効なライセンス（一意の英数字文字列）。
  - 有効化された日。
- EDR Optimum の予備ライセンスの情報。本製品が標準モードで使用されており、予備の EDR Optimum ライセンスが追加されている場合に表示されます。アプリケーションが仮想環境を保護するために Light Agent モードで使用されている場合、予備のライセンスに関する情報は表示されません。予備のライセンスは SVM に追加されます。
  - Kaspersky Endpoint Detection and Response Optimum 機能を使用するためのライセンスの有効期限日時。
  - 定義データベースのアップデートの制限に関する情報。
  - ライセンスのステータスに関する情報。
  - キーに関連付けられたライセンス種別。
  - キーのライセンス制限（ライセンスの個数）。
  - ライセンスを有効化するアプリケーションの名前。
  - 有効化された日。

コマンドラインでのライセンス管理

デバイス上のライセンスを管理するには、ライセンス管理コマンドを使用します。

ライセンスを管理するコマンドは、アプリケーションが標準モードで使用されている場合にのみ実行できます。Kaspersky Endpoint Security を Light Agent モードで仮想環境を保護している場合、ライセンスの管理コマンドはエラーで終了します。このアプリケーションは、Kaspersky Security for Virtualization Light Agent の一部として有効化されるため、アプリケーションを個別に有効化する必要はありません。

アプリケーションに有効なライセンスを追加するには、次のコマンドを実行します：

```
kesl-control [-L] --add-active-key <ライセンス情報ファイルへのパス / アクティベーションコード>
```

説明：

- <ライセンス情報ファイルへのパス> – ライセンス情報ファイルへのパス。ライセンス情報ファイルが現在のディレクトリにある場合は、ファイル名だけを指定します。
- <アクティベーションコード> – アクティベーションコード。

アプリケーションに予備のライセンスを追加するには、次のコマンドを実行します：

```
kesl-control [-L] --add-reserve-key <ライセンス情報ファイルへのパス / アクティベーションコード>
```

デバイス上の製品に現在のライセンスがまだ追加されていない場合、コマンドは失敗します。

［ライセンスの追加］コマンドを使用して、製品ライセンスと EDR Optimum ライセンスを追加できます。コマンドでライセンスの種別を指定する必要はありません。

現在のアプリケーションライセンスを削除するには、次のコマンドを実行します：

```
kesl-control [-L] --remove-active-key
```

予備のアプリケーションライセンスを削除するには、次のコマンドを実行します：

```
kesl-control [-L] --remove-reserve-key
```

現在の EDR Optimum ライセンスを削除するには、次のコマンドを実行します：

```
kesl-control [-L] --remove-active-key --edr-optimum
```

予備の EDR Optimum ライセンスを削除するには、次のコマンドを実行します：

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

アプリケーションデータベースとモジュールのアップデート

米国領土では、貿易制限に従い、2024 年 9 月 10 日東部夏時間（EDT）午前 12 時以降、更新機能（ウイルス対策シグネチャの更新およびコードベースの更新を含む）がアプリケーションで利用できなくなります。

Kaspersky Endpoint Security のデータベースとアプリケーションモジュールをアップデートすることで、デバイス上で最新の保護状態が保たれます。世界中で日々新たなウイルスや脅威が出現しています。定義データベースには、脅威に関する情報とその脅威を無害化する方法が記録されています。迅速に脅威を検知するには、定期的にアプリケーションデータベースとモジュールをアップデートしてください。

定義データベースの定期的なアップデートには、現在の製品ライセンスが必要です。現在のライセンスがない場合は、1 回のみアップデートを実行できます。

更新中に、定義データベースと機能がダウンロードされ、デバイスにインストールされます。

定義データベースのアップデートのアップデートは、カスペルスキーのアップデート サーバー、管理サーバー リポジトリ、ローカルまたはネットワークディレクトリ、およびその他のアップデート元から入手できます。

Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、SVM 上のディレクトリがアップデート元として使用されます。

アップデートの際、デバイス上の製品モジュールと定義データベースが、アップデート元の最新バージョンと比較されます。現在の定義データベースやソフトウェアモジュールが最新バージョンと異なる場合は、アップデートの不足している部分がデバイスにインストールされます。

定義データベースが長期間アップデートされていない場合、アップデートパッケージのサイズが大きくなり、インターネットのトラフィック量が増えることがあります（最大数十 MB）。ディスク容量は最大 3 GB です。

アップデートは、カスペルスキーのアップデートサーバーから、または標準のネットワークプロトコルを使用して他の FTP/HTTP/HTTPS サーバーからダウンロードされます。既定では、インターネット接続設定が自動的に決定されます。プロキシサーバーを使用している場合は、アプリケーションの全般設定でプロキシサーバーの設定を指定します。

アップデート元に関係なく、*アップデート*タスクを使用してアップデートパッケージがダウンロードされ、定義データベースと機能のアップデートがデバイスにインストールされます。

*アップデート*の事前定義済みタスクがアプリケーション内に作成されます。このタスクを使用すると、定義データベースと機能のスケジュールされたアップデートとオンデマンドのアップデートを実行し、アップデート設定を構成できます。

Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、保護対象仮想マシン上のデータベースは、SVM 上のディレクトリをアップデート元として指定した特別なローカルの *アップデート*タスクを使用してアップデートされます。アップデートタスクは自動的に開始されます。このタスクを削除したり、設定を変更したりすることはできません。

Kaspersky Security Center で作成されたタスクを使用した定義データベースと機能の更新には対応していません。

Kaspersky Endpoint Security が標準モードで使用されている場合は、Kaspersky Security Center で、MMC 管理プラグインまたは Kaspersky Endpoint Security Web 管理プラグインのインストール後に初期設定ウィザードが作成するグループアップデートタスクを使用できます。

コマンドラインや Kaspersky Security Center でユーザーアップデートタスクを作成することもできます。

定義データベースと機能をアップデートするために次の設定を構成できます：

- 使用するアップデートシナリオに応じて、アプリケーションのアップデート受信元を選択します。
- 選択したアップデート元に接続しようとするときの応答タイムアウトを設定します。指定した時間内にアップデート元が応答しなかった場合、リスト上の次のアップデート元に通信します。
- アプリケーションモジュールとアプリケーションバージョンのアップデートをダウンロードしてインストールするするモード（ダウンロードしてインストールする、ダウンロードのみ、またはダウンロードしない）を選択します。
- アップデートのタスク実行スケジュールを設定します。既定では、アプリケーションは 60 分ごとにデータベースをアップデートします。

データベースとモジュールのアップデート

アップデート中に、以下のオブジェクトがダウンロードされ、デバイスにインストールされます：

- 定義データベース。定義データベースには、マルウェアシグネチャのデータベースや、ネットワーク攻撃の説明、悪意のある Web サイトおよびフィッシングサイトのアドレスのデータベース、バナー広告のデータベース、スパムのデータベース、そしてその他のデータが含まれます。

  デバイス上の定義データベースのアップデートが中断されたり、エラーになったりした場合は、以前にインストールされた定義データベースが引き続き使用されます。以前に定義データベースがインストールされていなかった場合、製品は「定義データベースなし」モードでの動作を継続します。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引き続き使用できます。

  データベースが 3 日以内にダウンロードされたものであれば最新です。既定では、前回インストールされた定義データベースのアップデートが、カスペルスキーのサーバーで公開されてから 3 日～6 日経過している場合、*定義データベースが未アップデートイベント*（*BasesAreOutOfDate*）が生成されます。また、定義データベースをアップデートせずに 7 日間が過ぎると、*定義データベースが長期間アップデートされていません*（*BasesAreTotallyOutOfDate*）というイベントが生成されます。

- ソフトウェアモジュール。モジュールアップデートは、製品の脆弱性を解消し、デバイスを保護する方法を改善することを目的としています。モジュールのアップデートにより、製品コンポーネントの動作が変更され、新しい機能が追加される場合があります。

  ソフトウェアモジュールは製品の状態（起動、停止、Kaspersky Security Center のポリシーによる管理）やアップデートのスケジュールに関係なくインストールできます。ソフトウェアモジュールのアップデート処理中でも、Kaspersky Endpoint Security によりデバイスの保護が継続されます。アップデート中に、アプリケーション設定とアプリケーションログファイルが新しいバージョンのアプリケーションに移行されます。アップデート後、Kaspersky Endpoint Security を再起動する必要があります。

  製品の設定の移行が失敗した場合、失敗した理由にかかわらず、本製品の設定は既定値に設定されます。

  アップデートが完了した後、アプリケーションの再起動前にアプリケーションの設定に加えられた変更は保存されません。

本製品を自動パッチでバージョンをアップデートした後、オペレーティングシステムとの対話に使用するメカニズムが変更されます：iptables、iptables-restore システムユーティリティを使用してルールが管理されます。

アップデート後に本製品が正しく機能しない場合、本製品は自動的に旧バージョンにロールバックされます。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。

アップデート元とシナリオ

*アップデート元*とは、Kaspersky Endpoint Security 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が含まれているリソースのことです。アップデート元に指定できるのは、FTP サーバー、HTTP サーバー、または HTTPS サーバー（カスペルスキーのアップデートサーバーなど）、およびユーザーによってマウントされるローカルディレクトリやネットワークディレクトリです。

Kaspersky Endpoint Security をLight Agent モードで使用して仮想環境を保護する場合、保護対象の仮想マシン上のデータベースは SVM 上のディレクトリから更新されます。

主なアップデート元は、カスペルスキーのアップデートサーバーです。アップデートタスクの設定で、その他の *アップデート元*を指定できます。アップデート元からアップデートを実行できない場合、次のアップデート元に切り替わります。

Kaspersky Endpoint Security は、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ための、以下のシナリオをサポートしています：

- カスペルスキーのアップデートサーバーからのアップデート。カスペルスキーのアップデートサーバーは世界中の様々な国に配置されており、アップデートの高い信頼性を確保します。あるサーバーからアップデートを実行できない場合、アプリケーションは次のサーバーに切り替えます。アップデートは、HTTPS プロトコルを使用してダウンロードされます。

- 一元化されたアップデート。一元化されたアップデートは、外部のインターネットトラフィックを削減し、アップデートの便利な監視を提供します。

  一元化されたアップデートを設定するには、次の手順を実行します：

  1. アップデートパッケージを組織のネットワーク内のリポジトリにダウンロードします。

     Kaspersky Security Center 管理サーバーのリポジトリをリポジトリとして使用できます。

     アップデートパッケージは、管理サーバーの *管理サーバーリポジトリへのアップデートのダウンロード* タスクを介して管理サーバーリポジトリにダウンロードされます。

     Kaspersky Security Center Cloud コンソールを使用してアプリケーションを管理する場合は、配布ポイント（ネットワークエージェントがインストールされているデバイス）のリポジトリをリポジトリとして使用できます。ディストリビューションポイントの詳細については、Kaspersky Security Center のヘルプを参照してください。

  2. アップデートパッケージをクライアントデバイスに配布します。

     Kaspersky Endpoint Security の［*アップデート*］タスクにより、アップデートパッケージがクライアントデバイスに配布されます。タスク設定で、Kaspersky Security Center 管理サーバーをアップデート元として選択します。

- ユーザーによってマウントされたローカルまたはネットワークディレクトリ（SMB/NFS）、または FTP、HTTP、または HTTPS サーバーから更新します。*アップデート*タスクの設定で、カスタムのアップデート元を指定できます。

Web コンソールでの定義データベースと機能のアップデート

Kaspersky Endpoint Security のデータベースとアプリケーションモジュールをアップデートする手順は、アプリケーションの使用量モードによって異なります。ここでは、標準モードでアプリケーションをアップデートする手順を説明します。本製品 を Light Agent モードで使用して仮想環境を保護する場合、Kaspersky Security Center で作成したタスクを使用して定義データベースと機能をアップデートすることはできません。アップデートは、ローカルの事前定義済みタスクを使用して実行されます。

Web コンソールでは、*アップデートタスク*を使用して定義データベースと機能をアップデートできます。自動的に作成された*アップデートグループタスク*を使用したり、アップデート用のユーザータスクを作成したりできます。

Web コンソールでアップデートの設定を構成します：

1. Web コンソールのメインウィンドウで、**アセット（デバイス）→タスク**の順に選択します。

   タスクのリストが表示されます。

2. 次のいずれかの操作を実行します：

   - 特定の管理グループに含まれるすべてのデバイスで実行されているタスクの設定を編集するには、ウィンドウの上部にある**現在のパス**フィールドのリンクをクリックし、開いたウィンドウで管理グループを選択します。

     リストには、選択した管理グループのために設定されたタスクのみが表示されます。

   - 1つ以上のデバイスで実行されているタスク（一連のデバイスに対するタスク）の設定を編集するには、ウィンドウの上部にある**現在のパス**フィールドのリンクをクリックし、開いたウィンドウの管理サーバー名の最上位のノードを選択します。

     リストには、管理サーバーで作成されたすべてのタスクが表示されます。

3. タスクのリストで、必要な**アップデート**タスクを選択し、タスク名のリンクをクリックしてタスクのプロパティウィンドウを開きます。

4. タスク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。左側のリストで［**アップデート元**］セクションを選択します。

5. 使用するアップデートシナリオに応じて、定義データベースと機能に対するアプリケーションのアップデート受信元を選択します。

   Web コンソールを使用してアプリケーションを管理している場合、アップデート元のリストには、カスペルスキーのアップデートサーバーと Kaspersky Security Center 管理サーバーが含まれます。Kaspersky Security Center Cloud コンソールを使用してアプリケーションを管理している場合、アップデート元のリストには Kaspersky アップデートサーバーと配布ポイントが含まれています（配布ポイントの詳細については、Kaspersky Security Center のヘルプを参照してください）。他のアップデート元をリストに追加できます。

   ローカルまたはグローバルネットワーク内のその他のソースオプションを選択すると、アップデート元のリストを作成できます。アップデート元には、FTP/HTTP/HTTPS サーバーを指定できます。アップデート元からアップデートを実行できない場合、次のアップデート元に切り替わります。アプリケーションは、表に表示されている順序でアップデート元にアクセスします。

6. **設定**セクションを選択し、その他のアップデート設定を構成します。

7. **スケジュール**タブを選択し、アップデートタスクを実行するスケジュールを構成します。

Kaspersky Security Center をアップデート元として選択した場合は、**開始スケジュール**ドロップダウンリストから**リポジトリにアップデートをダウンロードするとき**を選択します。タスクのスケジュール設定に関する詳細は、Kaspersky Security Center のヘルプを参照してください。

8. **保存**をクリックして、変更内容を保存します。

タスクは設定されたスケジュールに従って開始されます。タスクを手動で実行することもできます。

アップデートタスクのアップデート元セクション

設定	説明
アップデート元	このセクションでは、アップデート元を選択できます： • **カスペルスキーのアップデートサーバー** - カスペルスキー製品用の定義データベースのアップデートが公開されます（既定値）。 • ［**Kaspersky Security Center**］– Kaspersky Security Center 管理サーバー（このオプションは、Web Console でのみ使用可能です）。 • **ディストリビューションポイント**（このオプションは、Kaspersky Security Center Cloud コンソールでのみ使用できます）。 • **ローカルネットワークまたはインターネット上の他のアップデート元** - HTTP / HTTPS / FTP サーバー、またはローカルネットワークサーバー上のディレクトリ。
他のアップデート元が使用できない場合はカスペルスキーのアップデートサーバーを使用する	このチェックボックスでは、選択したアップデート元が使用できない場合に、アップデート元としてカスペルスキーのアップデートサーバーを使用するかどうかを選択します。 このチェックボックスは、［**アップデート元**］ブロックで［**ローカルネットワークまたはインターネット上の他のアップデート元**］または［**Kaspersky Security Center**］が選択されている場合に使用できます。 既定では、このチェックボックスはオンです。
カスタムアップデート元	この表には、定義データベースのカスタムアップデート元のリストが含まれています。アップデートプロセス中、アップデート元の表の並び順に従ってアップデート元にアクセスします。 表には次の列があります： • ［**アップデート元**］：HTTP / HTTPS / FTP サーバー、またはローカルネットワークサーバー上のディレクトリ。 • この切り替えボタンでは、アップデート元がタスクで使用されているかどうかを示しています（［**有効**］または［**無効**］）。表内の切り替えボタンを有効または無効にするほか、アップデート元の名前のリンクをクリックして開く［**アップデート元**］ウィンドウで［**このアップデート元を使用する**］をオンまたはオフにすることができます。 この表は、［**ローカルネットワークまたはインターネット上の他のアップデート元**］をオンにすると使用できます。 既定では、表は空です。 表内のアップデート元に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

アップデートタスクの設定セクション

設定	説明
アップデート元からの応答を待つ時間（秒）	選択したアップデート元からの応答をアプリケーションが待機する最大時間（秒）。この時間が経過しても応答がない場合、アップデート元との通信がないことを示すイベントがタスクログに記録されます。 使用できる値：0 - 120。0 を指定すると、選択されたアップデート元からの応答を待つ時間は無制限になります。 既定値：10 秒。
ソフトウェアアップデートのダウンロードの設定	ドロップダウンリストでは、定義データベースのアップデートモードを選択できます： • アップデートを［**ダウンロードしない**］でください。このリスト項目が選択されている場合、アプリケーションをアップデートすることはできません。 • アップデートファイルを［**ダウンロード**］しますが、ユーザーデバイスにインストールしません（既定値）。 • クライアントデバイスへのアップデートを［**ダウンロードしてインストールする**］します。アップデートがインストールされると、アプリケーションは自動的に再起動します。 この機能は、KESL コンテナではサポートされていません。

管理コンソールでの定義データベースと機能のアップデート

Kaspersky Endpoint Security のデータベースとアプリケーションモジュールをアップデートする手順は、アプリケーションの使用量モードによって異なります。ここでは、標準モードでアプリケーションをアップデートする手順を説明します。本製品 を Light Agent モードで使用して仮想環境を保護する場合、Kaspersky Security Center で作成したタスクを使用して定義データベースと機能をアップデートすることはできません。アップデートは、ローカルの事前定義済みタスクを使用して実行されます。

管理コンソールでは、*アップデートタスク*を使用して定義データベースと機能をアップデートできます。自動的に作成された*アップデートグループタスク*を使用したり、アップデート用のユーザータスクを作成したりできます。

管理コンソールでアップデートの設定を構成します：

1. 管理コンソールで、次のいずれかの処理を実行します。
   - 指定した管理グループに含まれるデバイスで実行されるタスクの設定を編集するには、コンソールツリーでこの管理グループを選択し、ワークスペースで**タスク**タブを選択します。
   - 1つ以上のデバイスで実行されるタスク（一連のデバイスのタスク）の設定を編集するには、コンソール ツリーで**タスク**フォルダーを選択します。
2. タスクのリストから、必要な**アップデート**タスクを選択し、ダブルクリックしてプロパティウィンドウを開きます。
3. タスクのプロパティウィンドウで、左側のリストから［**アップデート元**］セクションを選択します。
4. 使用するアップデートシナリオに応じて、定義データベースと機能に対するアプリケーションのアップデート受信元を選択します。

   アップデート元のリストには、カスペルスキーのアップデートサーバーと Kaspersky Security Center 管理サーバーが含まれています。他のアップデート元をリストに追加できます。

   ローカルまたはグローバルネットワーク内のその他のソースオプションを選択すると、アップデート元のリストを作成できます。アップデート元には、FTP/HTTP/HTTPS サーバーを指定できます。アップデート元からアップデートを実行できない場合、次のアップデート元に切り替わります。アプリケーションは、表に表示されている順序でアップデート元にアクセスします。
5. **設定**セクションを選択し、その他のアップデート設定を構成します。
6. **スケジュール**セクションを選択し、アップデートタスクを実行するスケジュールを構成します。

   Kaspersky Security Center をアップデート元として選択した場合は、**開始スケジュール**ドロップダウンリストから**リポジトリにアップデートをダウンロードするとき**を選択します。タスクのスケジュール設定に関する詳細は、Kaspersky Security Center のヘルプを参照してください。
7. **プロパティ：<タスク名>** ウィンドウで**適用**または**OK**をクリックして、加えた変更を保存します。

タスクは設定されたスケジュールに従って開始されます。タスクを手動で実行することもできます。

アップデートタスクのアップデート元セクション

設定	説明
アップデート元	このセクションでは、アップデート元を選択できます：

	• **カスペルスキーのアップデートサーバー** - カスペルスキー製品用の定義データベースのアップデートが公開されます（既定値）。 • ［**Kaspersky Security Center**］– Kaspersky Security Center 管理サーバー。 • **ローカルネットワークまたはインターネット上の他のアップデート元** - HTTP / HTTPS / FTP サーバー、またはローカルネットワークサーバー上のディレクトリ。
他のアップデート元が使用できない場合はカスペルスキーのアップデートサーバーを使用する	このチェックボックスでは、選択したアップデート元が使用できない場合に、アップデート元としてカスペルスキーのアップデートサーバーを使用するかどうかを選択します。 このチェックボックスは、［**アップデート元**］ブロックで［**ローカルネットワークまたはインターネット上の他のアップデート元**］または［**Kaspersky Security Center**］が選択されている場合に使用できます。 既定では、このチェックボックスはオンです。
カスタムアップデート元	この表には、定義データベースのカスタムアップデート元のリストが含まれています。アップデートプロセス中、アップデート元の表の並び順に従ってアップデート元にアクセスします。 表には次の列があります： • **アップデート元のアドレス**：HTTP / HTTPS / FTP サーバー、またはローカルネットワークサーバー上のディレクトリ。 • **ステータス**：そのアップデート元がタスクで使用されるかどうかが表示されます（**使用中 / 未使用**）。ステータスを変更するには、［**アップデート元**］ウィンドウで［**このアップデート元を使用する**］をオンまたはオフにします。［アップデート元］ウィンドウは、［**編集**］をクリックすると表示されます。 この表は、［**ローカルネットワークまたはインターネット上の他のアップデート元**］をオンにすると使用できます。 表内のアップデート元に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。 ［**下へ**］をクリックすると、表内で選択した項目が下に移動します。 このボタンは、1つの項目のみを表から選択している場合に使用できます。 ［**上へ**］をクリックすると、表内で選択した項目が上に移動します。 このボタンは、1つの項目のみを表から選択している場合に使用できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。

	［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。 既定では、表は空です。

アップデートタスクの設定セクション

設定	説明
アップデート元からの応答を待つ時間（秒）	選択したアップデート元からの応答をアプリケーションが待機する最大時間（秒）。この時間が経過しても応答がない場合、アップデート元との通信がないことを示すイベントがタスクログに記録されます。 使用可能な値：0 - 120。0 を指定すると、選択されたアップデート元からの応答を待つ時間は無制限になります。 既定値：10 秒。
ソフトウェアアップデートのダウンロードの設定	ドロップダウンリストでは、定義データベースのアップデートモードを選択できます： • アップデートを［**ダウンロードしない**］でください。このリスト項目が選択されている場合、アプリケーションをアップデートすることはできません。 • アップデートファイルを［**ダウンロード**］しますが、ユーザーデバイスにインストールしません（既定値）。 • クライアントデバイスへのアップデートを［**ダウンロードしてインストールする**］します。アップデートがインストールされると、アプリケーションは自動的に再起動します。 この機能は、KESL コンテナではサポートされていません。

コマンドラインでの定義データベースと機能のアップデート

Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合、保護対象仮想マシン上のデータベースは、SVM 上のディレクトリをアップデート元として指定した特別なローカルの *アップデート*タスクを使用してアップデートされます。アップデートタスクは自動的に開始されます。このタスクを削除したり、設定を変更したりすることはできません。

コマンドラインでは、次の方法で定義データベースと機能のアップデートができます：

- *アップデート*の事前定義済みタスクを使用します。このタスクを手動で開始、停止、一時停止、再開し、タスクの実行スケジュールを設定できます。このタスクの設定を編集することで、スキャン設定を構成できます。
- アップデートにユーザータスクを使用します（*アップデート*タイプのタスク）。ユーザータスクを手動で開始し、タスクスケジュールを設定できます。

アップデートタスクの設定

設定	説明	値
SourceType	製品がアップデートを受信するアップデート元。	KLServers（既定値）- カスペルスキーのアップデートサーバーのいずれかからアップデートを受信します。アップデートは、HTTPS プロトコルを使用してダウンロードされます。 SCServer ローカルネットワーク上にインストールされている管理サーバーからアップデートを保護対象のデバイスにダウンロードします。組織のデバイス保護の集中管理に Kaspersky Security Center を使用する場合は、このアップデート元を選択できます。 Custom - [CustomSources.item_#] セクションで指定されたカスタムのアップデート元からアップデートをダウンロードします。FTP/HTTP/HTTP サーバーのディレクトリ、または保護されたクライアントデバイスにマウントされた任意のデバイスのディレクトリ（Samba プロトコルまたは NFS プロトコルでマウントされたリモートデバイスのディレクトリを含む）を指定できます。
UseKLServersWhenUnavailable	すべてのカスタムのアップデート元が使用できない場合における、カスペルスキーのアップデートサーバーへのアクセス。	Yes（既定値）- すべてのカスタムのアップデート元が使用できない場合に、カスペルスキーのアップデートサーバーに接続します。 No - すべてのカスタムのアップデート元が使用できない場合に、カスペルスキーのアップデートサーバーに接続しません。
ApplicationUpdateMode	ソフトウェアアップデートのダウンロードとインストールの設定。	Disabled - ソフトウェアアップデートのダウンロードもインストールもしません。 DownloadOnly（既定値）- ソフトウェアアップデートのダウンロードはするが、インストールはしません。 DownloadAndInstall - ソフトウェアアップデートを自動的にダウンロードしてインストールします。アップデートがインストールされると、アプリケーションは自動的に再起動します。
ConnectionTimeout	接続試行中のアップデート元の応答タイムアウト（秒単位）。指定した時間内にアップデート元が応答しなかった場合、リスト上の次のアップデート元に通信します。	0 ～120 の範囲内の整数のみを使用できます。 既定値：10
[CustomSources.item_#] セクションには、次の設定が含まれています：		
URL	ローカルエリアネットワークまたはインターネットに	既定値は定義されていません。 例：

	あるカスタムのアップデート元のアドレス。	`URL=http://example.com/bases/` - アップデートが置かれている HTTP サーバーのアドレスとディレクトリ。 `URL=/home/bases/` - 定義データベースが置かれている保護されたコンピューターのディレクトリ。
`Enabled`	`URL` 設定で指定されたアップデート元を使用します。 タスクを実行するには、少なくとも 1 つのアップデート元を有効にする必要があります。	`Yes` - アップデート元を使用します。 `No` - アップデート元を使用しません。 既定値は定義されていません。

Kaspersky Update Utility を使用したアップデート

インターネットトラフィックを抑制するため、Kaspersky Update Utility を使用して、組織の LAN のデバイスに対してアプリケーションデータベースとモジュールを共有ディレクトリからアップデートするように設定できます。これを行うには、組織の LAN 上の 1 台のデバイスが Kaspersky Security Center 管理サーバーまた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パッケージを取得し、このアップデートパッケージをユーティリティを使用して共有ディレクトリにコピーする必要があります。組織の LAN 上の他のデバイスは、この共有ディレクトリからアップデートパッケージを取得できます。

Kaspersky Update Utility を使用して共有ディレクトリからデータベースのアップデートを設定するには、次の手順を実行します。

1. 組織の LAN の 1 台のデバイスに Kaspersky Update Utility をインストールします。

   Kaspersky Update Utility 配布キットは、カスペルスキーのテクニカルサポートサイトからダウンロードできます。

2. Kaspersky Update Utility の設定で、アップデートパッケージの共有ディレクトリへのコピーを定義します。

   アップデート元（管理サーバーのリポジトリなど）を、Kaspersky Update Utility がアップデートパッケージをコピーする共有ディレクトリを選択します。Kaspersky Update Utility の使用に関する詳細は、ナレッジベースを参照してください。

3. 組織の LAN 上の他のデバイスに、指定された共有ディレクトリからのアプリケーションモジュールのアップデートを定義します。

   a. **Web コンソール**または管理コンソールを使用して、必要なデバイスで実行されるアップデートタスクのプロパティを開きます。

   b. タスクプロパティウィンドウで、**アップデート元**セクションを選択します。

   c. **アップデート元**セクションで、**ローカルネットワークまたはインターネット上の他のアップデート元**を選択します。

4. アップデート元の表で**追加**ボタンをクリックし、共有ディレクトリへのパスを指定します。

アップデート元のアドレスは、Kaspersky Update Utility で設定されているアドレスと一致する必要があります。

5. ［**このアップデート元を使用**］をオンにして、［OK］をクリックします。

6. 表内で、ボタン［**上**］と［**下**］でアップデート元の順番を設定します。

7. タスク設定への変更を保存します。

定義データベースと機能のアップデートのロールバック

Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護している場合は、タスクでデータベースのアップデートをロールバックすることはできません。

定義データベースのアップデートが初めて実行されると、定義データベースを以前のバージョンへロールバックする機能を使用できるようになります。

ユーザーがアップデートプロセスを開始するたびに、Kaspersky Endpoint Security では現在の定義データベースのバックアップコピーが作成されます。これにより、必要に応じて、定義データベースを旧バージョンにロールバックできます。

前回の定義データベースのアップデートへのロールバックは、たとえば新しい定義データベースバージョンに不適切なシグネチャが含まれていて、Kaspersky Endpoint Security が安全なアプリケーションをブロックしてしまっているような場合に役立ちます。

コマンドラインでアップデートをロールバックするには、事前定義済みの *ロールバック*タスクを実行するか、アップデートをロールバックするためのユーザー タスク（*ロールバック*タイプのタスク）を作成して実行できます。

Kaspersky Security Center では、Web コンソールまたは管理コンソールを使用して、管理グループまたは個々のデバイスのロールバックタスクを作成できます。

この *ロールバック*タスクには設定がありません。

ファイル脅威対策

ファイル脅威対策コンポーネントは、デバイスのファイルシステムへの感染を防止します。このコンポーネントは、Kaspersky Endpoint Security の起動時に既定で自動的に有効になります。デバイスのメモリに常駐し、開いたファイル、保存されたファイル、起動されたファイルをすべてリアルタイムでスキャンします。

マルウェアを検知すると、Kaspersky Endpoint Security は感染したファイルを削除し、このファイルから開始したマルウェアのプロセスを終了させることができます。

コンポーネントの動作は、アプリケーションの全般設定で選択できるファイル操作遮断モードの影響を受けます。既定では、スキャン中はファイルへのアクセスがブロックされます。

ファイル脅威対策が有効で、コンテナ監視が有効な場合、アプリケーションは、対応しているすべてのオペレーティングシステム上のすべての名前空間とコンテナもスキャンします。

ファイル脅威対策を有効または無効にしたり、次の保護設定を行うことができます：

- ファイルスキャンモード（開いたとき、または開いて変更したとき）を選択します。
- アーカイブ、メールデータベース、テキスト形式の電子メールメッセージのスキャンを有効または無効にします。
- テキスト形式のファイルを再スキャンから一時的に除外します。
- スキャンするオブジェクトのサイズとオブジェクトのスキャン時間を制限します。
- 感染したオブジェクトに対して実行される処理を選択します。
- スキャン範囲を設定します。アプリケーションは、ファイルシステムの指定された領域内のオブジェクトをスキャンします。
- スキャンからのオブジェクトの除外を設定します。［*スキャンの除外*］は一連の条件です。これらの条件を満たす場合、アプリケーションはオブジェクトのウイルスやその他のマルウェアのスキャンを行いません。スキャンから除外できるのは次のとおりです：
  - オブジェクトの名前またはマスク
  - オブジェクト内で検知された脅威の名前
  - ファイルシステムの指定された領域にあるファイルとディレクトリ
  - 指定されたプロセスによって変更されるプロセスとファイル
- スキャン中のヒューリスティック分析と iChecker テクノロジーの使用を設定します。
- スキャンされた非感染オブジェクト、アーカイブ内のスキャンオブジェクト、および未処理のオブジェクトに関する情報のログ記録を有効または無効にします。

ファイル脅威対策コンポーネントを最適化するには、ネットワークディレクトリからコピーされる任意のファイルをスキャンから除外します。ローカルディレクトリへのコピーのプロセスの完了後にのみ、ファイルがスキャンされます。ネットワークディレクトリのファイルをスキャンから除外するには、ネットワークディレクトリからのファイルのコピーに使用されるユーティリティ（cp ユーティリティなど）のプロセスに基づいて除外を設定します。Kaspersky Security Center を使用して製品を管理する場合は、Web コンソールまたは管理コンソールのプロセスに基づいて除外を設定できます。コマンドラインを使用して製品を管理している場合は、OAS タスクの設定に [ExcludedForProgram.item_ #] セクションを追加することで、プロセスによる除外を設定できます。

Web コンソールでのファイル脅威対策の設定

Web コンソールでは、ポリシーのプロパティ内でファイル脅威対策を管理できます（**製品設定 → 脅威対策 → ファイル脅威対策**）。

ファイル脅威対策の設定

設定	説明
ファイル脅威対策の有効化 / 無効化	この切り替えボタンでは、すべての管理対象デバイスでファイル脅威対策コンポーネントを有効にするかどうかを選択します。 この切り替えボタンは既定でオンになっています。
ファイル脅威対策の動作方法	ドロップダウンリストからファイル脅威対策コンポーネントの動作方法を選択できます： • **スマートチェック**（既定値） - ファイルが開かれた時にファイルをスキャンし、ファイルが変更された場合は閉じる時にもう一度スキャンします。ある処理によって一定期間の間にファイルが複数回アクセスおよび変更された場合は、処理によってファイルが最後に閉じられた時にのみ、もう一度スキャンが実行されます。 • **開いた時** - ファイルの読み込み、実行、変更のためにファイルが開かれた時にファイルをスキャンします。 • **開いた時と変更された時** - ファイルが開かれた時にファイルをスキャンし、ファイルが変更されている場合は閉じる時にもう一度スキャンします。
最初の処理	このドロップダウンリストでは、感染したオブジェクトの検知時に実行する最初の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています（既定値）。 • **ブロック**：オブジェクトへのアクセスをブロックします。
次の処理	このドロップダウンリストでは、感染したオブジェクトに対する最初の処理が成功しなかった場合に実行する次の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。

	• **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています。 • **ブロック**：オブジェクトへのアクセスをブロックします（既定値）。
スキャン範囲	［**スキャン範囲を設定する**］をクリックすると、［**保護範囲**］ウィンドウが表示されます。
アーカイブをスキャン	このチェックボックスでは、アーカイブをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、アーカイブがスキャンされます。 アーカイブをスキャンするには、アーカイブを解凍する必要があるためスキャン速度が遅くなる可能性があります。［**スキャン時間が次を超えたらファイルをスキップする（秒）**］および［**ファイルのサイズが次を超えたらスキップする（MB）**］を有効にして設定すると、アーカイブのスキャンの所要時間を減らすことができます。 このチェックボックスをオフにすると、アーカイブはスキャンされません。 既定では、このチェックボックスはオフです。
SFX アーカイブをスキャン	このチェックボックスでは、*自己解凍アーカイブ*をスキャンするかどうかを選択します。自己解凍アーカイブとは、実行可能な展開モジュールを含むアーカイブです。 このチェックボックスをオンにすると、自己解凍アーカイブがスキャンされます。 このチェックボックスをオフにすると、自己解凍アーカイブはスキャンされません。 このチェックボックスは、［**アーカイブをスキャン**］がオフの場合に使用できます。 既定では、このチェックボックスはオフです。
メールデータベースをスキャン	このチェックボックスでは、Microsoft Outlook、Outlook Express などのメールアプリケーションのメールデータベースをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、メールデータベースはスキャンされます。 このチェックボックスをオフにすると、メールデータベースはスキャンされません。 既定では、このチェックボックスはオフです。
メール形式のファイルをスキャン	このチェックボックスでは、プレーンテキストのメールメッセージのファイルをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、プレーンテキストのメッセージがスキャンされます。 このチェックボックスをオフにすると、プレーンテキストのメッセージはスキャンされません。 既定では、このチェックボックスはオフです。
テキストファイルをスキップ	テキスト形式のファイルをスキャンから一時的に除外します。 このチェックボックスをオンにすると、最後のスキャンから 10 分以内にテキストファイルが同じプロセスで再利用される場合は、テキストファイルはスキャンされません。この設定により、製品ログのスキャンを最適化できます。 このチェックボックスをオフにすると、ファイルはスキャンされます。 既定では、このチェックボックスはオフです。
スキャン時間が次を超えたらファイルをスキ	このフィールドでは、ファイルをスキャンする最大時間を秒単位で指定できます。指定した時間が経過した後、ファイルのスキャンは停止されます。 使用できる値：`0` ～ `9999`。値が `0` に設定されると、スキャン時間は制限されません。 既定値は `60` です。

ップする（秒）	
ファイルのサイズが次を超えたらスキップする（MB）	このフィールドでは、スキャンするファイルの最大サイズをメガバイト単位で指定できます。 使用できる値：`0` ～ `999999`。値が `0` に設定されると、サイズにかかわらず、すべてのファイルがスキャンされます。 既定値は `0` です。
感染していないオブジェクトを記録する	このチェックボックスでは、*ObjectProcessed* イベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、スキャンされたすべてのオブジェクトの *ObjectProcessed* イベントをログに記録します。 このチェックボックスをオフにすると、イベントは記録されません。 既定では、このチェックボックスはオフです。
処理されていないオブジェクトを記録する	このチェックボックスでは、スキャン中にファイルを処理できない場合、*ObjectNotProcessed* イベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、*ObjectNotProcessed* イベントをログに記録します。 このチェックボックスをオフにすると、イベントは記録されません。 既定では、このチェックボックスはオフです。
圧縮されたオブジェクトを記録する	このチェックボックスでは、検出されたすべての圧縮されたオブジェクトに関する *PackedObjectDetected* イベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、*PackedObjectDetected* イベントをログに記録します。 このチェックボックスをオフにすると、イベントは記録されません。 既定では、このチェックボックスはオフです。
iChecker 技術を使用する	このチェックボックスでは、前回のファイルのスキャン以降の新しいファイルおよび変更されたファイルのみをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、前回のスキャン以降の新しいファイルおよび変更されたファイルのみがスキャンされます。 このチェックボックスをオフにすると、作成日または変更日に関係なくファイルがスキャンされます。 既定では、このチェックボックスはオンです。
ヒューリスティック分析を使用する	このチェックボックスでは、オブジェクトのスキャン中にヒューリスティック分析を使用するかどうかを選択します。 既定では、このチェックボックスはオンです。
ヒューリスティック分析のレベル	［**ヒューリスティック分析を使用する**］をオンにすると、ドロップダウンリストでヒューリスティック分析レベルを選択できます。 • **低**：スキャンの詳細レベルが最も低く、システム負荷は最小です。 • **中**：スキャンの詳細レベルは中程度で、システム負荷のバランスが取れています。 • **高**：スキャンの詳細レベルが最も高く、システム負荷は最大です。 • **推奨**（既定値）：カスペルスキーが推奨する、最適なレベルです。保護の質と保護対象サーバーのパフォーマンスの最適な組み合わせを提供します。

［保護範囲］ウィンドウ

この表にはスキャン範囲が含まれます。表で指定されたパス内のファイルとディレクトリをすべてスキャンします。表には既定で、すべての共有ディレクトリを対象とする1つの保護範囲が表示されています。

保護範囲設定

設定	説明
範囲名	スキャン範囲名。
パス	スキャンするディレクトリのパス。
ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、範囲の表の並び順でスキャンされます。必要に応じて、サブディレクトリを親ディレクトリよりもリストの上に配置し、親ディレクトリとは異なるセキュリティ設定をサブディレクトリに設定します。

［保護範囲の追加］ウィンドウ

このウィンドウでは、保護範囲の追加や設定ができます。

設定	説明
範囲名	保護範囲の名前を入力するフィールド。この名前は、［**スキャン範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品がこの範囲をスキャンするかどうかを選択します。 チェックボックスをオンにすると、動作中にこの保護範囲が処理されます。 このチェックボックスをオフにすると、動作中にこの保護範囲は処理されません。このチェックボックスをオンにすることにより、後からこの範囲をコンポーネント設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	ドロップダウンリストからファイルシステムの種別を選択できます： • **Local**（既定値）：ローカルディレクトリ。この項目を選択する場合は、ローカルディレクトリのパスを指定する必要があります。 • **Mounted** – マウントされたリモートまたはローカルのディレクトリ。この項目を選択する場合は、ファイルシステムのプロトコルまたは名前を指定する必要があります。 • **Shared** – Samba または NFS プロトコルでアクセス可能な保護されているサーバーファイルシステムリソースを表示します。 • **リモートでマウント済みのすべての場所** – Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。 • **共有済みのすべての場所** – Samba および NFS プロトコルでアクセス可能なすべての保護されているサーバーファイルシステムリソース。
アクセスプロトコル	ドロップダウンリストからリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。 このドロップダウンリストは、ファイルシステムのドロップダウンリストから［**Shared**］または［**Mounted**］を選択した場合に使用できます。
パス	保護範囲に含めるディレクトリのパスを指定するための入力フィールドです。パスの指定にマスクおよびタグを使用できます。

特別なタグを使用してコンテナまたはイメージを指定できます：

- [container-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>]/<ローカルディレクトリへのパス>
- [image-id:<識別子>]/<ローカルディレクトリへのパス>
- [image-name:<名前>]/<ローカルディレクトリへのパス>

[container-id:<識別子>]、[container-name:<名前>]、[image-id:<識別子>]、および [image-name:<名前>]/<ローカルディレクトリ> タグの一意の組み合わせを使用することもできます。

1つのエリア内で1～4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。

例：

- [container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>

名前と識別子にはマスク（? および * 記号）を使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリをスキャンします。 このフィールドは、ファイルシステムのドロップダウンリストから［**Local**］を選択した場合に使用できます。 ファイルシステムのドロップダウンリストから［**Local**］が選択され、パスが指定されていない場合、ローカルファイルシステムのすべてのディレクトリがスキャンされます。
共有リソース名	保護範囲に追加するディレクトリがあるファイルシステム共有リソースの名前を入力するためのフィールドです。 このフィールドは、［ファイルシステム］ドロップダウンリストで［**Mounted**］が選択され、［**アクセスプロトコル**］ドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。
マスク	このリストには、動作中に製品がスキャンするオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

ファイル脅威対策の除外

*保護除外*とは、Kaspersky Endpoint Security がオブジェクトをスキャンしてウイルスやその他のマルウェアを検知しない一連の条件です。マスクと脅威名でオブジェクトを除外し、プロセスの除外を設定することもできます。

Web コンソールでは、ポリシーのプロパティ内でファイル脅威対策の除外を設定できます（［**商品設定**］→［**脅威対策**］→［**ファイル脅威対策の除外**］）。

保護除外の設定

設定	説明
除外範囲	［**除外リストを設定する**］をクリックすると、［**除外範囲**］ウィンドウが表示されます。このウィンドウでは、保護除外のリストを定義できます。
マスクによる除外	［**除外をマスクで設定する**］をクリックすると、［**マスクによる除外**］ウィンドウが表示されます。このウィンドウでは、名前のマスクにより、スキャンからのオブジェクトの除外を設定できます。
脅威の名前による除外	［**除外を脅威名で設定する**］をクリックすると、［**脅威の名前による除外**］ウィンドウが表示されます。このウィンドウでは、脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。
プロセスによる除外	［**除外をプロセスで設定する**］をクリックすると、［**プロセスによる除外**］ウィンドウが表示されます。このウィンドウで、プロセスの動作を除外できます。

［除外範囲］ウィンドウ

この表には、スキャンの除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	スキャンから除外されるディレクトリのパス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲の追加］ウィンドウ

このウィンドウでは、除外範囲の追加や設定ができます。

除外範囲の設定

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品の実行時にこの範囲を除外するかどうかを選択します。 チェックボックスをオンにすると、動作中にこの範囲がスキャンや保護の対象から除外されます。 チェックボックスをオフにすると、動作中にこの範囲がスキャンや保護の対象に含まれます。チェックボックスをオンにすることにより、この範囲をスキャンや保護の対象から後で除外できます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	このドロップダウンリストでは、スキャンの除外に追加するディレクトリがあるファイルシステムの種別を選択できます： • **Local**：ローカルディレクトリ。 • **Mounted** - デバイスにマウントされるリモートディレクトリ。 • **リモートでマウント済みのすべての場所** - Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。
アクセスプロトコル	ドロップダウンリストからリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。 このドロップダウンリストは、ファイルシステムのドロップダウンリストから［**Mounted**］を選択した場合に使用できます。
パス	除外範囲に追加するディレクトリのパスの入力フィールドです。パスの指定にマスクおよびタグを使用できます。

特別なタグを使用してコンテナまたはイメージを指定できます：

- [container-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>]/<ローカルディレクトリへのパス>
- [image-id:<識別子>]/<ローカルディレクトリへのパス>
- [image-name:<名前>]/<ローカルディレクトリへのパス>

[container-id:<識別子>]、[container-name:<名前>]、[image-id:<識別子>]、および [image-name:<名前>]/<ローカルディレクトリ> タグの一意の組み合わせを使用することもできます。

1つのエリア内で1～4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。

例：

- [container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>

名前と識別子にはマスク（? および * 記号）を使用できます。

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」

アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。

マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。

マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。

ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。

「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。

このフィールドは、ファイルシステムのドロップダウンリストから［**Local**］を選択した場合に使用できます。

共有リソース名

除外範囲に追加するディレクトリがある、ファイルシステム共有リソースの名前を入力するためのフィールドです。

このフィールドは、［ファイルシステム］ドロップダウンリストで［**Mounted**］が選択され、［**アクセスプロトコル**］ドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。

マスク

このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。マスクは、［**パス**］フィールドに指定されたディレクトリ内のオブジェクトにのみ適用されます。

既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、スキャンからのオブジェクトの除外を設定できます。指定したマスクが名前に含まれるファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［脅威の名前による除外］ウィンドウ

脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。指定された脅威はブロックされません。既定では、脅威の名前のリストは空です。

脅威の名前は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した脅威が除外リストから削除されます。

このボタンは、少なくとも1つの脅威の名前をリストから選択している場合に使用できます。

表内の脅威の名前をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を編集できます。

［**追加**］をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を指定できます。

［プロセスによる除外］ウィンドウ

表には、プロセスによる除外の範囲が含まれています。プロセスによる除外の範囲では、指定されたプロセスの動作と、指定されたプロセスによって変更されたファイルをスキャンから除外できます。既定では、表にはネットワークエージェントへのパスを含む 2 つの除外範囲が含まれています。必要に応じてこれらの除外を削除できます。

プロセスによる除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	除外されるプロセスの絶対パス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

［信頼するプロセス］ウィンドウ

このウィンドウでは、プロセスによる除外範囲の追加や設定ができます。

除外範囲の設定

設定	説明
プロセスベースの除外範囲名	プロセスベースの除外範囲名を入力するフィールド。この名前は、［**プロセスによる除外**］ウィンドウの表に表示されます。 この入力フィールドを空白のままにすることはできません。
この除外を使用する / 使用しない	この切り替えボタンは、このスキャン範囲の除外をオンまたはオフにします。 この切り替えボタンは既定でオンになっています。
子プロセスへ	［**除外するプロセスのパス**］設定で指定した、除外されるプロセスの子プロセスを除外

適用する	します。 既定では、このチェックボックスはオフです。
除外するプロセスのパス	スキャンから除外するプロセスへの絶対パスです。
ファイルシステム、アクセスプロトコル、パス	この設定グループでは、プロセスによって変更されたファイルのスキャン除外を設定できます。 ファイルシステムのドロップダウンリストで、スキャンから除外するディレクトリのファイルシステムの種別を選択できます： • **Local**：ローカルディレクトリ。 • **Mounted**：マウントされたディレクトリ。 • **リモートでマウント済みのすべての場所** - Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。
アクセスプロトコル	ドロップダウンリストからリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。 ［**アクセスプロトコル**］ドロップダウンリストは、ファイルシステムのドロップダウンリストで［**Mounted**］の種別を選択した場合に使用できます。
パス	入力フィールドには、除外範囲に追加するディレクトリへのパスを入力できます。パスの指定にマスクを使用できます。

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」

アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。

マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。

マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。

ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。

このフィールドは、ファイルシステムのドロップダウンリストから［**Local**］を選択した場合に使用できます。

共有リソース名

除外範囲に追加するディレクトリがある、ファイルシステム共有リソースの名前を入力するためのフィールドです。

このフィールドは、［ファイルシステム］ドロップダウンリストで［**Mounted**］が選択され、［**アクセスプロトコル**］ドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。

マスク

このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。マスクは、［**ファイルシステム、アクセスプロトコル、パス**］ブロックで指定されたディレクトリ内のオブジェクトにのみ適用されます。

既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

管理コンソールでのファイル脅威対策の設定

管理コンソールでは、ポリシーのプロパティ内でファイル脅威対策を管理できます（**脅威対策 → ファイル脅威対策**）。

ファイル脅威対策の設定

設定	説明
ファイル脅威対策を有効にする	このチェックボックスでは、すべての管理対象デバイスでファイル脅威対策コンポーネントを有効にするかどうかを選択します。 既定では、このチェックボックスはオンです。
ファイル脅威対策の動作方法	ドロップダウンリストからファイル脅威対策コンポーネントの動作方法を選択できます： • **スマートチェック**（既定値）- ファイルが開かれた時にファイルをスキャンし、ファイルが変更された場合は閉じる時にもう一度スキャンします。ある処理によって一定期間の間にファイルが複数回アクセスおよび変更された場合は、処理によってファイルが最後に閉じられた時にのみ、もう一度スキャンが実行されます。 • **開いた時** - ファイルの読み込み、実行、変更のためにファイルが開かれた時にファイルをスキャンします。 • **開いた時と変更された時** - ファイルが開かれた時にファイルをスキャンし、ファイルが変更されている場合は閉じる時にもう一度スキャンします。
スキャン	この設定グループには、スキャン範囲とスキャン設定を指定できるウィンドウを開くボタンが含まれています。
脅威の検知時の処理	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**脅威の検知時の処理**］ウィンドウが表示され、検知された感染オブジェクトに対して実行する処理を設定できます。

［スキャン範囲］ウィンドウ

この表にはスキャン範囲が含まれます。表で指定されたパス内のファイルとディレクトリをすべてスキャンします。表には既定で、ローカルファイルシステムのすべてのディレクトリを対象とする1つのスキャン範囲が表示されています。

スキャン範囲設定

設定	説明
範囲名	スキャン範囲名。
パス	スキャンするディレクトリのパス。
ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、範囲の表の並び順でスキャンされます。必要に応じて、サブディレクトリを親ディレクトリよりもリストの上に配置し、親ディレクトリとは異なるセキュリティ設定をサブディレクトリに設定します。

［<新しいスキャン範囲>］ウィンドウ

このウィンドウでは、スキャン範囲の追加や設定ができます。

スキャン範囲設定

設定	説明

スキャン範囲名	スキャン範囲の名前を入力するフィールド。この名前は、［**スキャン範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品がこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、製品がこのスキャン範囲を処理します。 このチェックボックスをオフにすると、製品がこのスキャン範囲を処理しません。このチェックボックスをオンにすることにより、後からこの範囲をコンポーネント設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	これらの設定では、スキャン範囲を設定できます。 ファイルシステムのドロップダウンリストで、ファイルシステムの種別を選択できます： • **Local**（既定値）：ローカルディレクトリ。この項目を選択する場合は、ローカルディレクトリのパスを指定する必要があります。 • **Mounted** – マウントされたリモートまたはローカルのディレクトリ。この項目を選択する場合は、ファイルシステムのプロトコルまたは名前を指定する必要があります。 • **Shared** – Samba または NFS プロトコルでアクセス可能な保護されているサーバーファイルシステムリソースを表示します。 • **リモートでマウント済みのすべての場所** – Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。 • **共有済みのすべての場所** – Samba および NFS プロトコルでアクセス可能なすべての保護されているサーバーファイルシステムリソース。
	ファイルシステムのドロップダウンリストで **Shared** または **Mounted** を選択した場合は、右側のドロップダウンリストでリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。
	ファイルシステムのドロップダウンリストで **Local** を選択した場合は、スキャン範囲に追加するディレクトリのパスを入力フィールドに入力できます。パスの指定にマスクおよびタグを使用できます。

特別なタグを使用してコンテナまたはイメージを指定できます：

- [container-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>]/<ローカルディレクトリへのパス>
- [image-id:<識別子>]/<ローカルディレクトリへのパス>
- [image-name:<名前>]/<ローカルディレクトリへのパス>

[container-id:<識別子>]、[container-name:<名前>]、[image-id:<識別子>]、および [image-name:<名前>]/<ローカルディレクトリ> タグの一意の組み合わせを使用することもできます。

1つのエリア内で1～4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。

例：

- [container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>

名前と識別子にはマスク（? および * 記号）を使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリをスキャンします。 ファイルシステムのドロップダウンリストから［**Local**］が選択され、パスが指定されていない場合、ローカルファイルシステムのすべてのディレクトリがスキャンされます。
ファイルシステム名	スキャン範囲に追加するディレクトリがあるファイルシステムの名前を入力するためのフィールドです。 このフィールドは、ファイルシステムのドロップダウンリストで［**Mounted**］が選択され、右側のドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。
マスク	このリストには、動作中に製品がスキャンするオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［スキャンの設定］ウィンドウ

このウィンドウでは、ファイル脅威対策が有効になっている時にファイルスキャンを設定できます。

設定	説明
アーカイブをスキャン	このチェックボックスでは、アーカイブをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、アーカイブがスキャンされます。 アーカイブをスキャンするには、アーカイブを解凍する必要があるためスキャン速度が遅くなる可能性があります。［**スキャンの全般設定**］セクションの［**スキャン時間が次を超えたらファイルをスキップする（秒）**］および［**ファイルのサイズが次を超えたらスキップする（MB）**］を有効にして設定することで、アーカイブのスキャンの所要時間を短縮することができます。 このチェックボックスをオフにすると、アーカイブはスキャンされません。 既定では、このチェックボックスはオフです。
SFX アーカイブをスキャン	このチェックボックスでは、*自己解凍アーカイブ*をスキャンするかどうかを選択します。自己解凍アーカイブとは、実行可能な展開モジュールを含むアーカイブです。 このチェックボックスをオンにすると、自己解凍アーカイブがスキャンされます。 このチェックボックスをオフにすると、自己解凍アーカイブはスキャンされません。 このチェックボックスは、［**アーカイブをスキャン**］がオフの場合に使用できます。 既定では、このチェックボックスはオフです。
メールデータベースをスキャン	このチェックボックスでは、Microsoft Outlook、Outlook Express などのメールアプリケーションのメールデータベースをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、メールデータベースがスキャンされます。 このチェックボックスをオフにすると、メールデータベースはスキャンされません。 既定では、このチェックボックスはオフです。
メール形式のファイルをスキャン	このチェックボックスでは、プレーンテキストのメールメッセージのファイルをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、プレーンテキストのメッセージがスキャンされます。 このチェックボックスをオフにすると、プレーンテキストのメッセージはスキャンされません。 既定では、このチェックボックスはオフです。
テキストファイルをスキップ	テキスト形式のファイルをスキャンから一時的に除外します。 このチェックボックスをオンにすると、最後のスキャンから 10 分以内にテキストファイルが同じプロセスで再利用される場合は、テキストファイルはスキャンされません。この設定により、製品ログのスキャンを最適化できます。 このチェックボックスをオフにすると、テキストファイルがスキャンされます。 既定では、このチェックボックスはオフです。
スキャン時間が次を超えたらファイルをスキップする（秒）	このフィールドでは、ファイルをスキャンする最大時間を秒単位で指定できます。指定した時間が経過した後、Kaspersky Endpoint Security はファイルのスキャンを停止します。 使用できる値：0 ～ 9999。値が 0 に設定されると、スキャン時間は制限されません。 既定値：60
ファイルのサイズが次を超えたらスキップする（MB）	このフィールドでは、スキャンするファイルの最大サイズをメガバイト単位で指定できます。 使用できる値：0 ～ 999999。値が 0 に設定されると、Kaspersky Endpoint Security はサイズにかかわらず、すべてのファイルをスキャンします。 既定値：0
感染してい	このチェックボックスでは、*ObjectProcessed* タイプのイベントをログに記録するかどう

ないオブジェクトを記録する	かを選択します。 このチェックボックスをオンにすると、スキャンされたすべてのオブジェクトの *ObjectProcessed* タイプのイベントをログに記録します。 このチェックボックスをオフにすると、Kaspersky Endpoint Security は、［*ObjectProcessed*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
処理されていないオブジェクトを記録する	このチェックボックスでは、スキャン中にファイルを処理できない場合、*ObjectNotProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、*ObjectNotProcessed* タイプのイベントをログに記録します。 このチェックボックスをオフにすると、*ObjectNotProcessed* タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
圧縮されたオブジェクトを記録する	このチェックボックスでは、検出されたすべての圧縮されたオブジェクトに関する *PackedObjectDetected* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、*PackedObjectDetected* タイプのイベントをログに記録します。 このチェックボックスをオフにすると、*PackedObjectDetected* タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
iChecker 技術を使用する	このチェックボックスでは、前回のファイルのスキャン以降の新しいファイルおよび変更されたファイルのみをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、前回のスキャン以降の新しいファイルおよび変更されたファイルのみがスキャンされます。 このチェックボックスをオフにすると、作成日または変更日に関係なくファイルがスキャンされます。 既定では、このチェックボックスはオンです。
ヒューリスティック分析を使用する	このチェックボックスでは、ファイルのスキャン中にヒューリスティック分析を使用するかどうかを選択します。 既定では、このチェックボックスはオンです。
ヒューリスティック分析のレベル	［**ヒューリスティック分析を使用する**］をオンにすると、ドロップダウンリストでヒューリスティック分析レベルを選択できます。 • **低**：スキャンの詳細レベルが最も低く、システム負荷は最小です。 • **中**：スキャンの詳細レベルは中程度で、システム負荷のバランスが取れています。 • **高**：スキャンの詳細レベルが最も高く、システム負荷は最大です。 • **推奨**（既定値）：カスペルスキーが推奨する、最適なレベルです。保護品質と保護対象デバイスの性能への影響の最適な組み合わせを保証します。

［脅威の検知時の処理］ウィンドウ

このウィンドウでは、検知された感染オブジェクトに対して実行する処理を設定できます：

設定	説明
最初の処理	このドロップダウンリストでは、感染したオブジェクトの検知時に実行する最初の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています（既定値）。 • **ブロック**：オブジェクトへのアクセスをブロックします。
次の処理	このドロップダウンリストでは、感染したオブジェクトに対する最初の処理が成功しなかった場合に実行する次の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています。 • **ブロック**：オブジェクトへのアクセスをブロックします（既定値）。

ファイル脅威対策の除外

*保護除外*とは、Kaspersky Endpoint Security がオブジェクトをスキャンしてウイルスやその他のマルウェアを検知しない一連の条件です。マスクと脅威名でオブジェクトを除外し、プロセスの除外を設定することもできます。

管理コンソールでは、ポリシーのプロパティ内でファイル脅威対策の除外を設定できます（**脅威対策 → ファイル脅威対策の除外**）。

スキャンの除外の設定

設定のグループ	説明
除外	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**除外範囲**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する範囲のリストを指定できます。
マスクによる除外	この設定グループには［**設定**］が含まれています。クリックすると、［**マスクによる除外**］ウィンドウが表示されます。このウィンドウでは、名前のマスクにより、スキャンからのオブジェクトの除外を設定できます。
脅威の名前に	この設定グループには［**設定**］が含まれています。クリックすると、［**脅威の名前による除外**］ウィンドウが表示されます。このウィンドウでは、脅威の名前に基づいて、スキャンから

よる除外	のオブジェクトの除外を設定できます。
プロセスによる除外	この設定グループには**設定**が含まれています。クリックすると、**プロセスによる除外**ウィンドウが表示されます。このウィンドウで、プロセスの動作を除外できます。

［除外範囲］ウィンドウ

この表には、スキャンの除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	スキャンから除外されるディレクトリのパス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［<新しい除外範囲>］ウィンドウ

このウィンドウでは、スキャンの除外範囲の追加や設定ができます。

除外範囲の設定

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品の実行時にこの範囲をスキャンから除外するかどうかを選択します。 チェックボックスをオンにすると、スキャン中にこの範囲が除外されます。 このチェックボックスをオフにすると、この範囲がスキャン範囲に含まれます。このチェックボックスをオンにすることにより、後からこの範囲を除外することができます。 既定では、このチェックボックスはオンです。

ファイルシステム、アクセスプロトコル、パス	これらの設定では、除外範囲を設定できます。 ファイルシステムのドロップダウンリストで、スキャンから除外するディレクトリのファイルシステムの種別を選択できます： • **Local**：ローカルディレクトリ。 • **Mounted**：マウントされたディレクトリ。 • **リモートでマウント済みのすべての場所** - Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。
	ファイルシステムのドロップダウンリストで **Mounted** を選択した場合は、右側のドロップダウンリストでリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。
	ファイルシステムのドロップダウンリストで **Local** を選択した場合は、除外範囲に追加するディレクトリのパスを入力フィールドに入力できます。パスの指定にマスクおよびタグを使用できます。

特別なタグを使用してコンテナまたはイメージを指定できます：

- [container-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>]/<ローカルディレクトリへのパス>
- [image-id:<識別子>]/<ローカルディレクトリへのパス>
- [image-name:<名前>]/<ローカルディレクトリへのパス>

[container-id:<識別子>]、[container-name:<名前>]、[image-id:<識別子>]、および [image-name:<名前>]/<ローカルディレクトリ> タグの一意の組み合わせを使用することもできます。

1つのエリア内で1～4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。

例：

- [container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>

名前と識別子にはマスク（? および * 記号）を使用できます。

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」

アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。

マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。

マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。

ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。

「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。

ファイルシステム名

除外範囲に追加するディレクトリがあるファイルシステムの名前を入力するためのフィールドです。

このフィールドは、ファイルシステムのドロップダウンリストで［**Mounted**］が選択され、右側のドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。

マスク

このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。マスクは、［パス］フィールドに指定されたディレクトリ内のオブジェクトにのみ適用されます。

既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも 1 つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「*.txt」というマスクはすべてのテキストファイルを表します。
「*_my_file_??.html」というマスクは、任意の文字列から始まって、ファイル名の末尾が「_my_file_」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、スキャンからのオブジェクトの除外を設定できます。指定したマスクが名前に含まれるファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「*.txt」というマスクはすべてのテキストファイルを表します。
「*_my_file_??.html」というマスクは、任意の文字列から始まって、ファイル名の末尾が「_my_file_」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［脅威の名前による除外］ウィンドウ

脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。指定された脅威はブロックされません。既定では、脅威の名前のリストは空です。

脅威の名前は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した脅威が除外リストから削除されます。

このボタンは、少なくとも1つの脅威の名前をリストから選択している場合に使用できます。

表内の脅威の名前をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を編集できます。

［**追加**］をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を指定できます。

［プロセスによる除外］ウィンドウ

表には、プロセスによる除外の範囲が含まれています。プロセスによる除外の範囲では、指定されたプロセスの動作と、指定されたプロセスによって変更されたファイルをスキャンから除外できます。既定では、表にはネットワークエージェントへのパスを含む 2 つの除外範囲が含まれています。必要に応じてこれらの除外を削除できます。

プロセスによる除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	除外されるプロセスの絶対パス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

また、［**詳細設定**］->［**インポート**］をクリックしてファイルから除外リストをインポートしたり、［**詳細設定**］->［**選択項目をエクスポート**］または［**詳細設定**］->［**すべてエクスポート**］をクリックして追加した除外リストをファイルにエクスポートすることもできます。

［信頼するプロセス］ウィンドウ

このウィンドウでは、プロセスによる除外範囲の追加や設定ができます。

プロセスによる除外範囲の設定

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**プロセスによる除外**］ウィンドウの表に表示されます。 この入力フィールドを空白のままにすることはできません。
除外するプロ	スキャンから除外するプロセスへの絶対パスです。

セスのパス	
子プロセスへ適用する	［**除外するプロセスのパス**］設定で指定した、除外されるプロセスの子プロセスを除外します。 既定では、このチェックボックスはオフです。
この範囲を使用する	このチェックボックスでは、この除外範囲をオンまたはオフにします。 チェックボックスをオンにすると、スキャン中にこの範囲が除外されます。 このチェックボックスをオフにすると、この範囲がスキャン範囲に含まれます。このチェックボックスをオンにすることにより、後からこの範囲を除外することができます。 既定では、このチェックボックスはオンです。
変更されたファイルのパス	この設定グループでは、プロセスによって変更されたファイルのスキャン除外を設定できます。 ファイルシステムのドロップダウンリストで、スキャンから除外するディレクトリのファイルシステムの種別を選択できます： • **Local**：ローカルディレクトリ。この項目を選択する場合は、ローカルディレクトリのパスを指定する必要があります。 • **Mounted** – マウントされたリモートまたはローカルのディレクトリ。この項目を選択する場合は、ファイルシステムのプロトコルまたは名前を指定する必要があります。 • **Shared** – Samba または NFS プロトコルでアクセス可能な保護されているサーバーファイルシステムリソースを表示します。 • **リモートでマウント済みのすべての場所** – Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。 • **共有済みのすべての場所** – Samba および NFS プロトコルでアクセス可能なすべての保護されているサーバーファイルシステムリソース。
	ファイルシステムのドロップダウンリストで **Mounted** または **Shared** を選択した場合は、アクセスプロトコルのドロップダウンリストでリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。
	ファイルシステムのドロップダウンリストで **Local** を選択した場合は、除外範囲に追加するディレクトリのパスを入力フィールドに入力できます。パスの指定にマスクを使用できます。この入力フィールドを空白のままにすることはできません。

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」

アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。

マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。

マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。

ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。

ファイルシステム名

除外範囲に追加するディレクトリがあるファイルシステムの名前を入力するためのフィールドです。

このフィールドは、ファイルシステムのドロップダウンリストで［**Mounted**］が選択され、右側のドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。

マスク

このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。マスクは、［**変更されたファイルのパス**］フィールドに指定されたディレクトリ内のオブジェクトにのみ適用されます。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも 1 つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

コマンドラインでのファイル脅威対策の設定

コマンドラインでは、ファイル脅威対策の事前定義済みタスク（*File_Threat_Protection*）を使用してファイル脅威対策を管理できます。

ファイル脅威対策タスクは既定で開始されます。このタスクは、手動で開始および停止できます。

ファイル脅威対策タスクをコマンドラインから開始または停止するには、Administrator ロール権限が必要です。

ファイル脅威対策の設定は、ファイル脅威対策の事前定義済みタスクの設定を編集することで構成できます。

ファイル脅威対策タスクの設定

この表では、ファイル脅威対策タスクで指定できるすべての設定と、その設定で使用可能なすべての値と既定値を説明します。

ファイル脅威対策タスクの設定

設定	説明	
`ScanArchived`	アーカイブ（自己解凍型アーカイブを含む）のスキャンを指定します。 アプリケーションは次のアーカイブをスキャンします：.zip、.7z*、.7-z、.rar、.iso、.cab、.jar、.bz、.bz2、.tbz、.tbz2、.gz、.tgz、.arj。サポートされているアーカイブ形式のリストは、使用されている製品データベースによって異なります。	`Yes` – `FirstA` れてい て、感 アーカ `No`（既 ません。
`ScanSfxArchived`	自己解凍型アーカイブ（実行可能な解凍モジュールを含むアーカイブ）のみのスキャンを指定します。	`Yes` – ます。 `No`（既 スキャ
`ScanMailBases`	Microsoft Outlook®、Outlook Express、およびその他のメールクライアントのメールデータベースのスキャンを指定します。	`Yes` – キャン

		No（既 ファイル
ScanPlainMail	プレーンテキストのメールメッセージのスキャンを指定します。	Yes – ジをス No（既 ルメッ
SkipPlainTextFiles	テキスト形式のファイルをスキャンから一時的に除外します。 この設定の値が SkipPlainTextFiles=Yes の場合、最後のスキャンから 10 分以内にテキストファイルが同じプロセスで再利用されると、テキストファイルはスキャンされません。この設定により、製品ログのスキャンを最適化できます。	Yes – 最 ストフ た場合 ません。 No（既 ファイ
SizeLimit	スキャン対象のオブジェクトの最大サイズ（メガバイト単位）。指定された値よりもスキャン対象のオブジェクトのサイズが大きい場合、オブジェクトはスキップされます。	0 ～ 99 0 – スキ 無制限 既定値
TimeLimit	オブジェクトの最大スキャン時間（秒単位）。 この設定で指定された時間よりもスキャンの時間がかかる場合、そのオブジェクトのスキャンが停止されます。	0～999 0 - オフ です。 既定値
FirstAction	感染したオブジェクトに対して実行される最初の処理の選択。	Disinf し、そ す。駆除 別または 除できな 更されな ［Disi ［Seco 処理を指 Remove アップ を削除 Recomm オブジ 報に基 に選択 の木馬 Security イの木 なく、 Block スをブ トに関 既定値
SecondAction	感染したオブジェクトに対して実行される次の処理の選択。最初の処理に失敗した場合に、次の処理を実行します。	Second FirstA

		Block 選択さ はあり つの処 指定し 適用さ 既定値
UseExcludeMasks	**ExcludeMasks.item_#** 設定で指定されたオブジェクトのスキャン除外を有効にします。	**Yes** – E された ます。 **No**（既 定で指 ら除外
ExcludeMasks.item_#	名前またはマスクにより、オブジェクトをスキャンから除外します。 この設定を使用すると、指定されたスキャン範囲から名前によって個別のファイルを除外したり、シェル形式でマスクを使用して複数のファイルを除外したりできます。	既定値 例： UseE Excl Excl
UseExcludeThreats	**ExcludeThreats.item_#** 設定で指定された脅威を含むオブジェクトのスキャン除外を有効にします。	**Yes** – E 定され ンから **No**（既 設定で をスキ
ExcludeThreats.item_#	オブジェクト内で検知された脅威の名前によってスキャンからオブジェクトを除外します。この設定の値を指定する前に、**UseExcludeThreats** 設定が有効になっていることを確認します。 スキャンから単一オブジェクトを除外するには、このオブジェクト内で検知された脅威の完全な名前（このオブジェクトが感染していると判定した際に使用された名前の文字列）を指定します。 たとえば、ネットワークに関する情報を収集するユーティリティを使用している場合があります。これをブロックしないようにするには、スキャンから除外される脅威のリストに、製品で使用される脅威の完全な名前を追加します。 オブジェクトで検知された脅威のフルネームは、アプリケーションログや https://threats.kaspersky.com の Web サイトで確認することができます。	設定値 す。 既定値 例： UseE Excl Test Excl roja
ReportCleanObjects	感染していないとレポートされたスキャン済みオブジェクトに関する情報のログへの記録を指定します。 この設定は、たとえば特定のオブジェクトがスキャン済みであることを確認するために有効にします。	**Yes** – 感 る情報 **No**（既 クトに
ReportPackedObjects	複合オブジェクトの一部を構成するスキャン済みオブジェクトに関する情報のログへの記録を指定します。 この設定は、たとえばアーカイブ内のオブジェクトがスキャン済みであることを確認するために有効にします。	**Yes** – ェクト **No**（既 済みオ 録しま
ReportUnprocessedObjects	何らかの理由により処理されていないオブジェクトに関する情	**Yes** – 処

	報のログへの記録を指定します。	する情 No（既 ェクトに ん。
UseAnalyzer	ヒューリスティック分析を指定します。 ヒューリスティック分析により、新しい脅威がウイルスアナリストに知られるようになる前に検知することができます。	Yes（既 を有効に No – ヒ ます。
HeuristicLevel	ヒューリスティック分析のレベルを指定します。 ヒューリスティック分析レベルは、脅威の検索範囲とオペレーティングシステムのリソースに対する負荷およびスキャンの所要時間のバランスを設定します。ヒューリスティック分析レベルが高いほど、スキャンに必要なリソースと時間が増加します。	Light い、シ Medium レベル が取れ Deep – ステム Recomm
UseIChecker	iChecker 技術の使用を指定します。	Yes（既 効にし No – iC す。
ScanByAccessType	ファイル脅威対策タスクの操作モード。ScanByAccessType の設定は、ファイル脅威対策タスクにのみ適用されます。	SmartC れた時 が変更 キャン クトが 変更さ クトが ンが再 OpenAn にファ されて ャンし Open – のため をスキ
[ScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	スキャン範囲の説明。スキャン範囲に関する詳細情報を含みます。 この設定を使用して指定される文字列の最大長は 4096 文字です。	既定値 例： Area data
UseScanArea	指定された範囲のスキャンを指定します。タスクを実行するには、少なくとも 1 つの範囲のスキャンを有効にします。	Yes（既 ンしま No – 指 ん。
AreaMask.item_#	スキャン範囲の制限。スキャン範囲では、シェル形式のマスクを使用して指定したファイルのみをスキャンします。	既定値 ャン） 例：

	この設定が指定されていない場合、スキャン範囲のすべてのオブジェクトがスキャンされます。この設定には、複数の値を指定できます。	`Area`
`Path`	スキャンされるオブジェクトがあるディレクトリのパス。	< ローカ れたデ ンしま を使用

特別
イメ

- [c
  一
- [c
  一
- [
  ル
- [
  ル

[con
[con
[ima
[ima
ィレ
せを

1つの
を任
リス
ませ

例：

- [c
  [i
  ル
- [c
  [i
  ル
- [
  id
  ク
- [c
  [c
  [i
  ル
- [c
  [i
  [c
  [i
  ル

名前
記号

		アス ファ スク ファ 「/」 文字 「*」 ます。 「/d 2つの ル名 「/」 列（C す。低 「/d アス 「** クト とえ 適切 ファ は、 示で Shared クセス リソー Shared てアク テムリ Mounte てデバ レクト Mounte してデ ィレク AllRem と NFS マウン トリを AllSha ロトコ スのす スキャ <ファ バイス ースを
[ExcludedFromScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	スキャンの除外範囲の説明。除外範囲に関する詳細情報を含み	既定値

	ます。	
UseScanArea	指定された範囲のスキャンの除外を指定します。	Yes（既 ます。 No – 指
AreaMask.item_#	スキャンの除外範囲の制限。除外範囲で、シェル形式のマスクを使用して指定したファイルのみをスキャンから除外します。 設定が指定されていない場合、除外範囲のオブジェクトはスキャンされません。この設定には、複数の値を指定できます。	既定値 ャンか
Path	除外するオブジェクトを含むディレクトリのパス。	< ローカ れたデ む）の ます。 用でき

特別
イメ

- [c
  一
- [c
  一
- [
  ル
- [
  ル

[con
[con
[ima
[ima
ィレ
せを

1つの
を任
リス
ませ

例：

- [c
  [i
  ル
- [c
  [i
  ル
- [
  id
  ク
- [c
  [c
  [i
  ル
- [c
  [i
  [c
  [i
  ル

名前
記号

		アスク ファイ スクネ ファイ 「/」 文字列 「*」 ます。 「/d 2 つの ル名ま 「/」 列（C す。低 「/d アスク 「** クト とえば 適切な ファイ は、フ 示でき
		Mounte てデバ ートデ す。 Mounte してデバ ィレク AllRem と NFS マウン トリを <ファイ イスの スをス
[ExcludedForProgram.item_#] セクションには、次の設定が含まれています：		
ProgramPath	除外するプロセスのパス。	<プロセ ーカル ンされ
ApplyToDescendants	ProgramPath 設定で指定された除外対象プロセスの子プロセスをスキャンから除外します。	Yes – 指 プロセス No（既 スキャ ンから除
AreaDesc	プロセスの除外範囲の説明。	既定値

UseExcludedForProgram	指定された範囲のスキャンの除外を指定します。	Yes（既 ます。 No – 指
AreaMask.item_#	プロセスの除外範囲の制限事項。プロセスの除外範囲で、シェル形式のマスクを使用して指定したファイルのみをスキャンから除外します。 この設定が指定されていない場合、プロセスの除外範囲内のすべてのオブジェクトが除外されます。この設定には、複数の値を指定できます。	既定値 ャンか
Path	プロセスにより変更されたファイルがあるディレクトリのパス。	< ロー れたデ ンから 使用で アス ファ スク ファ 「/」 文字 「*」 ます。 「/d 2 つ ル名 「/」 列（C す。 「/d アス 「** クト とえ 適切 ファ は、 示で Shared クセス リソー Shared アクセ ムリソ Mounte デバイ トディ す。

		Mounte してデ ィレク AllRem NFS プ ントさ をスキ AllSha ロトコ てのフ から除 < ファ バイス ースを

ネットワークディレクトリのスキャンの最適化

ファイル脅威対策タスクを最適化するには、ネットワークディレクトリからローカルディレクトリへコピーされる任意のファイルをスキャンから除外します。そのためには、ネットワークディレクトリからのコピーに使用するユーティリティ（例えば、cpユーティリティ）に対して、プロセスに基づく除外を設定します。

ネットワークディレクトリのスキャンからの除外を設定するには：

1. コマンドを使用して、ファイル脅威対策タスクの設定（*File_Threat_Protection*、ID:1）を設定情報ファイルに出力します：

   `kesl-control --get-settings 1 --file <設定情報ファイルの絶対パス> [--jason]`

2. 設定情報ファイルを開き、`[ExcludedForProgram.item_ #]` セクションを次の設定で追加します：

   - `ProgramPath` - 除外するプロセス、または除外するプロセスがあるディレクトリのパス。
   - `ApplyToDescendants`は、スキャンが除外プロセスの子プロセスを除外するかどうかを示すパラメータ（取り得る値：`Yes`または`No`）です。
   - `AreaDesc` - プロセスの除外範囲の説明。除外範囲に関する詳細情報を含みます。
   - `UseExcludedForProgram` は、タスク操作中に指定された範囲の除外を有効にします（取り得る値：`Yes` または `No`）。
   - `Path` - プロセスにより変更されたファイル、またはファイルがあるディレクトリのパス。
   - `AreaMask.item_#` - スキャン範囲から除外するファイルのファイル名マスク。ファイルの完全パスも指定可能です。

     例：

     ```
     [ExcludedForProgram.item_0000]
     ProgramPath=/usr/bin/cp
     ApplyToDescendants=No
     AreaDesc=
     UseExcludedForProgram=Yes
     Path=AllRemoteMounted
     AreaMask.item_0000=*
     ```

3. コマンドを実行します：

   `kesl-control --set-settings 1 --file <設定情報ファイルの絶対パス> [--json]`

   JSON形式の設定ファイルから設定をインポートする場合は、`--json` キーを指定します。ライセンスが指定されていない場合、設定は INI ファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

ネットワークディレクトリにあるファイルはスキャンされませんが、`cp` コマンド自体（上記の例の場合）とローカルファイルはスキャンされます。

シンボリックリンクとハードリンクのスキャンに関する特別な考慮事項

Kaspersky Endpoint Security では、ファイルへのシンボリックリンクとハードリンクをスキャンできます。

シンボリックリンクのスキャン

シンボリックリンクによって参照されるファイルがファイル脅威対策コンポーネントのスキャン範囲内にある場合にのみ、シンボリックリンクがスキャンされます。

シンボリックリンクによって参照されるファイルがファイル脅威対策コンポーネントのスキャン範囲内にない場合、このファイルはスキャンされません。ただし、ファイルに悪意のあるコードが含まれている場合、デバイスのセキュリティは危険な状態になります。

ハードリンクのスキャン

複数のハードリンクを持つファイルを処理する場合、製品はオブジェクトに指定されたアクションに応じたアクションを選択します：

- ［**推奨される処理を実行**］オプションが選択されている場合、オブジェクトで検知された脅威の危険度に関するデータ、およびその脅威を駆除できる可能性に関するデータに基づいて自動的に処理が選択され、オブジェクトに対して実行します。
- ［**削除**］処理が選択されている場合、処理中のハードリンクを削除します。このファイルに対するその他のハードリンクは処理されません。
- ［**駆除**］処理が選択されている場合、ソースファイルを駆除します。駆除できない場合は、ハードリンクを削除し、その削除されたハードリンクの名前でソースファイルのコピーを作成します。

バックアップ保管領域からハードリンクを持つファイルを復元する場合、バックアップ保管領域に移動されたハードリンクの名前でソースファイルのコピーを作成します。ソースファイルとその他のハードリンクの接続は復元されません。

マルウェアのスキャン

*マルウェアのスキャン*は、オンデマンドで実行されるデバイス上の1回限りの全体またはカスタムファイルスキャンです。複数のマルウェアのスキャンタスクを同時に実行することができます。

*マルウェアのスキャン（Scan_My_Computer）*事前定義済みタスクがアプリケーションに作成されます。このタスクを使用して、デバイス全体のスキャンを実行できます。完全スキャンでは、デバイスのローカルドライブ上にあるすべてのオブジェクトがスキャンされます。さらに、推奨されるセキュリティ設定を使用してSambaプロトコルおよびNFSプロトコルでアクセスされる、マウントおよび共有されたすべてのオブジェクトも同様にスキャンされます。

Kaspersky Security Centerでは、MMC管理プラグインまたはKaspersky Endpoint Security Web管理プラグインをインストールした後、Kaspersky Security Center初期設定ウィザードによってマルウェアのスキャンのグループタスクが自動的に作成されます。

完全スキャン中は、プロセッサがビジー状態になります。完全スキャンタスクはビジネスがアイドル状態の時に実行してください。

Kaspersky Security Centerおよびコマンドラインで自動的に作成されたタスクの設定を構成したり、マルウェアのスキャンのユーザータスクを作成したりできます。

マルウェアを検知すると、Kaspersky Endpoint Securityは感染したファイルを削除し、このファイルから開始したマルウェアのプロセスを終了させることができます。

マルウェアのスキャンタスクの実行中に、コントロールサービスによって、またはユーザーによって手動で本製品が再起動された場合、タスクは停止します。*OnDemandTaskInterrupted*イベントがログに記録されます。

マルウェアのスキャンタスクを実行し、スキャン設定を構成できます。

- スキャンするオペレーティングシステムオブジェクトを選択します：ファイル、アーカイブ、ブートセクター、プロセスメモリとカーネルメモリ、スタートアップオブジェクト。
- スキャンするオブジェクトのサイズとオブジェクトのスキャン時間を制限します。
- 感染したオブジェクトに対して実行される処理を選択します。
- スキャンからのオブジェクトの除外を設定します：
  - 名前またはマスクに基づく
  - オブジェクトで検知された脅威の名前に基づく
- スキャン時にグローバル除外とファイル脅威対策除外を有効または無効にします。
- スキャンされた非感染オブジェクト、アーカイブ内のスキャンオブジェクト、および未処理のオブジェクトに関する情報のログ記録を有効にします。
- スキャン中のヒューリスティック分析とiCheckerテクノロジーの使用を設定します。
- ブートセクターをスキャンする必要がある一連のデバイスを制限します。
- スキャン範囲とスキャン除外範囲を設定します。

Web コンソールでのマルウェアのスキャン

Web コンソールでは、 *マルウェアのスキャンタスク*を使用してマルウェアをスキャンできます。

自動的に作成されたグループタスクを実行したり、スキャン用のユーザータスクを作成して実行することもできます。マルウェアのスキャンタスクの設定を編集することで、スキャン設定を構成できます。

マルウェアのスキャンタスクの設定

設定	説明
アーカイブをスキャン	このチェックボックスでは、アーカイブをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、アーカイブがスキャンされます。 アーカイブをスキャンするには、アーカイブを解凍する必要があるためスキャン速度が遅くなる可能性があります。［**スキャンの全般設定**］セクションの［**スキャン時間が次を超えたらファイルをスキップする（秒）**］および［**ファイルのサイズが次を超えたらスキップする（MB）**］を設定すると、アーカイブのスキャンの所要時間を減らすことができます。 このチェックボックスをオフにすると、アーカイブはスキャンされません。 既定では、このチェックボックスはオンです。
SFX アーカイブをスキャン	このチェックボックスでは、*自己解凍アーカイブ*をスキャンするかどうかを選択します。自己解凍アーカイブとは、実行可能な展開モジュールを含むアーカイブです。 このチェックボックスをオンにすると、自己解凍アーカイブがスキャンされます。 このチェックボックスをオフにすると、自己解凍アーカイブはスキャンされません。 このチェックボックスは、［**アーカイブをスキャン**］がオフの場合に使用できます。 既定では、このチェックボックスはオンです。
メールデータベースをスキャン	このチェックボックスでは、Microsoft Outlook、Outlook Express などのメールアプリケーションのメールデータベースをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、メールデータベースはスキャンされます。 このチェックボックスをオフにすると、メールデータベースはスキャンされません。 既定では、このチェックボックスはオフです。
メール形式のファイルをスキャン	このチェックボックスでは、プレーンテキストのメールメッセージのファイルをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、プレーンテキストのメッセージがスキャンされます。 このチェックボックスをオフにすると、プレーンテキストのメッセージはスキャンされません。 既定では、このチェックボックスはオフです。
スキャン時間が次を超えたらファイルをスキップする（秒）	このフィールドでは、ファイルをスキャンする最大時間を秒単位で指定できます。指定した時間が経過した後、ファイルのスキャンは停止されます。 使用できる値：0 ～ 9999。値が 0 に設定されると、スキャン時間は制限されません。 既定値：0
ファイルのサイズが次を超えたらスキップする（MB）	このフィールドでは、スキャンするファイルの最大サイズをメガバイト単位で指定できます。 使用できる値：0 ～ 999999。値が 0 に設定されると、サイズにかかわらず、すべてのファイルがスキャンされます。

	既定値：0
感染していないオブジェクトを記録する	このチェックボックスでは、*ObjectProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、スキャンされたすべてのオブジェクトの *ObjectProcessed* タイプのイベントをログに記録します。 このチェックボックスをオフにすると、スキャンされたオブジェクトの *ObjectProcessed* タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
処理されていないオブジェクトを記録する	このチェックボックスでは、スキャン中にファイルを処理できない場合、*ObjectNotProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、［*ObjectNotProcessed*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*ObjectNotProcessed*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
圧縮されたオブジェクトを記録する	このチェックボックスでは、検出されたすべての圧縮されたオブジェクトに関する *PackedObjectDetected* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、［*PackedObjectDetected*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*PackedObjectDetected*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
iChecker 技術を使用する	このチェックボックスでは、前回のファイルのスキャン以降の新しいファイルおよび変更されたファイルのみをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、前回のスキャン以降の新しいファイルおよび変更されたファイルのみがスキャンされます。 このチェックボックスをオフにすると、作成日または変更日に関係なくファイルがスキャンされます。 既定では、このチェックボックスはオンです。
ヒューリスティック分析を使用する	このチェックボックスでは、ファイルのスキャン中にヒューリスティック分析を使用するかどうかを選択します。 既定では、このチェックボックスはオンです。
ヒューリスティック分析のレベル	［**ヒューリスティック分析を使用する**］をオンにすると、ドロップダウンリストでヒューリスティック分析レベルを選択できます。 • **低**：スキャンの詳細レベルが最も低く、システム負荷は最小です。 • **中**：スキャンの詳細レベルは中程度で、システム負荷のバランスが取れています。 • **高**：スキャンの詳細レベルが最も高く、システム負荷は最大です。 • **推奨**（既定値）：カスペルスキーが推奨する、最適なレベルです。保護品質と保護対象デバイスの性能への影響の最適な組み合わせを保証します。
最初の処理	このドロップダウンリストでは、感染したオブジェクトの検知時に実行する最初の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。

	• **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています（既定値）。 • **スキップ**：オブジェクトをスキップします。
次の処理	このドロップダウンリストでは、感染したオブジェクトに対する最初の処理が成功しなかった場合に実行する次の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています。 • **スキップ**：オブジェクトをスキップします（既定値）。
スキャン範囲	タスクによってスキャンされた範囲を示す表。表には既定で、ローカルファイルシステムのすべてのディレクトリを対象とする1つのスキャン範囲が表示されています。 表内ではスキャン範囲に対して次の操作ができます：追加、設定、削除、上に移動、下に移動。 ［**下へ**］をクリックすると、表内で選択した項目が下に移動します。 指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。 このボタンは、1つの範囲を表から選択している場合に使用できます。 ［**上へ**］をクリックすると、表内で選択した項目が上に移動します。 指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。 このボタンは、1つの範囲を表から選択している場合に使用できます。 ［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。 このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

スキャン範囲名をクリックすると、［**<スキャン範囲>**］ウィンドウが表示されます。このウィンドウでは、選択したスキャン範囲の設定を編集できます。

［**追加**］をクリックすると、［**<新しいスキャン範囲>**］ウィンドウが表示されます。このウィンドウでは、新しいスキャン範囲を指定できます。

［スキャン範囲の追加］ウィンドウ

このウィンドウでは、スキャン範囲の追加や設定ができます。

スキャン範囲設定

設定	説明
範囲名	スキャン範囲の名前を入力するフィールド。この名前は、**スキャン設定**セクションの**スキャン範囲**表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品がこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、製品がこのスキャン範囲を処理します。 このチェックボックスをオフにすると、製品がこのスキャン範囲を処理しません。このチェックボックスをオンにすることにより、後からこの範囲をコンポーネント設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	ドロップダウンリストからファイルシステムの種別を選択できます： • **Local**（既定値）：ローカルディレクトリ。この項目を選択する場合は、ローカルディレクトリのパスを指定する必要があります。 • **Mounted** – マウントされたリモートまたはローカルのディレクトリ。この項目を選択する場合は、ファイルシステムのプロトコルまたは名前を指定する必要があります。 • **Shared** – Samba または NFS プロトコルでアクセス可能な保護されているサーバーファイルシステムリソースを表示します。 • **リモートでマウント済みのすべての場所** – Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。 • **共有済みのすべての場所** – Samba および NFS プロトコルでアクセス可能なすべての保護されているサーバーファイルシステムリソース。
アクセスプロトコル	ドロップダウンリストからリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。

	• **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。 このドロップダウンリストは、ファイルシステムのドロップダウンリストから［**Shared**］または［**Mounted**］を選択した場合に使用できます。
パス	これは、スキャン範囲に含めるディレクトリのパスを指定するための入力フィールドです。パスの指定にマスクおよびタグを使用できます。 特別なタグを使用してコンテナまたはイメージを指定できます： • `[container-id:<識別子>]/<ローカルディレクトリへのパス>` • `[container-name:<名前>]/<ローカルディレクトリへのパス>` • `[image-id:<識別子>]/<ローカルディレクトリへのパス>` • `[image-name:<名前>]/<ローカルディレクトリへのパス>` `[container-id:<識別子>]`、`[container-name:<名前>]`、`[image-id:<識別子>]`、および `[image-name:<名前>]/<ローカルディレクトリ>` タグの一意の組み合わせを使用することもできます。 1つのエリア内で1〜4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。 例： • `[container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>` • `[container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>` • `[image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>` • `[container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>` • `[container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>` 名前と識別子にはマスク（`?` および `*` 記号）を使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリをスキャンします。 このフィールドは、ファイルシステムのドロップダウンリストから［**Local**］を選択した場合に使用できます。 ファイルシステムのドロップダウンリストから［**Local**］が選択され、パスが指定されていない場合、ローカルファイルシステムのすべてのディレクトリがスキャンされます。
共有リソース名	スキャン範囲に追加するディレクトリがある、ファイルシステム共有リソースの名前を入力するためのフィールドです。 このフィールドは、［ファイルシステム］ドロップダウンリストで［**Mounted**］が選択され、［**アクセスプロトコル**］ドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。
マスク	このリストには、動作中に製品がスキャンするオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［スキャン範囲］ウィンドウ

マルウェアのスキャンタスクのスキャン範囲を設定できます。ファイル、ブートセクター、クライアントデバイスのメモリ、スタートアップオブジェクトをスキャンできます。

マルウェアのスキャン範囲タスクの設定

設定	説明
ファイルをスキャン	このチェックボックスでは、ファイルスキャンを有効にするかどうかを選択します。 このチェックボックスをオンにすると、ファイルがスキャンされます。 このチェックボックスをオフにすると、ファイルはスキャンされません。 既定では、このチェックボックスはオンです。
ブートセクターをスキャン	このチェックボックスでは、ブートセクターをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、ブートセクターがスキャンされます。 このチェックボックスをオフにすると、ブートセクターはスキャンされません。 既定では、このチェックボックスはオフです。
カーネルメモリおよび実行中処理のスキャン	このチェックボックスでは、クライアントデバイスのメモリをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、カーネルメモリと実行中のプロセスがスキャンされます。 このチェックボックスをオフにすると、カーネルメモリと実行中のプロセスはスキャンされません。 既定では、このチェックボックスはオフです。
スタートアップオブジェクトをスキャン	このチェックボックスでは、スタートアップオブジェクトをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、スタートアップオブジェクトがスキャンされます。 このチェックボックスをオフにすると、スタートアップオブジェクトはスキャンされません。 既定では、このチェックボックスはオフです。
スキャン対象デバイス	［**デバイスマスクの設定**］をクリックすると［**スキャン範囲**］ウィンドウが表示され、ブートセクターをスキャンするデバイスを指定できます。

［スキャン範囲］ウィンドウ

この表には、スキャンする必要のあるブートセクターを持つデバイスの名前マスクが含まれています。既定では、すべてのデバイスを示すマスク「**/****」がリストに含まれています。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲］セクション

マルウェアのスキャンタスクの［**除外範囲**］セクションでは、除外範囲、マスクと脅威名による除外、およびタスク実行時のグローバル除外とファイル脅威対策除外の使用を設定できます。

スキャンの除外の設定

設定	説明
監視の除外範囲を設定する	［**除外リストを設定する**］をクリックすると、［**除外範囲**］ウィンドウが表示されます。このウィンドウでは、スキャンの除外のリストを定義できます。
除外をマスクで設定する	［**除外をマスクで設定する**］をクリックすると、［**マスクによる除外**］ウィンドウが表示されます。このウィンドウでは、名前のマスクにより、スキャンからのオブジェクトの除外を設定できます。
除外を脅威名で設定する	［**除外を脅威名で設定する**］をクリックすると、［**脅威の名前による除外**］ウィンドウが表示されます。このウィンドウでは、脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。
グローバル除外リストを使用	チェックボックスは、本製品の実行中にグローバル例外で指定されたマウントポイントの除外を有効または無効にします。 チェックボックスをオンにすると、設定されたマウントポイントをスキャンから除外します。 既定では、このチェックボックスはオンです。
ファイル脅威対策の除外リストを使用	このチェックボックスは、アプリケーションの実行時に設定されたファイル脅威対策の除外の使用を有効または無効にします。 チェックボックスをオンにすると、アプリケーションはファイル脅威対策コンポーネントの除外に指定されたオブジェクトをスキャンしません。 既定では、このチェックボックスはオンです。

［除外範囲］ウィンドウ

この表には、スキャンの除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	スキャンから除外されるディレクトリのパス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲の追加］ウィンドウ

このウィンドウでは、除外範囲の追加や設定ができます。

除外範囲の設定

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品の実行時にこの範囲を除外するかどうかを選択します。 チェックボックスをオンにすると、動作中にこの範囲がスキャンや保護の対象から除外されます。 チェックボックスをオフにすると、動作中にこの範囲がスキャンや保護の対象に含まれます。チェックボックスをオンにすることにより、この範囲をスキャンや保護の対象から後で除外できます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	このドロップダウンリストでは、スキャンの除外に追加するディレクトリがあるファイルシステムの種別を選択できます： • **Local**：ローカルディレクトリ。 • **Mounted** - デバイスにマウントされるリモートディレクトリ。 • **リモートでマウント済みのすべての場所** - Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。
アクセスプロトコル	ドロップダウンリストからリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。 このドロップダウンリストは、ファイルシステムのドロップダウンリストから［**Mounted**］を選択した場合に使用できます。

パス

除外範囲に追加するディレクトリのパスの入力フィールドです。パスの指定にマスクおよびタグを使用できます。

特別なタグを使用してコンテナまたはイメージを指定できます：

- [container-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>]/<ローカルディレクトリへのパス>
- [image-id:<識別子>]/<ローカルディレクトリへのパス>
- [image-name:<名前>]/<ローカルディレクトリへのパス>

[container-id:<識別子>]、[container-name:<名前>]、[image-id:<識別子>]、および [image-name:<名前>]/<ローカルディレクトリ> タグの一意の組み合わせを使用することもできます。

1つのエリア内で1～4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。

例：

- [container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>

名前と識別子にはマスク（? および * 記号）を使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。 マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。 ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。 このフィールドは、ファイルシステムのドロップダウンリストから［**Local**］を選択した場合に使用できます。
共有リソース名	除外範囲に追加するディレクトリがある、ファイルシステム共有リソースの名前を入力するためのフィールドです。 このフィールドは、［ファイルシステム］ドロップダウンリストで［**Mounted**］が選択され、［**アクセスプロトコル**］ドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。
マスク	このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。マスクは、［**パス**］フィールドに指定されたディレクトリ内のオブジェクトにのみ適用されます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。 このボタンは、少なくとも 1 つのファイルマスクをリストから選択している場合に使用できます。 マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、スキャンからのオブジェクトの除外を設定できます。指定したマスクが名前に含まれるファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［脅威の名前による除外］ウィンドウ

脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。指定された脅威はブロックされません。既定では、脅威の名前のリストは空です。

脅威の名前は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した脅威が除外リストから削除されます。

このボタンは、少なくとも1つの脅威の名前をリストから選択している場合に使用できます。

表内の脅威の名前をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を編集できます。

［**追加**］をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を指定できます。

管理コンソールでのマルウェアのスキャン

管理コンソールでは、*マルウェアのスキャン*タスクを使用してマルウェアをスキャンできます。

自動的に作成されたグループタスクを実行したり、スキャン用のユーザータスクを作成して実行することもできます。マルウェアのスキャンタスクの設定を編集することで、スキャン設定を構成できます。

マルウェアのスキャンタスクのプロパティの［**設定**］セクションでは、次の表に示す設定を構成できます。

マルウェアのスキャンタスクの設定

設定	説明
スキャン	この設定グループには、スキャン範囲、スキャン範囲設定、およびスキャン設定を指定できるウィンドウを開くボタンが含まれています。
脅威の検知時の処理	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**脅威の検知時の処理**］ウィンドウが表示され、検知された感染オブジェクトに対して実行する処理を設定できます。

マルウェアのスキャンタスクのプロパティの［**除外**］セクションでは、マスクと脅威名による除外範囲または除外を設定することもできます。

［スキャン範囲］ウィンドウ

この表にはスキャン範囲が含まれます。表で指定されたパス内のファイルとディレクトリをすべてスキャンします。表には既定で、ローカルファイルシステムのすべてのディレクトリを対象とする1つのスキャン範囲が表示されています。

スキャン範囲設定

設定	説明
範囲名	スキャン範囲名。
パス	スキャンするディレクトリのパス。
ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、範囲の表の並び順でスキャンされます。必要に応じて、サブディレクトリを親ディレクトリよりもリストの上に配置し、親ディレクトリとは異なるセキュリティ設定をサブディレクトリに設定します。

［<新しいスキャン範囲>］ウィンドウ

このウィンドウでは、スキャン範囲の追加や設定ができます。

スキャン範囲設定

設定	説明
スキャン範囲名	スキャン範囲の名前を入力するフィールド。この名前は、［**スキャン範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品がこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、製品がこのスキャン範囲を処理します。 このチェックボックスをオフにすると、製品がこのスキャン範囲を処理しません。このチェックボックスをオンにすることにより、後からこの範囲をコンポーネント設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステ	これらの設定では、スキャン範囲を設定できます。

ム、アクセスプロトコル、パス	ファイルシステムのドロップダウンリストで、ファイルシステムの種別を選択できます： • **Local**（既定値）：ローカルディレクトリ。この項目を選択する場合は、ローカルディレクトリのパスを指定する必要があります。 • **Mounted** – マウントされたリモートまたはローカルのディレクトリ。この項目を選択する場合は、ファイルシステムのプロトコルまたは名前を指定する必要があります。 • **Shared** – Samba または NFS プロトコルでアクセス可能な保護されているサーバーファイルシステムリソースを表示します。 • **リモートでマウント済みのすべての場所** – Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。 • **共有済みのすべての場所** – Samba および NFS プロトコルでアクセス可能なすべての保護されているサーバーファイルシステムリソース。
	ファイルシステムのドロップダウンリストで **Shared** または **Mounted** を選択した場合は、右側のドロップダウンリストでリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。
	ファイルシステムのドロップダウンリストで **Local** を選択した場合は、スキャン範囲に追加するディレクトリのパスを入力フィールドに入力できます。パスの指定にマスクおよびタグを使用できます。

特別なタグを使用してコンテナまたはイメージを指定できます：

- [container-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>]/<ローカルディレクトリへのパス>
- [image-id:<識別子>]/<ローカルディレクトリへのパス>
- [image-name:<名前>]/<ローカルディレクトリへのパス>

[container-id:<識別子>]、[container-name:<名前>]、[image-id:<識別子>]、および [image-name:<名前>]/<ローカルディレクトリ> タグの一意の組み合わせを使用することもできます。

1つのエリア内で1～4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。

例：

- [container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>

名前と識別子にはマスク（? および * 記号）を使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリをスキャンします。 ファイルシステムのドロップダウンリストから［**Local**］が選択され、パスが指定されていない場合、ローカルファイルシステムのすべてのディレクトリがスキャンされます。
ファイルシステム名	スキャン範囲に追加するディレクトリがあるファイルシステムの名前を入力するためのフィールドです。 このフィールドは、ファイルシステムのドロップダウンリストで［**Mounted**］が選択され、右側のドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。
マスク	このリストには、動作中に製品がスキャンするオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［スキャン範囲の設定］ウィンドウ

このウィンドウでは、マルウェアのスキャンタスクのファイルスキャンを設定します。ファイル、ブートセクター、デバイスのメモリ、スタートアップオブジェクトをスキャンできます。

スキャン範囲設定

設定	説明
ファイルをスキャン	このチェックボックスでは、ファイルスキャンを有効にするかどうかを選択します。 このチェックボックスをオンにすると、ファイルがスキャンされます。 このチェックボックスをオフにすると、ファイルはスキャンされません。 既定では、このチェックボックスはオンです。
ブートセクターをスキャン	このチェックボックスでは、ブートセクターをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、ブートセクターがスキャンされます。 このチェックボックスをオフにすると、ブートセクターはスキャンされません。 既定では、このチェックボックスはオフです。
カーネルメモリと実行中のプロセスをスキャンする	このチェックボックスでは、デバイスのメモリをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、カーネルメモリと実行中のプロセスがスキャンされます。 このチェックボックスをオフにすると、カーネルと実行中のプロセスはスキャンされません。 既定では、このチェックボックスはオフです。
スタートアップオブジェクトをスキャン	このチェックボックスでは、スタートアップオブジェクトをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、スタートアップオブジェクトがスキャンされます。 このチェックボックスをオフにすると、スタートアップオブジェクトはスキャンされません。 既定では、このチェックボックスはオフです。
スキャン対象デバイス	この設定グループには、**設定**が含まれています。このボタンをクリックすると［**スキャン範囲**］ウィンドウが表示され、ブートセクターをスキャンするデバイスを指定できます。
グローバル除外リストを使用	チェックボックスは、本製品の実行中にグローバル例外で指定されたマウントポイントの除外を有効または無効にします。 チェックボックスをオンにすると、設定されたマウントポイントをスキャンから除外します。 既定では、このチェックボックスはオンです。
ファイル脅威対策の除外リストを使用	このチェックボックスは、アプリケーションの実行時に設定されたファイル脅威対策の除外の使用を有効または無効にします。 チェックボックスをオンにすると、アプリケーションはファイル脅威対策コンポーネントの除外に指定されたオブジェクトをスキャンしません。 既定では、このチェックボックスはオンです。

［スキャン範囲］ウィンドウ

この表には、スキャンする必要のあるブートセクターを持つデバイスの名前マスクが含まれています。既定では、すべてのデバイスを示すマスク「**/****」がリストに含まれています。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［スキャンの設定］ウィンドウ

このウィンドウでは、タスクのファイルスキャンを設定します。

スキャン設定

設定	説明
アーカイブをスキャン	このチェックボックスでは、アーカイブをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、アーカイブがスキャンされます。 アーカイブをスキャンするには、アーカイブを解凍する必要があるためスキャン速度が遅くなる可能性があります。［**スキャンの全般設定**］セクションの［**スキャン時間が次を超えたらファイルをスキップする（秒）**］および［**ファイルのサイズが次を超えたらスキップする（MB）**］を設定すると、アーカイブのスキャンの所要時間を減らすことができます。 このチェックボックスをオフにすると、アーカイブはスキャンされません。 既定では、このチェックボックスはオンです。
SFX アーカイブをスキャン	このチェックボックスでは、*自己解凍アーカイブ*をスキャンするかどうかを選択します。自己解凍アーカイブとは、実行可能な展開モジュールを含むアーカイブです。 このチェックボックスをオンにすると、自己解凍アーカイブがスキャンされます。 このチェックボックスをオフにすると、自己解凍アーカイブはスキャンされません。 このチェックボックスは、［**アーカイブをスキャン**］がオフの場合に使用できます。 既定では、このチェックボックスはオンです。
メールデータベースをスキャン	このチェックボックスでは、Microsoft Outlook、Outlook Express などのメールアプリケーションのメールデータベースをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、メールデータベースはスキャンされます。 このチェックボックスをオフにすると、メールデータベースはスキャンされません。 既定では、このチェックボックスはオフです。
メール形式のファイルをスキャン	このチェックボックスでは、プレーンテキストのメールメッセージのファイルをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、プレーンテキストのメッセージがスキャンされます。

	このチェックボックスをオフにすると、プレーンテキストのメッセージはスキャンされません。 既定では、このチェックボックスはオフです。
スキャン時間が次を超えたらファイルをスキップする（秒）	このフィールドでは、ファイルをスキャンする最大時間を秒単位で指定できます。指定した時間が経過した後、ファイルのスキャンは停止されます。 使用できる値：0 ～ 9999。値が 0 に設定されると、スキャン時間は制限されません。 既定値：0
ファイルのサイズが次を超えたらスキップする（MB）	このフィールドでは、スキャンするファイルの最大サイズをメガバイト単位で指定できます。 使用できる値：0 ～ 999999。値が 0 に設定されると、サイズにかかわらず、すべてのファイルがスキャンされます。 既定値：0
感染していないオブジェクトを記録する	このチェックボックスでは、*ObjectProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、スキャンされたすべてのオブジェクトの *ObjectProcessed* タイプのイベントをログに記録します。 このチェックボックスをオフにすると、スキャンされたオブジェクトの *ObjectProcessed* タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
処理されていないオブジェクトを記録する	このチェックボックスでは、スキャン中にファイルを処理できない場合、*ObjectNotProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、［*ObjectNotProcessed*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*ObjectNotProcessed*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
圧縮されたオブジェクトを記録する	このチェックボックスでは、検出されたすべての圧縮されたオブジェクトに関する *PackedObjectDetected* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、［*PackedObjectDetected*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*PackedObjectDetected*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
iChecker 技術を使用する	このチェックボックスでは、前回のファイルのスキャン以降の新しいファイルおよび変更されたファイルのみをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、前回のスキャン以降の新しいファイルおよび変更されたファイルのみがスキャンされます。 このチェックボックスをオフにすると、作成日または変更日に関係なくファイルがスキャンされます。 既定では、このチェックボックスはオンです。
ヒューリスティック分析を使用する	このチェックボックスでは、ファイルのスキャン中にヒューリスティック分析を使用するかどうかを選択します。 既定では、このチェックボックスはオンです。
ヒューリスティック分	［**ヒューリスティック分析を使用する**］をオンにすると、ドロップダウンリストでヒューリスティック分析レベルを選択できます。

析のレベル	• **低**：スキャンの詳細レベルが最も低く、システム負荷は最小です。 • **中**：スキャンの詳細レベルは中程度で、システム負荷のバランスが取れています。 • **高**：スキャンの詳細レベルが最も高く、システム負荷は最大です。 • **推奨**（既定値）：カスペルスキーが推奨する、最適なレベルです。保護品質と保護対象デバイスの性能への影響の最適な組み合わせを保証します。

［脅威の検知時の処理］ウィンドウ

このウィンドウでは、検知された感染オブジェクトに対して実行する処理を設定できます：

脅威の検知時の処理

設定	説明
最初の処理	このドロップダウンリストでは、感染したオブジェクトの検知時に実行する最初の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています（既定値）。 • **スキップ**：オブジェクトをスキップします。
次の処理	このドロップダウンリストでは、感染したオブジェクトに対する最初の処理が成功しなかった場合に実行する次の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています。 • **スキップ**：オブジェクトをスキップします（既定値）。

除外セクション

［*スキャンの除外*］は一連の条件です。これらの条件を満たす場合、Kaspersky Endpoint Security はオブジェクトのウイルスやその他のマルウェアのスキャンを行いません。マスクと脅威の名前で指定することで、スキャンからオブジェクトを除外することもできます。

スキャンの除外の設定

設定のグループ	説明
除外範囲	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**除外範囲**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する範囲のリストを指定できます。
マスクによる除外	この設定グループには［**設定**］が含まれています。クリックすると、［**マスクによる除外**］ウィンドウが表示されます。このウィンドウでは、名前のマスクにより、スキャンからのオブジェクトの除外を設定できます。
脅威の名前による除外	この設定グループには［**設定**］が含まれています。クリックすると、［**脅威の名前による除外**］ウィンドウが表示されます。このウィンドウでは、脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。

［除外範囲］ウィンドウ

この表には、スキャンの除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	スキャンから除外されるディレクトリのパス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［<新しい除外範囲>］ウィンドウ

このウィンドウでは、スキャンの除外範囲の追加や設定ができます。

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品の実行時にこの範囲をスキャンから除外するかどうかを選択します。 チェックボックスをオンにすると、スキャン中にこの範囲が除外されます。 このチェックボックスをオフにすると、この範囲がスキャン範囲に含まれます。このチェックボックスをオンにすることにより、後からこの範囲を除外することができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	これらの設定では、除外範囲を設定できます。 ファイルシステムのドロップダウンリストで、スキャンから除外するディレクトリのファイルシステムの種別を選択できます： • **Local**：ローカルディレクトリ。 • **Mounted**：マウントされたディレクトリ。 • **リモートでマウント済みのすべての場所** - Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。
	ファイルシステムのドロップダウンリストで **Mounted** を選択した場合は、右側のドロップダウンリストでリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。
	ファイルシステムのドロップダウンリストで **Local** を選択した場合は、除外範囲に追加するディレクトリのパスを入力フィールドに入力できます。パスの指定にマスクおよびタグを使用できます。

特別なタグを使用してコンテナまたはイメージを指定できます：

- [container-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>]/<ローカルディレクトリへのパス>
- [image-id:<識別子>]/<ローカルディレクトリへのパス>
- [image-name:<名前>]/<ローカルディレクトリへのパス>

[container-id:<識別子>]、[container-name:<名前>]、[image-id:<識別子>]、および [image-name:<名前>]/<ローカルディレクトリ> タグの一意の組み合わせを使用することもできます。

1つのエリア内で1～4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。

例：

- [container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>

名前と識別子にはマスク（? および * 記号）を使用できます。

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」

アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。

マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。

マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。

ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。

「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。

ファイルシステム名

除外範囲に追加するディレクトリがあるファイルシステムの名前を入力するためのフィールドです。

このフィールドは、ファイルシステムのドロップダウンリストで［**Mounted**］が選択され、右側のドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。

マスク

このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。マスクは、［パス］フィールドに指定されたディレクトリ内のオブジェクトにのみ適用されます。

既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも 1 つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、スキャンからのオブジェクトの除外を設定できます。指定したマスクが名前に含まれるファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも 1 つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［脅威の名前による除外］ウィンドウ

脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。指定された脅威はブロックされません。既定では、脅威の名前のリストは空です。

脅威の名前は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した脅威が除外リストから削除されます。

このボタンは、少なくとも1つの脅威の名前をリストから選択している場合に使用できます。

表内の脅威の名前をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を編集できます。

［**追加**］をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を指定できます。

コマンドラインでのマルウェアのスキャン

コマンドラインでは、次の方法でマルウェアをスキャンできます：

- マルウェアのスキャンの事前定義済みタスク（*Scan_My_Computer*）を使用します。このタスクを手動で開始、停止、一時停止、再開し、タスクの実行スケジュールを設定できます。このタスクの設定を編集することで、スキャン設定を構成できます。
- マルウェアのスキャンのユーザータスク（*ODS* タイプのタスク）を使用します。ユーザータスクを手動で開始、停止、一時停止、再開し、タスクのスケジュールを設定できます。
- `kesl-control --scan-file` コマンドを使用すると、指定したファイルとディレクトリのオブジェクトスキャンを実行できます。

マルウェアのスキャン事前定義済みタスクの設定

この表では、マルウェアのスキャンタスクで指定できるすべての設定で使用可能なすべての値と既定値を説明します。

マルウェアスキャンタスクの設定

設定	説明	
ScanFiles	ファイルのスキャンを指定します。	Yes（既 す。 No – フ
ScanBootSectors	ブートセクタースキャンを指定します。	Yes（既 ンしま No – ブ ん。
ScanComputerMemory	プロセスメモリとカーネルメモリのスキャンを指定します。	Yes（既 ルメモ No – プ スキャ
ScanStartupObjects	スタートアップオブジェクトのスキャンを指定します。	Yes（既

		クトを No – ス ャンし
ScanArchived	アーカイブ（自己解凍型アーカイブを含む）のスキャンを指定します。 アプリケーションは次のアーカイブをスキャンします：.zip、.7z*、.7-z、.rar、.iso、.cab、.jar、.bz、.bz2、.tbz、.tbz2、.gz、.tgz、.arj。サポートされているアーカイブ形式のリストは、使用されている製品データベースによって異なります。	Yes（既 ます。I 指定さ 応じて、 含むア No – ア
ScanSfxArchived	自己解凍型アーカイブ（実行可能な解凍モジュールを含むアーカイブ）のみのスキャンを指定します。	Yes（既 キャン No – 自 ません。
ScanMailBases	Microsoft Outlook、Outlook Express、およびその他のメールクライアントのメールデータベースのスキャンを指定します。	Yes – キャン No（既 ァイル
ScanPlainMail	プレーンテキストのメールメッセージのスキャンを指定します。	Yes – ジをス No（既 ルメッ
SizeLimit	スキャン対象のオブジェクトの最大サイズ（メガバイト単位）。指定された値よりもスキャン対象のオブジェクトのサイズが大きい場合、オブジェクトはスキップされます。	0 ～ 99 0 – スキ 無制限 既定値
TimeLimit	オブジェクトの最大スキャン時間（秒単位）。この設定で指定された時間よりもスキャンの時間がかかる場合、そのオブジェクトのスキャンが停止されます。	0～999 0 – オ です。 既定値
FirstAction	感染したオブジェクトに対して実行される最初の処理の選択。	Disinf し、そ す。駆 別また 除でき 更され ［Disi ［Seco 処理を Remove アップ を削除 Recomm オブジ 報に基 に選択 の木馬 Securit イの木 なく、

		Skip – は削除 トに関 既定値
SecondAction	感染したオブジェクトに対して実行される次の処理の選択。最初の処理に失敗した場合に、次の処理を実行します。	Second FirstA Skip ま 選択さ はあり つの処 指定し 適用さ 既定値
UseExcludeMasks	ExcludeMasks.item_# 設定で指定されたオブジェクトのスキャン除外を有効にします。	Yes – E された ます。 No（既 定で指 ら除外
ExcludeMasks.item_#	名前またはマスクにより、オブジェクトをスキャンから除外します。この設定を使用すると、指定されたスキャン範囲から名前によって個別のファイルを除外したり、シェル形式でマスクを使用して複数のファイルを除外したりできます。 この設定の値を指定する前に、UseExcludeMasks 設定が有効になっていることを確認します。	既定値 例： UseE Excl Excl
UseExcludeThreats	ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトのスキャン除外を有効にします。	Yes – E 定され ンから No（既 設定で をスキ
ExcludeThreats.item_#	オブジェクト内で検知された脅威の名前によってスキャンからオブジェクトを除外します。この設定の値を指定する前に、UseExcludeThreats 設定が有効になっていることを確認します。 スキャンから単一オブジェクトを除外するには、このオブジェクト内で検知された脅威の完全な名前（このオブジェクトが感染していると判定した際に使用された名前の文字列）を指定します。 たとえば、ネットワークに関する情報を収集するユーティリティを使用している場合があります。これをブロックしないようにするには、スキャンから除外される脅威のリストに、製品で使用される脅威の完全な名前を追加します。 オブジェクトで検知された脅威のフルネームは、アプリケーションログや https://threats.kaspersky.com の Web サイトで確認することができます。	設定値 す。 既定値 例： UseE Excl Test Excl roja
UseGlobalExclusions	スキャンのグローバル除外を有効にします。	Yes（既 ます。 No – グ

UseOASExclusions	スキャン時にファイル脅威対策の除外を有効にします。	はい（ を使用 いいえ しません
ReportCleanObjects	感染していないとレポートされたスキャン済みオブジェクトに関する情報のログへの記録を指定します。 この設定は、たとえば特定のオブジェクトがスキャン済みであることを確認するために有効にします。	Yes – 感 る情報 No（既 クトに
ReportPackedObjects	複合オブジェクトの一部を構成するスキャン済みオブジェクトに関する情報のログへの記録を指定します。 この設定は、たとえばアーカイブ内のオブジェクトがスキャン済みであることを確認するために有効にします。	Yes – オ ェクト No（既 済みオ 録しま
ReportUnprocessedObjects	何らかの理由により処理されていないオブジェクトに関する情報のログへの記録を指定します。	Yes – 処 する情 No（既 ェクト ん。
UseAnalyzer	ヒューリスティック分析を指定します。 ヒューリスティック分析により、新しい脅威がウイルスアナリストに知られるようになる前に検知することができます。	Yes（既 を有効 No – ヒ ます。
HeuristicLevel	ヒューリスティック分析のレベルを指定します。 ヒューリスティック分析のレベルを指定できます。ヒューリスティック分析レベルは、脅威の検索範囲とオペレーティングシステムのリソースに対する負荷およびスキャンの所要時間のバランスを設定します。ヒューリスティック分析レベルが高いほど、スキャンに必要なリソースと時間が増加します。	Light い、シ Medium レベル が取れ Deep – ステム Recomm
UseIChecker	iChecker 技術の使用を指定します。	Yes（既 効にし No – iC す。
DeviceNameMasks.item_#	デバイス名のリスト。本製品はこれらのデバイスのブートセクターをスキャンします。 この設定値は空白にはできません。このタスクを実行するには、デバイス名マスクを少なくとも 1 つ設定する必要があります。	AllObj セクタ <デバ と名前 ーをス 既定値 文字。
[ScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	スキャン範囲の説明。スキャン範囲に関する詳細情報を含みます。この設定を使用して指定される文字列の最大長は 4096 文字です。	既定値 例： Area

UseScanArea	指定された範囲のスキャンを指定します。タスクを実行するには、少なくとも1つの範囲のスキャンを有効にします。	Yes（既 ンしま No – 指 ん。
AreaMask.item_#	スキャン範囲の制限。スキャン範囲内で、シェル形式のマスクを使用して指定したファイルのみをスキャンします。 この設定が指定されていない場合、スキャン範囲のすべてのオブジェクトがスキャンされます。この設定には、複数の値を指定できます。	既定値 ャン） 例： Area
Path	スキャンされるオブジェクトがあるディレクトリのパス。	< ローカ れたデ ンしま Shared クセス リソー Shared てアク テムリ Mounte てデバ レクト Mounte してデ ィレク AllRem と NFS マウン トリを AllSha ロトコ スのす スキャ < ファイ バイス ースを
[ExcludedFromScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	スキャンの除外範囲の説明。除外範囲に関する詳細情報を含みます。	既定値
UseScanArea	指定された範囲のスキャンの除外を指定します。	Yes（既 ます。 No – 指
AreaMask.item_#	スキャンの除外範囲の制限。除外範囲で、シェル形式のマスクを使用して指定したファイルのみを除外します。 この設定が指定されていない場合、除外範囲のすべてのオブジェクトが除外されます。この設定には、複数の値を指定できます。	既定値 外）。
Path	除外するオブジェクトを含むディレクトリのパス。	< ローカ れたデ む）の

ます。
す。

アス
ファ
スク

ファ
「/」
文字
「*」
ます。
「/d

2つの
ル名
「/」
列（
す。
「/d

アス
「**
クト
とえ
適切

ファ
は、
示で

スキャ
に、シ
でマウ
パスを
し、現
ている
奨しま
をベー
を追加
す：/.

Mounte
てデバ
ートデ
す。

Mounte
してデ
ィレク

AllRem
と NFS
マウン
トリを

<ファ
バイス
ースを

		リモ 始前 み、 から マウ はス

ファイルとディレクトリのオブジェクトスキャン

`kesl-control --scan-file` コマンドを使用すると、指定したファイルとディレクトリのオブジェクトスキャンを実行できます。

オブジェクトスキャンは、事前定義済みのタスク *Scan_File* (ID: 3) に保存された設定で実行されます。このタスクの設定を編集することで、ファイルのオブジェクトスキャン用の設定を構成することができます（以下の表を参照）。

指定したファイルとディレクトリのオブジェクトスキャンを開始するには、次のコマンドを実行します：

```
kesl-control --scan-file <パス> [--action <処理>]
```

説明：

- `<path>` はスキャンしたいファイルやディレクトリへのパスです。スペースで区切って複数のパスを指定することもできる。
- `--action <action>` は、感染したオブジェクトに対してアプリケーションが実行する処理です。`--action` キーを指定しないと、アプリケーションは推奨される処理を実行します。

コマンド実行の結果、一時ファイルスキャンタスクが作成され、完了後自動的に削除されます。この場合、スキャン結果はコンソールに出力されます。

この表では、*Scan_File* タスクで指定できるすべての設定と、その設定で使用可能なすべての値と既定値を説明します。

> *Scan_File* タスクで定義された `[ScanScope.item_ #]` および `[ExcludedFromScanScope.item_ #]` セクションは、オブジェクトスキャンの実行時には考慮されません。

Scan_File タスクの設定

設定	説明	
`ScanFiles`	ファイルのスキャンを指定します。	`Yes`（既 す。 `No` – フ
`ScanBootSectors`	ブートセクタースキャンを指定します。	`Yes` – フ `No`（既 ンしま
`ScanComputerMemory`	プロセスメモリとカーネルメモリのスキャンを指定します。	`Yes` – フ スキャ

		No（既 ルメモ
ScanStartupObjects	スタートアップオブジェクトのスキャンを指定します。	Yes – ス ャンしま No（既 クトをス
ScanArchived	アーカイブ（自己解凍型アーカイブを含む）のスキャンを指定します。 アプリケーションは次のアーカイブをスキャンします：.zip、.7z*、.7-z、.rar、.iso、.cab、.jar、.bz、.bz2、.tbz、.tbz2、.gz、.tgz、.arj。サポートされているアーカイブ形式のリストは、使用されている製品データベースによって異なります。	Yes（既 ます。I 指定さ 応じて、 含むア No – ア
ScanSfxArchived	自己解凍型アーカイブ（実行可能な解凍モジュールを含むアーカイブ）のみのスキャンを指定します。	Yes（既 キャン No – 自 ません。
ScanMailBases	Microsoft Outlook、Outlook Express、The Bat!、およびその他のメールクライアントのメールデータベースのスキャンを有効にします。	Yes – メ キャン No（既 ァイル
ScanPlainMail	プレーンテキストのメールメッセージのスキャンを指定します。	Yes – プ ジをス No（既 ルメッ
SizeLimit	スキャン対象のオブジェクトの最大サイズ（メガバイト単位）。指定された値よりもスキャン対象のオブジェクトのサイズが大きい場合、オブジェクトはスキップされます。	0 ～ 99 0 – スキ 無制限 既定値
TimeLimit	オブジェクトの最大スキャン時間（秒単位）。この設定で指定された時間よりもスキャンの時間がかかる場合、そのオブジェクトのスキャンが停止されます。	0～999 0 – オプ です。 既定値
FirstAction	感染したオブジェクトに対して実行される最初の処理の選択。	Disinf し、そ す。駆除 別または 除できな 更され ［Disi ［Seco 処理を指 Remove アップ を削除

		Recomm オブジ 報に基 に選択 の木馬 Security イの木 なく、 Skip – は削除 トに関 既定値
SecondAction	感染したオブジェクトに対して実行される次の処理の選択。最初の処理に失敗した場合に、次の処理を実行します。	Second FirstA Skip ま 選択さ はあり つの処 指定し 適用さ 既定値
UseExcludeMasks	ExcludeMasks.item_# 設定で指定されたオブジェクトのスキャン除外を有効にします。	Yes – E された ます。 No（既 定で指 ら除外
ExcludeMasks.item_#	名前またはマスクにより、オブジェクトをスキャンから除外します。この設定を使用すると、指定されたスキャン範囲から名前によって個別のファイルを除外したり、シェル形式でマスクを使用して複数のファイルを除外したりできます。	既定値 例： UseE Excl Excl
UseExcludeThreats	ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトのスキャン除外を有効にします。	Yes – E 定され ンから No（既 設定で をスキ
ExcludeThreats.item_#	オブジェクト内で検知された脅威の名前によってスキャンからオブジェクトを除外します。この設定の値を指定する前に、UseExcludeThreats 設定が有効になっていることを確認します。 スキャンから単一オブジェクトを除外するには、このオブジェクト内で検知された脅威の完全な名前（このオブジェクトが感染していると判定した際に使用された名前の文字列）を指定します。 たとえば、ネットワークに関する情報を収集するユーティリティを使用している場合があります。これをブロックしないようにするには、スキャンから除外される脅威のリストに、製品で使用される脅威の完全な名前を追加します。	設定値 す。 既定値 例： UseE Excl Test Excl roja

	オブジェクトで検知された脅威のフルネームは、アプリケーションログや https://threats.kaspersky.com の Web サイトで確認することができます。	
UseGlobalExclusions	スキャンのグローバル除外を有効にします。	Yes（既 ます。 No – グ
UseOASExclusions	スキャン時にファイル脅威対策の除外を有効にします。	はい（ を使用 いいえ しませ
ReportCleanObjects	感染していないとレポートされたスキャン済みオブジェクトに関する情報のログへの記録を指定します。 この設定は、たとえば特定のオブジェクトがスキャン済みであることを確認するために有効にします。	Yes – 感 る情報 No（既 クトに
ReportPackedObjects	複合オブジェクトの一部を構成するスキャン済みオブジェクトに関する情報のログへの記録を指定します。 この設定は、たとえばアーカイブ内のオブジェクトがスキャン済みであることを確認するために有効にします。	Yes – ブ ェクト No（既 済みオ 録しま
ReportUnprocessedObjects	何らかの理由により処理されていないオブジェクトに関する情報のログへの記録を指定します。	Yes – 処 する情 No（既 ェクト ん。
UseAnalyzer	ヒューリスティック分析を指定します。 ヒューリスティック分析により、新しい脅威がウイルスアナリストに知られるようになる前に検知することができます。	Yes（既 を有効 No – ヒ ます。
HeuristicLevel	ヒューリスティック分析のレベルを指定します。 ヒューリスティック分析のレベルを指定できます。ヒューリスティック分析レベルは、脅威の検索範囲とオペレーティングシステムのリソースに対する負荷およびスキャンの所要時間のバランスを設定します。ヒューリスティック分析レベルが高いほど、スキャンに必要なリソースと時間が増加します。	Light い、シ Medium レベル が取れ Deep – ステム Recomm
UseIChecker	iChecker 技術の使用を指定します。	Yes（既 効にし No – iC す。
DeviceNameMasks.item_#	デバイス名のリスト。本製品はこれらのデバイスのブートセクターをスキャンします。 この設定値は空白にはできません。このタスクを実行するには、デバイス名マスクを少なくとも 1 つ設定する必要があります。	AllObj セクタ <デバ と名前 ーをス 既定値 文字。

[ScanScope.item_#] セクションには、次の設定が含まれています：

AreaDesc	スキャン範囲の説明。スキャン範囲に関する詳細情報を含みます。この設定を使用して指定される文字列の最大長は 4096 文字です。	既定値 例： Area data
UseScanArea	指定された範囲のスキャンを指定します。タスクを実行するには、少なくとも 1 つの範囲のスキャンを有効にします。	Yes（既 ンしま No – 指 ん。
AreaMask.item_#	スキャン範囲の制限。スキャン範囲内で、シェル形式のマスクを使用して指定したファイルのみをスキャンします。 この設定が指定されていない場合、スキャン範囲のすべてのオブジェクトがスキャンされます。この設定には、複数の値を指定できます。	既定値 ャン） 例： Area
Path	スキャンされるオブジェクトがあるディレクトリのパス。	< ローカ れたデ ンしま Shared クセス リソー Shared てアク テムリ Mounte てデバ レクト Mounte してデ ィレク AllRem と NFS マウン トリを AllSha ロトコ スのす スキャ < ファ バイス ースを

[ExcludedFromScanScope.item_#] セクションには、次の設定が含まれています：

AreaDesc	スキャンの除外範囲の説明。除外範囲に関する詳細情報を含みます。	既定値
UseScanArea	指定された範囲のスキャンの除外を指定します。	Yes（既 ます。 No – 指

AreaMask.item_#	スキャンの除外範囲の制限。除外範囲で、シェル形式のマスクを使用して指定したファイルのみを除外します。 この設定が指定されていない場合、除外範囲のすべてのオブジェクトが除外されます。この設定には、複数の値を指定できます。	既定値 外）。
Path	除外するオブジェクトを含むディレクトリのパス。	<ロー れたデ む）の ます。 す。 アス ファ スク ファ 「/」 文字 「*」 ます。 「/d 2つの ル名 「/」 列（ す。 「/d アス 「** クト とえ 適切 ファ は、 示で スキャ に、シ でマウ パスを、 し、現 ている 奨しま をベー を追加 す：/. Mounte てデバ ートデ す。 Mounte してデ ィレク

		AllRem と NFS マウン トリを <ファ バイス ースを リモ 始前 み、 から マウ はス

簡易スキャン

簡易スキャンを実行する場合、Kaspersky Endpoint Security はブートセクター、スタートアップオブジェクト、プロセスメモリ、およびカーネルメモリをスキャンできます。

マルウェアを検知すると、本製品は感染したファイルを削除し、このファイルから開始したマルウェアのプロセスを終了させることができます。

簡易スキャンを開始し、スキャンの設定を構成できます。

- スキャンするオペレーティングシステムオブジェクトを選択します。ブートセクター、プロセスメモリとカーネルメモリ、スタートアップオブジェクト、アーカイブのスキャンは既定で有効になっています。既定では、簡易スキャン中にファイルはスキャンされません。
- スキャンするオブジェクトのサイズとオブジェクトのスキャン時間を制限します。
- 感染したオブジェクトに対して実行される処理を選択します。
- スキャンからのオブジェクトの除外を設定します：
  - 名前またはマスクに基づく
  - オブジェクトで検知された脅威の名前に基づく
- スキャン時にグローバル除外とファイル脅威対策除外を有効または無効にします。
- スキャンされた非感染オブジェクト、アーカイブ内のスキャンオブジェクト、および未処理のオブジェクトに関する情報のログ記録を有効にします。
- スキャン中のヒューリスティック分析と iChecker テクノロジーの使用を設定します。
- ブートセクターをスキャンする必要がある一連のデバイスを制限します。
- スキャン範囲とスキャン除外範囲を設定します。

Web コンソールでの簡易スキャン

Web コンソールでは、*簡易スキャン*タスクを使用して、保護対象デバイスのオペレーティングシステムの簡易スキャンを実行できます。

簡易スキャンのユーザータスクを作成し、実行できます。タスクの設定を編集してスキャン設定を管理できます。

簡易スキャンタスクの設定

設定	説明
アーカイブをスキャン	このチェックボックスでは、アーカイブをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、アーカイブがスキャンされます。 アーカイブをスキャンするには、アーカイブを解凍する必要があるためスキャン速度が遅くなる可能性があります。［**スキャンの全般設定**］セクションの［**スキャン時間が次を超えたらファイルをスキップする（秒）**］および［**ファイルのサイズが次を超えたらスキップする（MB）**］を設定すると、アーカイブのスキャンの所要時間を減らすことができます。

	このチェックボックスをオフにすると、アーカイブはスキャンされません。 既定では、このチェックボックスはオンです。
SFX アーカイブをスキャン	このチェックボックスでは、*自己解凍アーカイブ*をスキャンするかどうかを選択します。自己解凍アーカイブとは、実行可能な展開モジュールを含むアーカイブです。 このチェックボックスをオンにすると、自己解凍アーカイブがスキャンされます。 このチェックボックスをオフにすると、自己解凍アーカイブはスキャンされません。 このチェックボックスは、［**アーカイブをスキャン**］がオフの場合に使用できます。 既定では、このチェックボックスはオンです。
メールデータベースをスキャン	このチェックボックスでは、Microsoft Outlook、Outlook Express などのメールアプリケーションのメールデータベースをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、メールデータベースはスキャンされます。 このチェックボックスをオフにすると、メールデータベースはスキャンされません。 既定では、このチェックボックスはオフです。
メール形式のファイルをスキャン	このチェックボックスでは、プレーンテキストのメールメッセージのファイルをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、プレーンテキストのメッセージがスキャンされます。 このチェックボックスをオフにすると、プレーンテキストのメッセージはスキャンされません。 既定では、このチェックボックスはオフです。
スキャン時間が次を超えたらファイルをスキップする（秒）	このフィールドでは、ファイルをスキャンする最大時間を秒単位で指定できます。指定した時間が経過した後、ファイルのスキャンは停止されます。 使用できる値：0 ～ 9999。値が 0 に設定されると、スキャン時間は制限されません。 既定値：0
ファイルのサイズが次を超えたらスキップする（MB）	このフィールドでは、スキャンするファイルの最大サイズをメガバイト単位で指定できます。 使用できる値：0 ～ 999999。値が 0 に設定されると、サイズにかかわらず、すべてのファイルがスキャンされます。 既定値：0
感染していないオブジェクトを記録する	このチェックボックスでは、*ObjectProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、スキャンされたすべてのオブジェクトの *ObjectProcessed* タイプのイベントをログに記録します。 このチェックボックスをオフにすると、スキャンされたオブジェクトの *ObjectProcessed* タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
処理されていないファイルについて通知する	このチェックボックスでは、スキャン中にファイルを処理できない場合、*ObjectNotProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、［*ObjectNotProcessed*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*ObjectNotProcessed*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
圧縮されたオブジェク	このチェックボックスでは、検出されたすべての圧縮されたオブジェクトに関する *PackedObjectDetected* タイプのイベントをログに記録するかどうかを選択します。

トを記録する	このチェックボックスをオンにすると、［*PackedObjectDetected*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*PackedObjectDetected*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
iChecker 技術を使用する	このチェックボックスでは、前回のファイルのスキャン以降の新しいファイルおよび変更されたファイルのみをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、前回のスキャン以降の新しいファイルおよび変更されたファイルのみがスキャンされます。 このチェックボックスをオフにすると、作成日または変更日に関係なくファイルがスキャンされます。 既定では、このチェックボックスはオンです。
ヒューリスティック分析を使用する	このチェックボックスでは、ファイルのスキャン中にヒューリスティック分析を使用するかどうかを選択します。 既定では、このチェックボックスはオンです。
ヒューリスティック分析のレベル	［**ヒューリスティック分析を使用する**］をオンにすると、ドロップダウンリストでヒューリスティック分析レベルを選択できます。 • **低**：スキャンの詳細レベルが最も低く、システム負荷は最小です。 • **中**：スキャンの詳細レベルは中程度で、システム負荷のバランスが取れています。 • **高**：スキャンの詳細レベルが最も高く、システム負荷は最大です。 • **推奨**（既定値）：カスペルスキーが推奨する、最適なレベルです。保護品質と保護対象デバイスの性能への影響の最適な組み合わせを保証します。
最初の処理	このドロップダウンリストでは、感染したオブジェクトの検知時に実行する最初の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています（既定値）。 • **スキップ**：オブジェクトをスキップします。
次の処理	このドロップダウンリストでは、感染したオブジェクトに対する最初の処理が成功しなかった場合に実行する次の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています。

	• **スキップ**：オブジェクトをスキップします（既定値）。
スキャン範囲	タスクによってスキャンされた範囲を示す表。表には既定で、ローカルファイルシステムのすべてのディレクトリを対象とする1つのスキャン範囲が表示されています。 表内ではスキャン範囲に対して次の操作ができます：追加、設定、削除、上に移動、下に移動。 ［**下へ**］をクリックすると、表内で選択した項目が下に移動します。 指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。 このボタンは、1つの範囲を表から選択している場合に使用できます。 ［**上へ**］をクリックすると、表内で選択した項目が上に移動します。 指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。 このボタンは、1つの範囲を表から選択している場合に使用できます。 ［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。 このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。 スキャン範囲名をクリックすると、［**<スキャン範囲>**］ウィンドウが表示されます。このウィンドウでは、選択したスキャン範囲の設定を編集できます。 ［**追加**］をクリックすると、［**<新しいスキャン範囲>**］ウィンドウが表示されます。このウィンドウでは、新しいスキャン範囲を指定できます。

［スキャン範囲の追加］ウィンドウ

このウィンドウでは、スキャン範囲の追加や設定ができます。

スキャン範囲設定

設定	説明
範囲名	スキャン範囲の名前を入力するフィールド。この名前は、**スキャン設定**セクションの**スキャン範囲**表で表示されます。 この入力フィールドを空白のままにすることはできません。

この範囲を使用する	このチェックボックスでは、製品がこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、製品がこのスキャン範囲を処理します。 このチェックボックスをオフにすると、製品がこのスキャン範囲を処理しません。このチェックボックスをオンにすることにより、後からこの範囲をコンポーネント設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	ドロップダウンリストからファイルシステムの種別を選択できます： • **Local**（既定値）：ローカルディレクトリ。この項目を選択する場合は、ローカルディレクトリのパスを指定する必要があります。 • **Mounted** – マウントされたリモートまたはローカルのディレクトリ。この項目を選択する場合は、ファイルシステムのプロトコルまたは名前を指定する必要があります。 • **Shared** – Samba または NFS プロトコルでアクセス可能な保護されているサーバーファイルシステムリソースを表示します。 • **リモートでマウント済みのすべての場所** – Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。 • **共有済みのすべての場所** – Samba および NFS プロトコルでアクセス可能なすべての保護されているサーバーファイルシステムリソース。
アクセスプロトコル	ドロップダウンリストからリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。 このドロップダウンリストは、ファイルシステムのドロップダウンリストから［**Shared**］または［**Mounted**］を選択した場合に使用できます。
パス	これは、スキャン範囲に含めるディレクトリのパスを指定するための入力フィールドです。パスの指定にマスクおよびタグを使用できます。

特別なタグを使用してコンテナまたはイメージを指定できます：

- [container-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>]/<ローカルディレクトリへのパス>
- [image-id:<識別子>]/<ローカルディレクトリへのパス>
- [image-name:<名前>]/<ローカルディレクトリへのパス>

[container-id:<識別子>]、[container-name:<名前>]、[image-id:<識別子>]、および [image-name:<名前>]/<ローカルディレクトリ> タグの一意の組み合わせを使用することもできます。

1つのエリア内で1〜4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。

例：

- [container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>

名前と識別子にはマスク（? および * 記号）を使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリをスキャンします。 このフィールドは、ファイルシステムのドロップダウンリストから［**Local**］を選択した場合に使用できます。 ファイルシステムのドロップダウンリストから［**Local**］が選択され、パスが指定されていない場合、ローカルファイルシステムのすべてのディレクトリがスキャンされます。
共有リソース名	スキャン範囲に追加するディレクトリがある、ファイルシステム共有リソースの名前を入力するためのフィールドです。 このフィールドは、［ファイルシステム］ドロップダウンリストで［**Mounted**］が選択され、［**アクセスプロトコル**］ドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。
マスク	このリストには、動作中に製品がスキャンするオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［スキャン範囲］ウィンドウ

設定	説明
ファイルをスキャン	このチェックボックスでは、ファイルスキャンを有効にするかどうかを選択します。 このチェックボックスをオンにすると、ファイルがスキャンされます。 このチェックボックスをオフにすると、ファイルはスキャンされません。 既定では、このチェックボックスはオフです。
ブートセクターをスキャン	このチェックボックスでは、ブートセクターをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、ブートセクターがスキャンされます。 このチェックボックスをオフにすると、ブートセクターはスキャンされません。 既定では、このチェックボックスはオンです。
カーネルメモリおよび実行中処理のスキャン	このチェックボックスでは、クライアントデバイスのメモリをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、カーネルメモリと実行中のプロセスがスキャンされます。 このチェックボックスをオフにすると、カーネルメモリと実行中のプロセスはスキャンされません。 既定では、このチェックボックスはオンです。
スタートアップオブジェクトをスキャン	このチェックボックスでは、スタートアップオブジェクトをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、スタートアップオブジェクトがスキャンされます。 このチェックボックスをオフにすると、スタートアップオブジェクトはスキャンされません。 既定では、このチェックボックスはオンです。
スキャン対象デバイス	［**デバイスマスクの設定**］をクリックすると［**スキャン範囲**］ウィンドウが表示され、ブートセクターをスキャンするデバイスを指定できます。

［スキャン範囲］ウィンドウ

この表には、スキャンする必要のあるブートセクターを持つデバイスの名前マスクが含まれています。既定では、すべてのデバイスを示すマスク「**/****」がリストに含まれています。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲］セクション

簡易スキャンタスクの［**除外範囲**］セクションでは、除外範囲、マスクと脅威名による除外、およびタスク実行時のグローバル除外とファイル脅威対策除外の使用を設定できます。

スキャンの除外の設定

設定	説明
監視の除外範囲を設定する	［**除外リストを設定する**］をクリックすると、［**除外範囲**］ウィンドウが表示されます。このウィンドウでは、スキャンの除外のリストを定義できます。
除外をマスクで設定する	［**除外をマスクで設定する**］をクリックすると、［**マスクによる除外**］ウィンドウが表示されます。このウィンドウでは、名前のマスクにより、スキャンからのオブジェクトの除外を設定できます。
除外を脅威名で設定する	［**除外を脅威名で設定する**］をクリックすると、［**脅威の名前による除外**］ウィンドウが表示されます。このウィンドウでは、脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。
グローバル除外リストを使用	チェックボックスは、本製品の実行中にグローバル例外で指定されたマウントポイントの除外を有効または無効にします。 チェックボックスをオンにすると、設定されたマウントポイントをスキャンから除外します。 既定では、このチェックボックスはオンです。
ファイル脅威対策の除外リストを使用	このチェックボックスは、アプリケーションの実行時に設定されたファイル脅威対策の除外の使用を有効または無効にします。 チェックボックスをオンにすると、アプリケーションはファイル脅威対策コンポーネントの除外に指定されたオブジェクトをスキャンしません。 既定では、このチェックボックスはオンです。

［除外範囲］ウィンドウ

この表には、スキャンの除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	スキャンから除外されるディレクトリのパス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲の追加］ウィンドウ

このウィンドウでは、除外範囲の追加や設定ができます。

除外範囲の設定

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品の実行時にこの範囲を除外するかどうかを選択します。 チェックボックスをオンにすると、動作中にこの範囲がスキャンや保護の対象から除外されます。 チェックボックスをオフにすると、動作中にこの範囲がスキャンや保護の対象に含まれます。チェックボックスをオンにすることにより、この範囲をスキャンや保護の対象から後で除外できます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	このドロップダウンリストでは、スキャンの除外に追加するディレクトリがあるファイルシステムの種別を選択できます： • **Local**：ローカルディレクトリ。 • **Mounted** - デバイスにマウントされるリモートディレクトリ。 • **リモートでマウント済みのすべての場所** - Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。
アクセスプロトコル	ドロップダウンリストからリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。 このドロップダウンリストは、ファイルシステムのドロップダウンリストから［**Mounted**］を選択した場合に使用できます。
パス	除外範囲に追加するディレクトリのパスの入力フィールドです。パスの指定にマスクおよびタグを使用できます。

特別なタグを使用してコンテナまたはイメージを指定できます：

- [container-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>]/<ローカルディレクトリへのパス>
- [image-id:<識別子>]/<ローカルディレクトリへのパス>
- [image-name:<名前>]/<ローカルディレクトリへのパス>

[container-id:<識別子>]、[container-name:<名前>]、[image-id:<識別子>]、および [image-name:<名前>]/<ローカルディレクトリ> タグの一意の組み合わせを使用することもできます。

1つのエリア内で1～4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。

例：

- [container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>

名前と識別子にはマスク（? および * 記号）を使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。 マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。 ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。 このフィールドは、ファイルシステムのドロップダウンリストから［**Local**］を選択した場合に使用できます。
共有リソース名	除外範囲に追加するディレクトリがある、ファイルシステム共有リソースの名前を入力するためのフィールドです。 このフィールドは、［ファイルシステム］ドロップダウンリストで［**Mounted**］が選択され、［**アクセスプロトコル**］ドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。
マスク	このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。マスクは、［**パス**］フィールドに指定されたディレクトリ内のオブジェクトにのみ適用されます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。 このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。 マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、スキャンからのオブジェクトの除外を設定できます。指定したマスクが名前に含まれるファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［脅威の名前による除外］ウィンドウ

脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。指定された脅威はブロックされません。既定では、脅威の名前のリストは空です。

脅威の名前は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した脅威が除外リストから削除されます。

このボタンは、少なくとも1つの脅威の名前をリストから選択している場合に使用できます。

表内の脅威の名前をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を編集できます。

［**追加**］をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を指定できます。

管理コンソールでの簡易スキャン

管理コンソールでは、*簡易スキャンタスク*を使用して、保護対象デバイスのオペレーティングシステムの簡易スキャンを実行できます。

簡易スキャンのユーザータスクを作成し、実行できます。タスクの設定を編集してスキャン設定を管理できます。

簡易スキャンタスクのプロパティの［**設定**］セクションでは、次の表に示す設定を構成できます。

簡易スキャンタスクの設定

設定	説明
スキャン	この設定グループには、スキャン範囲、スキャン範囲設定、およびスキャン設定を指定できるウィンドウを開くボタンが含まれています。
脅威の検知時の処理	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**脅威の検知時の処理**］ウィンドウが表示され、検知された感染オブジェクトに対して実行する処理を設定できます。

簡易スキャンタスクのプロパティの［**除外**］セクションでは、マスクと脅威名による除外範囲または除外を設定することもできます。

［スキャン範囲］ウィンドウ

この表にはスキャン範囲が含まれます。表で指定されたパス内のファイルとディレクトリをすべてスキャンします。表には既定で、ローカルファイルシステムのすべてのディレクトリを対象とする1つのスキャン範囲が表示されています。

スキャン範囲設定

設定	説明
範囲名	スキャン範囲名。
パス	スキャンするディレクトリのパス。
ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、範囲の表の並び順でスキャンされます。必要に応じて、サブディレクトリを親ディレクトリよりもリストの上に配置し、親ディレクトリとは異なるセキュリティ設定をサブディレクトリに設定します。

［<新しいスキャン範囲>］ウィンドウ

このウィンドウでは、スキャン範囲の追加や設定ができます。

スキャン範囲設定

設定	説明
スキャン範囲名	スキャン範囲の名前を入力するフィールド。この名前は、［**スキャン範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品がこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、製品がこのスキャン範囲を処理します。 このチェックボックスをオフにすると、製品がこのスキャン範囲を処理しません。このチェックボックスをオンにすることにより、後からこの範囲をコンポーネント設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステ	これらの設定では、スキャン範囲を設定できます。

ム、アクセスプロトコル、パス	ファイルシステムのドロップダウンリストで、ファイルシステムの種別を選択できます： • **Local**（既定値）：ローカルディレクトリ。この項目を選択する場合は、ローカルディレクトリのパスを指定する必要があります。 • **Mounted** – マウントされたリモートまたはローカルのディレクトリ。この項目を選択する場合は、ファイルシステムのプロトコルまたは名前を指定する必要があります。 • **Shared** – Samba または NFS プロトコルでアクセス可能な保護されているサーバーファイルシステムリソースを表示します。 • **リモートでマウント済みのすべての場所** – Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。 • **共有済みのすべての場所** – Samba および NFS プロトコルでアクセス可能なすべての保護されているサーバーファイルシステムリソース。
	ファイルシステムのドロップダウンリストで **Shared** または **Mounted** を選択した場合は、右側のドロップダウンリストでリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。
	ファイルシステムのドロップダウンリストで **Local** を選択した場合は、スキャン範囲に追加するディレクトリのパスを入力フィールドに入力できます。パスの指定にマスクおよびタグを使用できます。

特別なタグを使用してコンテナまたはイメージを指定できます：

- [container-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>]/<ローカルディレクトリへのパス>
- [image-id:<識別子>]/<ローカルディレクトリへのパス>
- [image-name:<名前>]/<ローカルディレクトリへのパス>

[container-id:<識別子>]、[container-name:<名前>]、[image-id:<識別子>]、および [image-name:<名前>]/<ローカルディレクトリ> タグの一意の組み合わせを使用することもできます。

1つのエリア内で1〜4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。

例：

- [container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>

名前と識別子にはマスク（? および * 記号）を使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリをスキャンします。 ファイルシステムのドロップダウンリストから［**Local**］が選択され、パスが指定されていない場合、ローカルファイルシステムのすべてのディレクトリがスキャンされます。
ファイルシステム名	スキャン範囲に追加するディレクトリがあるファイルシステムの名前を入力するためのフィールドです。 このフィールドは、ファイルシステムのドロップダウンリストで［**Mounted**］が選択され、右側のドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。
マスク	このリストには、動作中に製品がスキャンするオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［スキャン範囲の設定］ウィンドウ

このウィンドウでは、簡易スキャンタスクのファイルスキャンを設定します。ファイル、ブートセクター、スタートアップオブジェクト、プロセスメモリ、カーネルメモリをスキャンできます。

スキャン範囲設定

設定	説明
ファイルをスキャン	このチェックボックスでは、ファイルスキャンを有効にするかどうかを選択します。 このチェックボックスをオンにすると、ファイルがスキャンされます。 チェックボックスをオフにすると、ファイルはスキャンされません。 既定では、このチェックボックスはオフです。
ブートセクターをスキャン	このチェックボックスでは、ブートセクターをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、ブートセクターがスキャンされます。 このチェックボックスをオフにすると、ブートセクターはスキャンされません。 既定では、このチェックボックスはオンです。
カーネルメモリおよび実行中処理のスキャン	このチェックボックスでは、デバイスのメモリをスキャンするかどうかを選択します。 このチェックボックスがオンにすると、Kaspersky Endpoint Security はカーネルメモリと実行中のプロセスをスキャンします。 このチェックボックスをオフにすると、Kaspersky Endpoint Security はカーネルメモリと実行中のプロセスをスキャンしません。 既定では、このチェックボックスはオンです。
スタートアップオブジェクトをスキャン	このチェックボックスでは、スタートアップオブジェクトをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、スタートアップオブジェクトがスキャンされます。 このチェックボックスをオフにすると、スタートアップオブジェクトはスキャンされません。 既定では、このチェックボックスはオンです。
スキャン対象デバイス	この設定グループには、**設定**が含まれています。このボタンをクリックすると［**スキャン範囲**］ウィンドウが表示され、ブートセクターをスキャンするデバイスを指定できます。
グローバル除外リストを使用	チェックボックスは、本製品の実行中にグローバル例外で指定されたマウントポイントの除外を有効または無効にします。 チェックボックスをオンにすると、設定されたマウントポイントをスキャンから除外します。 既定では、このチェックボックスはオンです。
ファイル脅威対策の除外リストを使用	このチェックボックスは、アプリケーションの実行時に設定されたファイル脅威対策の除外の使用を有効または無効にします。 チェックボックスをオンにすると、アプリケーションはファイル脅威対策コンポーネントの除外に指定されたオブジェクトをスキャンしません。 既定では、このチェックボックスはオンです。

［スキャン範囲］ウィンドウ

この表には、スキャンする必要のあるブートセクターを持つデバイスの名前マスクが含まれています。既定では、すべてのデバイスを示すマスク「**/****」がリストに含まれています。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［スキャンの設定］ウィンドウ

このウィンドウでは、タスクのファイルスキャンを設定します。

スキャン設定

設定	説明
アーカイブをスキャン	このチェックボックスでは、アーカイブをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、アーカイブがスキャンされます。 アーカイブをスキャンするには、アーカイブを解凍する必要があるためスキャン速度が遅くなる可能性があります。［**スキャンの全般設定**］セクションの［**スキャン時間が次を超えたらファイルをスキップする（秒）**］および［**ファイルのサイズが次を超えたらスキップする（MB）**］を設定すると、アーカイブのスキャンの所要時間を減らすことができます。 このチェックボックスをオフにすると、アーカイブはスキャンされません。 既定では、このチェックボックスはオンです。
SFX アーカイブをスキャン	このチェックボックスでは、*自己解凍アーカイブ*をスキャンするかどうかを選択します。自己解凍アーカイブとは、実行可能な展開モジュールを含むアーカイブです。 このチェックボックスをオンにすると、自己解凍アーカイブがスキャンされます。 このチェックボックスをオフにすると、自己解凍アーカイブはスキャンされません。 このチェックボックスは、［**アーカイブをスキャン**］がオフの場合に使用できます。 既定では、このチェックボックスはオンです。
メールデータベースをスキャン	このチェックボックスでは、Microsoft Outlook、Outlook Express などのメールアプリケーションのメールデータベースをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、メールデータベースはスキャンされます。 このチェックボックスをオフにすると、メールデータベースはスキャンされません。 既定では、このチェックボックスはオフです。
メール形式のファイルをスキャン	このチェックボックスでは、プレーンテキストのメールメッセージのファイルをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、プレーンテキストのメッセージがスキャンされます。

	このチェックボックスをオフにすると、プレーンテキストのメッセージはスキャンされません。 既定では、このチェックボックスはオフです。
スキャン時間が次を超えたらファイルをスキップする（秒）	このフィールドでは、ファイルをスキャンする最大時間を秒単位で指定できます。指定した時間が経過した後、ファイルのスキャンは停止されます。 使用できる値：0 ～ 9999。値が 0 に設定されると、スキャン時間は制限されません。 既定値：0
ファイルのサイズが次を超えたらスキップする（MB）	このフィールドでは、スキャンするファイルの最大サイズをメガバイト単位で指定できます。 使用できる値：0 ～ 999999。値が 0 に設定されると、サイズにかかわらず、すべてのファイルがスキャンされます。 既定値：0
感染していないオブジェクトを記録する	このチェックボックスでは、*ObjectProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、スキャンされたすべてのオブジェクトの *ObjectProcessed* タイプのイベントをログに記録します。 このチェックボックスをオフにすると、スキャンされたオブジェクトの *ObjectProcessed* タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
処理されていないオブジェクトを記録する	このチェックボックスでは、スキャン中にファイルを処理できない場合、*ObjectNotProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、［*ObjectNotProcessed*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*ObjectNotProcessed*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
圧縮されたオブジェクトを記録する	このチェックボックスでは、検出されたすべての圧縮されたオブジェクトに関する *PackedObjectDetected* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、［*PackedObjectDetected*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*PackedObjectDetected*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
iChecker 技術を使用する	このチェックボックスでは、前回のファイルのスキャン以降の新しいファイルおよび変更されたファイルのみをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、前回のスキャン以降の新しいファイルおよび変更されたファイルのみがスキャンされます。 このチェックボックスをオフにすると、作成日または変更日に関係なくファイルがスキャンされます。 既定では、このチェックボックスはオンです。
ヒューリスティック分析を使用する	このチェックボックスでは、ファイルのスキャン中にヒューリスティック分析を使用するかどうかを選択します。 既定では、このチェックボックスはオンです。
ヒューリスティック分	［**ヒューリスティック分析を使用する**］をオンにすると、ドロップダウンリストでヒューリスティック分析レベルを選択できます。

析のレベル	• **低**：スキャンの詳細レベルが最も低く、システム負荷は最小です。 • **中**：スキャンの詳細レベルは中程度で、システム負荷のバランスが取れています。 • **高**：スキャンの詳細レベルが最も高く、システム負荷は最大です。 • **推奨**（既定値）：カスペルスキーが推奨する、最適なレベルです。保護品質と保護対象デバイスの性能への影響の最適な組み合わせを保証します。

［脅威の検知時の処理］ウィンドウ

このウィンドウでは、検知された感染オブジェクトに対して実行する処理を設定できます：

脅威の検知時の処理

設定	説明
最初の処理	このドロップダウンリストでは、感染したオブジェクトの検知時に実行する最初の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています（既定値）。 • **スキップ**：オブジェクトをスキップします。
次の処理	このドロップダウンリストでは、感染したオブジェクトに対する最初の処理が成功しなかった場合に実行する次の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています。 • **スキップ**：オブジェクトをスキップします（既定値）。

除外セクション

［*スキャンの除外*］は一連の条件です。これらの条件を満たす場合、Kaspersky Endpoint Security はオブジェクトのウイルスやその他のマルウェアのスキャンを行いません。マスクと脅威の名前で指定することで、スキャンからオブジェクトを除外することもできます。

スキャンの除外の設定

設定のグループ	説明
除外範囲	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**除外範囲**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する範囲のリストを指定できます。
マスクによる除外	この設定グループには［**設定**］が含まれています。クリックすると、［**マスクによる除外**］ウィンドウが表示されます。このウィンドウでは、名前のマスクにより、スキャンからのオブジェクトの除外を設定できます。
脅威の名前による除外	この設定グループには［**設定**］が含まれています。クリックすると、［**脅威の名前による除外**］ウィンドウが表示されます。このウィンドウでは、脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。

［除外範囲］ウィンドウ

この表には、スキャンの除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	スキャンから除外されるディレクトリのパス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［<新しい除外範囲>］ウィンドウ

このウィンドウでは、スキャンの除外範囲の追加や設定ができます。

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品の実行時にこの範囲をスキャンから除外するかどうかを選択します。 チェックボックスをオンにすると、スキャン中にこの範囲が除外されます。 このチェックボックスをオフにすると、この範囲がスキャン範囲に含まれます。このチェックボックスをオンにすることにより、後からこの範囲を除外することができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	これらの設定では、除外範囲を設定できます。 ファイルシステムのドロップダウンリストで、スキャンから除外するディレクトリのファイルシステムの種別を選択できます： • **Local**：ローカルディレクトリ。 • **Mounted**：マウントされたディレクトリ。 • **リモートでマウント済みのすべての場所** - Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。
	ファイルシステムのドロップダウンリストで **Mounted** を選択した場合は、右側のドロップダウンリストでリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。
	ファイルシステムのドロップダウンリストで **Local** を選択した場合は、除外範囲に追加するディレクトリのパスを入力フィールドに入力できます。パスの指定にマスクおよびタグを使用できます。

特別なタグを使用してコンテナまたはイメージを指定できます：

- [container-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>]/<ローカルディレクトリへのパス>
- [image-id:<識別子>]/<ローカルディレクトリへのパス>
- [image-name:<名前>]/<ローカルディレクトリへのパス>

[container-id:<識別子>]、[container-name:<名前>]、[image-id:<識別子>]、および [image-name:<名前>]/<ローカルディレクトリ> タグの一意の組み合わせを使用することもできます。

1つのエリア内で1～4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。

例：

- [container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>

名前と識別子にはマスク（? および * 記号）を使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。 マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。 ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。
ファイルシステム名	除外範囲に追加するディレクトリがあるファイルシステムの名前を入力するためのフィールドです。 このフィールドは、ファイルシステムのドロップダウンリストで［**Mounted**］が選択され、右側のドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。
マスク	このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。マスクは、［パス］フィールドに指定されたディレクトリ内のオブジェクトにのみ適用されます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。 このボタンは、少なくとも 1つのファイルマスクをリストから選択している場合に使用できます。 マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、スキャンからのオブジェクトの除外を設定できます。指定したマスクが名前に含まれるファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［脅威の名前による除外］ウィンドウ

脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。指定された脅威はブロックされません。既定では、脅威の名前のリストは空です。

脅威の名前は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した脅威が除外リストから削除されます。

このボタンは、少なくとも1つの脅威の名前をリストから選択している場合に使用できます。

表内の脅威の名前をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を編集できます。

［**追加**］をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を指定できます。

コマンドラインでの簡易スキャン

コマンドラインでは、簡易スキャン事前定義済みタスク（*Critical_Areas_Scan*）を使用して、保護対象デバイスのオペレーティングシステムの簡易スキャンを実行できます。

このタスクを手動で開始、停止、一時停止、再開し、タスクの実行スケジュールを設定できます。このタスクの設定を編集することで、スキャン設定を構成できます。

簡易スキャンタスクの設定

設定	説明	
ScanFiles	ファイルのスキャンを指定します。	Yes – フ No（既 ん。
ScanBootSectors	ブートセクタースキャンを指定します。	Yes（既 ンしま No – ブ ん。
ScanComputerMemory	プロセスメモリとカーネルメモリのスキャンを指定します。	Yes（既 ルメモ No – プ スキャ
ScanStartupObjects	スタートアップオブジェクトのスキャンを指定します。	Yes（既 クトを No – ス ャンし
ScanArchived	アーカイブ（自己解凍型アーカイブを含む）のスキャンを指定します。 アプリケーションは次のアーカイブをスキャンします：.zip、.7z*、.7-z、.rar、.iso、.cab、.jar、.bz、.bz2、.tbz、.tbz2、.gz、.tgz、.arj。サポートされているアーカイブ形式のリストは、使用されている製品データベースによって異なります。	Yes（既 ます。I 指定さ 応じて、 含むア No – ア
ScanSfxArchived	自己解凍型アーカイブ（実行可能な解凍モジュールを含むアーカイブ）のみのスキャンを指定します。	Yes（既 キャン

		No – 自 ません。
ScanMailBases	Microsoft Outlook、Outlook Express、およびその他のメールクライアントのメールデータベースのスキャンを指定します。	Yes – メ キャン No（既 ァイル
ScanPlainMail	プレーンテキストのメールメッセージのスキャンを指定します。	Yes – プ ジをス No（既 ルメッ
SizeLimit	スキャン対象のオブジェクトの最大サイズ（メガバイト単位）。指定された値よりもスキャン対象のオブジェクトのサイズが大きい場合、オブジェクトはスキップされます。	0 ～ 99 0 – スキ 無制限 既定値
TimeLimit	オブジェクトの最大スキャン時間（秒単位）。この設定で指定された時間よりもスキャンの時間がかかる場合、そのオブジェクトのスキャンが停止されます。	0～999 0 – オフ です。 既定値
FirstAction	感染したオブジェクトに対して実行される最初の処理の選択。	Disinf し、そ す。駆除 別または 除できな 更され ［Disi ［Seco 処理を指 Remove アップ を削除 Recomm オブジ 報に基づ に選択 の木馬や Security イの木馬 なく、駆 Skip – は削除や トに関す 既定値
SecondAction	感染したオブジェクトに対して実行される次の処理の選択。最初の処理に失敗した場合に、次の処理を実行します。	Second FirstA Skip ま 選択され はありま つの処理 指定しな 適用され

		既定値
UseExcludeMasks	ExcludeMasks.item_# 設定で指定されたオブジェクトのスキャン除外を有効にします。	Yes – E された ます。 No（既 定で指 ら除外
ExcludeMasks.item_#	名前またはマスクにより、オブジェクトをスキャンから除外します。この設定を使用すると、指定されたスキャン範囲から名前によって個別のファイルを除外したり、シェル形式でマスクを使用して複数のファイルを除外したりできます。 この設定の値を指定する前に、UseExcludeMasks 設定が有効になっていることを確認します。	既定値 例： UseE Excl Excl
UseExcludeThreats	ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトのスキャン除外を有効にします。	Yes – E 定され ンから No（既 設定で をスキ
ExcludeThreats.item_#	オブジェクト内で検知された脅威の名前によってスキャンからオブジェクトを除外します。この設定の値を指定する前に、UseExcludeThreats 設定が有効になっていることを確認します。 スキャンから単一オブジェクトを除外するには、このオブジェクト内で検知された脅威の完全な名前（このオブジェクトが感染していると判定した際に使用された名前の文字列）を指定します。 たとえば、ネットワークに関する情報を収集するユーティリティを使用している場合があります。これをブロックしないようにするには、スキャンから除外される脅威のリストに、製品で使用される脅威の完全な名前を追加します。 オブジェクトで検知された脅威のフルネームは、アプリケーションログや https://threats.kaspersky.com の Web サイトで確認することができます。	設定値 す。 既定値 例： UseE Excl Test Excl roja
UseGlobalExclusions	スキャンのグローバル除外を有効にします。	Yes（ ます。 No – グ
UseOASExclusions	スキャン時にファイル脅威対策の除外を有効にします。	はい（ を使用 いいえ しませ
ReportCleanObjects	感染していないとレポートされたスキャン済みオブジェクトに関する情報のログへの記録を指定します。 この設定は、たとえば特定のオブジェクトがスキャン済みであることを確認するために有効にします。	Yes – る情報 No（既 クトに
ReportPackedObjects	複合オブジェクトの一部を構成するスキャン済みオブジェクトに関する情報のログへの記録を指定します。 この設定は、たとえばアーカイブ内のオブジェクトがスキャン済みであることを確認するために有効にします。	Yes – ェクト

		No（既 済みオ 録しま
ReportUnprocessedObjects	何らかの理由により処理されていないオブジェクトに関する情報のログへの記録を指定します。	Yes – 処 する情 No（既 ェクトは ん。
UseAnalyzer	ヒューリスティック分析を指定します。 ヒューリスティック分析により、新しい脅威がウイルスアナリストに知られるようになる前に検知することができます。	Yes（既 を有効に No – ヒ ます。
HeuristicLevel	ヒューリスティック分析のレベルを指定します。 ヒューリスティック分析のレベルを指定できます。ヒューリスティック分析レベルは、脅威の検索範囲とオペレーティングシステムのリソースに対する負荷およびスキャンの所要時間のバランスを設定します。ヒューリスティック分析レベルが高いほど、スキャンに必要なリソースと時間が増加します。	Light い、シ Medium レベル が取れ Deep – ステム Recomm
UseIChecker	iChecker 技術の使用を指定します。	Yes（既 効にし No – iC す。
DeviceNameMasks.item_#	デバイス名のリスト。本製品はこれらのデバイスのブートセクターをスキャンします。 この設定値は空白にはできません。このタスクを実行するには、デバイス名マスクを少なくとも1つ設定する必要があります。	AllObj セクター < デバ と名前 ーをス 既定値 文字。
[ScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	スキャン範囲の説明。スキャン範囲に関する詳細情報を含みます。この設定を使用して指定される文字列の最大長は 4096 文字です。	既定値 例： Area
UseScanArea	指定された範囲のスキャンを指定します。タスクを実行するには、少なくとも1つの範囲のスキャンを有効にします。	Yes（既 ンしま No – 指 ん。
AreaMask.item_#	スキャン範囲の制限。スキャン範囲内で、シェル形式のマスクを使用して指定したファイルのみをスキャンします。 この設定が指定されていない場合、スキャン範囲のすべてのオブジェクトがスキャンされます。この設定には、複数の値を指定できます。	既定値 ャン） 例： Area

Path	スキャンされるオブジェクトがあるディレクトリのパス。	< ロー れたデ ンしま Shared クセス リソー Shared てアク テムリ Mounte てデバ レクト Mounte してデ ィレク AllRem と NFS マウン トリを AllSha ロトコ スのす スキャ < ファ バイス ースを
[ExcludedFromScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	スキャンの除外範囲の説明。除外範囲に関する詳細情報を含みます。	既定値
UseScanArea	指定された範囲のスキャンの除外を指定します。	Yes（ ます。 No – 指
AreaMask.item_#	スキャンの除外範囲の制限。除外範囲で、シェル形式のマスクを使用して指定したファイルのみを除外します。 この設定が指定されていない場合、除外範囲のすべてのオブジェクトが除外されます。この設定には、複数の値を指定できます。	既定値 外）。
Path	除外するオブジェクトを含むディレクトリのパス。	< ロー れたデ ンから 使用で

アスク
ファイ
スクネ

ファイ
「/」
文字列
「*」
ます。
「/d

2つの
ル名ま
「/」
列（C
す。低
「/d

アスク
「**
クト
とえば
適切な

ファイ
は、
示でき

スキャン
に、シス
でマウン
パスを、
し、現在
ている
奨しま
をベー
を追加で
す：/.

< ローカ
れたデー
む）の
ます。パ
す。

アス
ファ
スク

ファ
「/」
文字
「*」
ます。
「/d

2つの
ル名
「/」
列（C
す。
「/d

アス
「**
クト
とえ
適切

ファ
は、
示で

スキャ
に、シ
でマウ
パスを、
し、現
ている
奨しま
をベー
を追加
す：/.

Mounte
てデバ
ートデ
す。

Mounte
してデ
ィレク

AllRem
と NFS
マウン
トリを

<ファ
バイス
ースを

		リモ- 始前 み、 から マウ はス

リムーバブルドライブのスキャン

Kaspersky Endpoint Security は、保護対象デバイスが接続されたときに次のリムーバブルドライブをスキャンできます：CD、DVD、Blu-ray ディスク、フラッシュドライブ（USB モデムを含む）、外付けハードディスク、フロッピーディスク。

リムーバブルドライブのスキャンが有効になっている場合、Kaspersky Endpoint Security は、保護対象デバイスへのリムーバブルドライブの接続を監視し、接続されたリムーバブル ドライブが検知されると、ドライブとそのブートセクタをスキャンしてウイルスやその他のマルウェアがないか確認します。

デフォルトでは、アプリケーションはリムーバブルドライブの接続を監視したり、スキャンしたりしません。

この機能は、KESL コンテナではサポートされていません。

Web コンソールでのリムーバブルドライブのスキャンの設定

Web コンソールでは、ポリシーのプロパティでリムーバブルドライブのスキャンの設定を構成できます（**製品設定 → ローカルタスク → リムーバブルドライブのスキャン**）。

リムーバブルドライブスキャンのコンポーネント設定

設定	説明
リムーバブルドライブスキャンの有効化 / 無効化	このオプションでは、リムーバブルドライブをユーザーデバイスに接続した時にスキャンするかどうかを選択します。 この切り替えボタンは既定でオフになっています。
リムーバブルドライブの接続時の処理	ドロップダウンリストで、リムーバブルドライブをユーザーデバイスに接続した時に実行される処理を選択します。 • **スキャンしない** - 接続時にリムーバブルドライブをスキャンしません（既定値）。 • **簡易スキャン** - リムーバブルドライブ（CD ドライブ、DVD ドライブ、Blu-ray ディスクを除く）の特定の種別のファイルのみをスキャンし、複合ファイルの解凍は行いません。簡易スキャンは、*簡易スキャンタスク*の既定を使用して実行されます。 リムーバブルドライブでは、次のファイル形式がスキャンされます：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hta、asp、chm、pht、wsh、wsf、the、hip、eml、nws、msg、pig、mbx、doc*、dot*、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。 • **詳細スキャン** - リムーバブルドライブ（CD ドライブ、DVD ドライブ、Blu-ray ディスクを除く）のすべてのファイルをスキャンします。詳細スキャンは、*マルウェアのスキャンタスク*の既定を使用して実行されます。
CD / DVD ドライブの接続時の処理	このドロップダウンリストでは、CD ドライブ、DVD ドライブ、Blu-ray ディスクをユーザーデバイスに接続した時に実行する処理を選択します： • **スキャンしない** - 接続時に CD ドライブ、DVD ドライブ、Blu-ray ディスクをスキャンしません（既定値）。

	• **簡易スキャン**：CD ドライブ、DVD ドライブ、Blu-ray ディスクの特定の種別のファイルのみをスキャンします。簡易スキャンは、*簡易スキャンタスク*の既定を使用して実行されます。 リムーバブルドライブでは、次のファイル形式がスキャンされます：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hta、asp、chm、pht、wsh、wsf、the、hip、eml、nws、msg、pig、mbx、doc*、dot*、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。 • **詳細スキャン**：CD ドライブ、DVD ドライブ、Blu-ray ディスクのすべてのファイルをスキャンします。詳細スキャンは、*マルウェアのスキャンタスク*の既定を使用して実行されます。
スキャン中はリムーバブルドライブへのアクセスをブロックする	このチェックボックスは、スキャンの実行中に接続されたドライブ上のファイルのブロックを有効または無効にします。 既定では、このチェックボックスはオフです。

管理コンソールでのリムーバブルドライブのスキャンの設定

管理コンソールでは、ポリシーのプロパティでリムーバブルドライブのスキャンの設定を構成できます（製品設定 → **ローカルタスク → リムーバブルドライブのスキャン**）。

リムーバブルドライブスキャンのコンポーネント設定

設定	説明
デバイスへの接続時にリムーバブルドライブのスキャンを有効にします	このチェックボックスでは、リムーバブルドライブをユーザーデバイスに接続した時にスキャンするかどうかを選択します。 既定では、このチェックボックスはオフです。
リムーバブルドライブの接続時の処理	ドロップダウンリストで、リムーバブルドライブをユーザーデバイスに接続した時に実行される処理を選択します。 • **スキャンしない** - 接続時にリムーバブルドライブをスキャンしません（既定値）。 • **簡易スキャン** - リムーバブルドライブ（CD ドライブ、DVD ドライブ、Blu-ray ディスクを除く）の特定の種別のファイルのみをスキャンし、複合ファイルの解凍は行いません。簡易スキャンは、*簡易スキャンタスク*の既定を使用して実行されます。 リムーバブルドライブでは、次のファイル形式がスキャンされます：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hta、asp、chm、pht、wsh、wsf、the、hip、eml、nws、msg、pig、mbx、doc*、dot*、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。

	• **詳細スキャン** - リムーバブルドライブ（CD ドライブ、DVD ドライブ、Blu-ray ディスクを除く）のすべてのファイルをスキャンします。詳細スキャンは、 *マルウェアのスキャンタスクの既定を使用して実行されます。*
CD / DVD ドライブの接続時の処理	このドロップダウンリストでは、CD ドライブ、DVD ドライブ、Blu-ray ディスクをユーザーデバイスに接続した時に実行する処理を選択します： • **スキャンしない** - 接続時に CD ドライブ、DVD ドライブ、Blu-ray ディスクをスキャンしません（既定値）。 • **簡易スキャン**：CD ドライブ、DVD ドライブ、Blu-ray ディスクの特定の種別のファイルのみをスキャンします。簡易スキャンは、*簡易スキャンタスクの既定を使用して実行されます。* リムーバブルドライブでは、次のファイル形式がスキャンされます：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hta、asp、chm、pht、wsh、wsf、the、hip、eml、nws、msg、pig、mbx、doc*、dot*、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。 • **詳細スキャン**：CD ドライブ、DVD ドライブ、Blu-ray ディスクのすべてのファイルをスキャンします。詳細スキャンは、 *マルウェアのスキャンタスクの既定を使用して実行されます。*
スキャン中はリムーバブルドライブへのアクセスをブロックする	このチェックボックスは、スキャンの実行中に接続されたドライブ上のファイルのブロックを有効または無効にします。 既定では、このチェックボックスはオフです。

コマンドラインでのリムーバブルドライブのスキャンの設定

コマンドラインでは、リムーバブルドライブのスキャンの事前定義済みタスク（*Removable_Drives_Scan*）を使用して、リムーバブルドライブのスキャンを管理できます。

既定では、リムーバブルドライブのスキャンタスクが停止されます。このタスクは、手動で開始および停止できます。このタスクの設定を編集することで、スキャン設定を構成できます。

タスクが実行中の場合、アプリケーションはデバイスへのリムーバブルドライブの接続を監視し、リムーバブルドライブが接続されると、一時的なブートセクタースキャンタスク（*ODS* タイプのタスク）を作成して開始します。このタスクは停止できません。タスクの実行が完了すると、そのタスクは自動的に削除されます。

リムーバブルドライブのスキャンタスク設定でファイル スキャンを有効にした場合、アプリケーションは1つ以上の一時的なカスタムファイルスキャンタスク（*ODS* タイプのタスク）も開始します。必要に応じて、管理者権限を持つユーザーはこれらのタスクを停止できます。

リムーバブルドライブのスキャンタスクの設定を変更した場合、新しい値はすでに実行されている一時タスクには適用されません。リムーバブルドライブのスキャンタスクを停止しても、すでに実行中の一時タスクは停止しません。

リムーバブルドライブのスキャンタスクの設定

設定	説明	値
ScanRemovableDrives	デバイス接続時のリムーバブルドライブのスキャンを指定します。 この設定は、CD/DVD ドライブおよび Blu-ray ディスクには適用されません（ScanOpticalDrives 設定を参照してください）。	DetailedScan - リムーバブルドライブ（CD ドライブ、DVD ドライブ、Blu-ray ディスクを除く）のすべてのファイルをスキャンします。 詳細スキャンは、*Scan_File* タスク (ID: 3) の既定で実行されます。 QuickScan - リムーバブルドライブ（CD ドライブ、DVD ドライブ、Blu-ray ディスクを除く）の特定の種別のファイルのみをスキャンします。 リムーバブルドライブでは、次のファイル形式がスキャンされます：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hta、asp、chm、pht、wsh、wsf、the、hip、eml、nws、msg、pig、mbx、doc*、dot*、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。 クイックスキャンは、*Critical_Areas_Scan* タスク (ID: 4) の既定で実行されます。 NoScan（既定値） - リムーバブルドライブの接続時にスキャンを実行しません。
ScanOpticalDrives	デバイス接続時の CD/DVD ドライブと Blu-ray ディスクのスキャンを指定します。	DetailedScan - CD/DVD ドライブ、Blu-ray ディスクのすべてのファイルをスキャンします。 詳細スキャンは、*Scan_File* タスク (ID: 3) の既定で実行されます。 QuickScan - CD/DVD ドライブ、Blu-ray ディスクの特定の種別のファイルのみをスキャンします。 リムーバブルドライブでは、次のファイル形式がスキャンされます：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hta、asp、chm、pht、wsh、wsf、the、hip、eml、nws、msg、pig、mbx、doc*、dot*、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。 クイックスキャンは、*Critical_Areas_Scan* タスク (ID: 4) の既定で実行されます。 NoScan（既定値） - CD/DVD ドライブ、Blu-ray ディスクの接続時にスキャンを実行しません。
BlockDuringScan	スキャン中に接続されたディスク上のファイルのブロックを指定します。ブートセクタースキャン中は、ファイ	Yes - スキャン中にファイルをブロックします。 No（既定値） - スキャン中にファイルをブロックしません。

	ルはブロックされません。	

コンテナースキャン

コンテナとイメージのマルウェアをリアルタイムかつオンデマンドでスキャンできます。

- *コンテナ監視*コンポーネントを使用すると、起動されたコンテナと名前空間をリアルタイムでスキャンできます。
- *コンテナースキャン*タスクを使用して、コンテナとイメージをオンデマンドでスキャンできます。

Docker コンテナ管理システム、CRI-O フレームワーク、Podman ユーティリティ、runc ユーティリティとのアプリケーションの連携に対応しています。

コンテナスキャンタスクを使用するには、この機能を含むライセンスが必要です。

コンテナの監視

コンテナ監視コンポーネントは既定で有効になっています。アプリケーションは、実行中のコンテナと名前空間をリアルタイムでスキャンします。

コンテナ監視コンポーネントが機能するには、ファイル脅威対策コンポーネントが有効になっている必要があります。ファイル脅威対策設定は、コンテナと名前空間をスキャンするときに使用されます。

コンテナと名前空間を操作するためのコンポーネントがオペレーティングシステムにインストールされていない限り、アプリケーションは名前空間とコンテナをスキャンしません。この場合、コマンドラインのコンテナ監視のコンポーネントのステータスは「タスクは利用可能ですが実行されていません」と表示されますが、Kaspersky Security Center では「停止」と表示されます。

コンテナ監視コンポーネントを有効または無効にしたり、コンテナと名前空間をリアルタイムでスキャンするための設定を構成したりできます。

- 感染したオブジェクトを検知した際に、本製品がコンテナに対して実行する処理を選択します。

  この設定は、この機能をサポートするライセンスでアプリケーションを使用する場合に使用できます。

- Kaspersky Endpoint Security と Docker コンテナ管理システム、CRI-O フレームワーク、Podman および runc ユーティリティとの連携を設定します。

Web コンソールからのコンテナ監視の設定

Web コンソールでは、ポリシーのプロパティで *コンテナ監視*コンポーネントの動作を管理できます（**製品設定 → 全般設定 → コンテナースキャン設定**）。

コンテナの監視設定

設定	説明
名前空間とコンテナースキャンの有効化 / 無効化	この切り替えボタンは、名前空間とコンテナのリアルタイムのスキャンを有効または無効にします。 この切り替えボタンは既定でオンになっています。
脅威の検知時のコンテナに対する処理	感染したオブジェクトを検知した際に、本製品がコンテナに対して実行する処理を選択することができます： • **コンテナをスキップ**：感染したオブジェクトが検知されても、コンテナに対して何の処理も実行しません。 • **コンテナを停止**：感染したオブジェクトが検知された場合、コンテナを停止します。 • **駆除できなかった場合はコンテナを停止**（既定値） - 感染したオブジェクトの駆除が失敗した場合はコンテナを停止します。 この設定は、この機能をサポートするライセンスでアプリケーションを使用する場合に使用できます。
Docker を使用	このチェックボックスでは、Docker 環境を使用するかどうかを選択できます。 既定では、このチェックボックスはオンです。
Docker ソケットのパス	Docker ソケットのパスまたは URI（ユニバーサルリソース識別子）を入力するフィールド。 既定値：/var/run/docker.sock
CRI-O を使用	このチェックボックスでは、CRI-O 環境を使用するかどうかを選択できます。 既定では、このチェックボックスはオンです。
ファイルパス	CRI-O 設定情報ファイルのパスを入力するフィールド。 既定値：/etc/crio/crio.conf
Podman を使用	このチェックボックスでは、Podman ユーティリティを使用するかどうかを選択できます。 既定では、このチェックボックスはオンです。
ファイルパス	Podman ユーティリティの実行ファイルへのパスを入力するフィールド。 既定値：/usr/bin/podman
ルートディレクトリ	コンテナの保管領域のルートディレクトリへのパスを入力するフィールド。 既定値：/var/lib/containers/storage
runc を使用	このチェックボックスでは、runc ユーティリティを使用するかどうかを選択できます。 既定では、このチェックボックスはオンです。
ファイルパス	runc ユーティリティ実行ファイルへのパスを入力するフィールド。 既定値：/usr/bin/runc
ルートディレクトリ	コンテナ状態の保管領域のルートディレクトリへのパスを入力するフィールド。 既定値：/run/runc.

管理コンソールからのコンテナ監視の設定

管理コンソールでは、ポリシーのプロパティでコンテナ監視コンポーネントの動作を管理できます（アプリケーション設定 → **全般設定** → **コンテナースキャン設定**）。

コンテナの監視設定

設定	説明
名前空間とコンテナースキャンを有効にする	このチェック ボックスは、名前空間とコンテナのリアルタイムのスキャンを有効または無効にします。 既定では、このチェックボックスはオンです。
脅威の検知時のコンテナに対する処理	ドロップダウンリストで、感染したオブジェクトの検知時にコンテナに対して実行する処理を選択します： • **コンテナをスキップ**：感染したオブジェクトが検知されても、コンテナに対して何の処理も実行しません。 • **コンテナを停止**：感染したオブジェクトが検知された場合、コンテナを停止します。 • **駆除できなかった場合はコンテナを停止**（既定値） - 感染したオブジェクトの駆除が失敗した場合はコンテナを停止します。 この設定は、この機能をサポートするライセンスでアプリケーションを使用する場合に使用できます。
コンテナースキャン設定	設定のグループには、［**設定**］が含まれています。このボタンをクリックすると、［**コンテナースキャン設定**］ウィンドウが表示されます。

［コンテナースキャン設定］ウィンドウ

このウィンドウでは、Kaspersky Endpoint Security を Docker コンテナ管理システム、CRI-O 環境、Podman および runc ユーティリティと統合するための設定を編集できます。

コンテナースキャン設定

設定	説明
Docker を使用	このチェックボックスでは、Docker 環境を使用するかどうかを選択できます。 既定では、このチェックボックスはオンです。
Docker ソケットのパス	Docker ソケットのパスまたは URI（ユニバーサルリソース識別子）を入力するフィールド。 既定値：/var/run/docker.sock
CRI-O を使用	このチェックボックスでは、CRI-O 環境を使用するかどうかを選択できます。 既定では、このチェックボックスはオンです。
ファイルパス	CRI-O 設定情報ファイルのパスを入力するフィールド。 既定値：/etc/crio/crio.conf

Podman を使用	このチェックボックスでは、Podman ユーティリティを使用するかどうかを選択できます。 既定では、このチェックボックスはオンです。
ファイルパス	Podman ユーティリティの実行ファイルへのパスを入力するフィールド。 既定値：/usr/bin/podman
ルートディレクトリ	コンテナの保管領域のルートディレクトリへのパスを入力するフィールド。
runc を使用	このチェックボックスでは、runc ユーティリティを使用するかどうかを選択できます。 既定では、このチェックボックスはオンです。
ファイルパス	runc ユーティリティ実行ファイルへのパスを入力するフィールド。 既定値：/usr/bin/runc
ルートディレクトリ	コンテナ状態の保管領域のルートディレクトリへのパスを入力するフィールド。 既定値：/run/runc.

コマンドラインからのコンテナ監視の設定

コマンドラインでは、アプリケーションの全般設定の `NamespaceMonitoring=Yes/No` 設定を使用して、名前空間とコンテナのリアルタイムスキャンを有効または無効にできます。

アプリケーション全般設定をすべて含む設定情報ファイルを使用するか、コマンドラインキーを使用して、`NamespaceMonitoring` 設定の値を編集できます。

名前空間とコンテナをリアルタイムでスキャンする場合、コンテナースキャンの全般設定が使用されます。特別な Kaspersky Endpoint Security 管理コマンドを使用して、これらの設定を表示および編集できます。

- コンテナースキャンの全般設定の現在の値をコンソールまたは設定情報ファイルに出力できます。このファイルを使用して設定を編集できます。
- 設定を含む設定情報ファイルを使用して、コンテナースキャンの全般設定をすべて編集できます。コンテナースキャンの全般設定を表示するコマンドを使用して、設定情報ファイルを取得できます。
- コマンドラインキーを使用して、< 設定名 >=< 設定値 > の形式で個々の設定を編集できます。コンテナースキャンの全般設定を表示するコマンドを使って設定の現在の値を取得できます。

コンテナースキャンの全般設定の現在の値をコンソールに出力するには、次のコマンドを実行します：

```
kesl-control --get-container-settings [--json]
```

`--json` を指定すると、設定はJSON形式で出力されます。もし `--json` キーが指定されなければ、設定はINI形式でインポートされます。

コンテナースキャンの全般設定の現在の値をファイルに出力するには、次のコマンドを実行します：

```
kesl-control --get-container-settings --file <設定情報ファイルへのパス> [--json]
```

説明：

- `--file <`設定情報ファイルへのパス`>` は、コンテナースキャンの全般設定が保存されるファイルへのパスです。パスを指定しないでファイルの名前を指定した場合、そのファイルは現在のディレクトリに作成されます。指定された名前のファイルが指定されたパスに既に存在する場合は、上書きされます。指定されたディレクトリがディスクに見つからない場合、ファイルは作成されません。

- `--json` を指定すると、設定はJSON形式で出力されます。もし `--json` キーが指定されなければ、設定はINI形式でインポートされます。

設定情報ファイルを使用してコンテナースキャンの全般設定の値を編集するには、次の手順を実行します：

1. 上で説明したように、一般的なコンテナースキャン設定を設定情報ファイルに出力します。

2. ファイル内の必要なパラメータの値を編集し、変更を保存します。

3. コマンドを実行します：

   `kesl-control --set-container-settings --file <`設定情報ファイルへのパス`> [--json]`

   説明：

   - `--file <`設定情報ファイルへのパス`>` は、コンテナースキャンの全般設定が含まれる設定情報ファイルへの絶対パスです。

   - `--json`：JSON形式の設定情報ファイルから設定をインポートする場合は、このライセンスを指定します。`--jason` のライセンスが指定されていない場合、設定はINIファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

   ファイルで定義されたコンテナースキャンの全般設定のすべての値がアプリケーションにインポートされます。

コマンドラインキーを使ってコンテナースキャンの全般設定の値を編集するには、次のコマンドを実行します：

`kesl-control --set-container-settings <`設定名`>=<`設定値`> [<`設定名`>=<`設定値`>]`

`<`設定名`>=<`設定値`>`は、コンテナースキャンの全般設定の1つの名前と値です。

指定されたコンテナースキャンの全般設定の値が変更されます。

コンテナとイメージのオンデマンドスキャン

*コンテナースキャンタスク*が実行されている場合、Kaspersky Endpoint Securityはコンテナとイメージをスキャンしてウイルスやその他のマルウェアを検知します。本製品は、複数のコンテナースキャンタスクを同時実行できます。

Dockerコンテナ管理システム、CRI-Oフレームワーク、Podmanユーティリティ、runcユーティリティとの連携がサポートされています。

このタスクを使用するには、対応する機能を含むライセンスが要求されます。

コンテナースキャンを開始し、スキャンの設定を構成できます。

- スキャンするコンテナとイメージを名前または名前マスクで指定します。

- イメージとコンテナの全レイヤーのスキャンを有効にします。
- 感染オブジェクトが検知されたときにアプリケーションがコンテナに対して実行する処理と、アプリケーションがイメージに対して実行する処理を選択します。
- コンテナまたはイメージ内のオブジェクトをスキャンするための設定を構成します：
  - アーカイブ、メールデータベース、テキスト形式の電子メールメッセージのスキャンを有効または無効にします。
  - スキャンするオブジェクトのサイズとオブジェクトのスキャン時間を制限します。
  - 感染したオブジェクトに対して実行される処理を選択します。
  - スキャンからのオブジェクトの除外を設定します：
    - 名前またはマスクに基づく
    - オブジェクトで検知された脅威の名前に基づく
  - スキャン時にグローバル除外の使用を有効または無効にします。
  - スキャン中のヒューリスティック分析と iChecker テクノロジーの使用を設定します。
  - スキャンされた非感染オブジェクト、アーカイブ内のスキャンオブジェクト、および未処理のオブジェクトに関する情報のログ記録を有効または無効にします。

Web コンソールでのコンテナースキャン

Web コンソールでは、*コンテナスのキャンタスク*を使用してコンテナとイメージをスキャンできます。

コンテナのスキャンのユーザータスクを作成し、実行できます。タスクの設定を編集してスキャン設定を管理できます。

コンテナのスキャンタスクの設定

設定	説明
アーカイブをスキャン	このチェックボックスでは、アーカイブをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、アーカイブがスキャンされます。 アーカイブをスキャンするには、アーカイブを解凍する必要があるためスキャン速度が遅くなる可能性があります。［**スキャンの全般設定**］セクションの［**スキャン時間が次を超えたらファイルをスキップする（秒）**］および［**ファイルのサイズが次を超えたらスキップする（MB）**］を設定すると、アーカイブのスキャンの所要時間を減らすことができます。 このチェックボックスをオフにすると、アーカイブはスキャンされません。 既定では、このチェックボックスはオンです。
SFX アーカイブをスキャン	このチェックボックスでは、*自己解凍アーカイブ*をスキャンするかどうかを選択します。自己解凍アーカイブとは、実行可能な展開モジュールを含むアーカイブです。 このチェックボックスをオンにすると、自己解凍アーカイブがスキャンされます。 このチェックボックスをオフにすると、自己解凍アーカイブはスキャンされません。 このチェックボックスは、［**アーカイブをスキャン**］がオフの場合に使用できます。

	既定では、このチェックボックスはオンです。
メールデータベースをスキャン	このチェックボックスでは、Microsoft Outlook、Outlook Express などのメールアプリケーションのメールデータベースをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、メールデータベースはスキャンされます。 このチェックボックスをオフにすると、メールデータベースはスキャンされません。 既定では、このチェックボックスはオフです。
メール形式のファイルをスキャン	このチェックボックスでは、プレーンテキストのメールメッセージのファイルをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、プレーンテキストのメッセージがスキャンされます。 このチェックボックスをオフにすると、プレーンテキストのメッセージはスキャンされません。 既定では、このチェックボックスはオフです。
スキャン時間が次を超えたらファイルをスキップする（秒）	このフィールドでは、ファイルをスキャンする最大時間を秒単位で指定できます。指定した時間が経過した後、ファイルのスキャンは停止されます。 使用できる値：0 ～ 9999。値が 0 に設定されると、スキャン時間は制限されません。 既定値：0
ファイルのサイズが次を超えたらスキップする（MB）	このフィールドでは、スキャンするファイルの最大サイズをメガバイト単位で指定できます。 使用できる値：0 ～ 999999。値が 0 に設定されると、サイズにかかわらず、すべてのファイルがスキャンされます。 既定値：0
感染していないオブジェクトを記録する	このチェックボックスでは、*ObjectProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、スキャンされたすべてのオブジェクトの *ObjectProcessed* タイプのイベントをログに記録します。 このチェックボックスをオフにすると、スキャンされたオブジェクトの *ObjectProcessed* タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
処理されていないオブジェクトを記録する	このチェックボックスでは、スキャン中にファイルを処理できない場合、*ObjectNotProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、［*ObjectNotProcessed*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*ObjectNotProcessed*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
圧縮されたオブジェクトを記録する	このチェックボックスでは、検出されたすべての圧縮されたオブジェクトに関する *PackedObjectDetected* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、［*PackedObjectDetected*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*PackedObjectDetected*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
iChecker 技術を使用する	このチェックボックスでは、前回のファイルのスキャン以降の新しいファイルおよび変更されたファイルのみをスキャンするかどうかを選択します。

	このチェックボックスをオンにすると、前回のスキャン以降の新しいファイルおよび変更されたファイルのみがスキャンされます。 このチェックボックスをオフにすると、作成日または変更日に関係なくファイルがスキャンされます。 既定では、このチェックボックスはオンです。
ヒューリスティック分析を使用する	このチェックボックスでは、ファイルのスキャン中にヒューリスティック分析を使用するかどうかを選択します。 既定では、このチェックボックスはオンです。
ヒューリスティック分析のレベル	［**ヒューリスティック分析を使用する**］をオンにすると、ドロップダウンリストでヒューリスティック分析レベルを選択できます。 • **低**：スキャンの詳細レベルが最も低く、システム負荷は最小です。 • **中**：スキャンの詳細レベルは中程度で、システム負荷のバランスが取れています。 • **高**：スキャンの詳細レベルが最も高く、システム負荷は最大です。 • **推奨**（既定値）：カスペルスキーが推奨する、最適なレベルです。保護品質と保護対象デバイスの性能への影響の最適な組み合わせを保証します。
最初の処理	このドロップダウンリストでは、感染したオブジェクトの検知時に実行する最初の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています（既定値）。 • **スキップ**：オブジェクトをスキップします。
次の処理	このドロップダウンリストでは、感染したオブジェクトに対する最初の処理が成功しなかった場合に実行する次の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています。 • **スキップ**：オブジェクトをスキップします（既定値）。
コンテナースキャン	このチェックボックスでは、コンテナをスキャンするかどうかを選択します。チェックボックスがオンの場合、スキャン対象に含めるコンテナの名前または名前のマスクを指定できます。 既定では、このチェックボックスはオンです。

名前のマスク	スキャン対象に含めるコンテナの名前または名前のマスクを入力するフィールド。 既定では、「*」というマスクが指定されています。これは、すべてのコンテナがスキャン対象となります。
脅威の検知時の処理	感染したオブジェクトを検知した際に、本製品がコンテナに対して実行する処理を選択することができます： • **コンテナをスキップ** – 感染したオブジェクトが検知されても、コンテナに対して何の処理も実行しません。 • **コンテナを停止** – 感染したオブジェクトが検知された場合、コンテナを停止します。 • **駆除できなかった場合はコンテナを停止**（既定値） – 感染したオブジェクトの駆除、または脅威の除去に失敗した場合はコンテナを停止します。 CRI-O 環境の仕組みにより、感染したオブジェクトは CRI-O 環境のコンテナ内で駆除または削除されません。［**コンテナを停止**］操作を選択することを推奨します。
イメージをスキャン	このチェックボックスでは、イメージをスキャンするかどうかを選択します。このチェックボックスをオンにすると、スキャン対象に含めるイメージの名前または名前のマスクを指定できます。 既定では、このチェックボックスはオンです。
名前のマスク	スキャン対象に含めるイメージの名前または名前のマスクを入力するフィールド。 既定では、「*」というマスクが指定されています。これは、すべてのイメージがスキャン対象となります。
脅威の検知時の処理	感染したオブジェクトを検知した際に、本製品がコンテナに対して実行する処理を選択することができます： • **イメージをスキップ**（既定値） – 感染したオブジェクトが検知されても、イメージに対して何の処理も実行しません。 • **イメージを削除** – 感染したオブジェクトの検知時に、イメージを削除します（推奨しないオプションです）。すべての依存関係も削除されます。実行中のコンテナは停止され、それから削除されます。
各レイヤーをスキャン	このチェックボックスでは、イメージと実行中のコンテナのすべてのレイヤーのスキャンを行うかどうかを選択できます。 既定では、このチェックボックスはオフです。

［除外範囲］セクション

コンテナスキャンタスクの［**除外範囲**］セクションでは、マスクと脅威名による除外、およびタスク実行時のグローバル除外の使用を設定できます。

スキャンの除外の設定

設定	説明
除外をマスクで設定する	［**除外をマスクで設定する**］をクリックすると、［**マスクによる除外**］ウィンドウが表示されます。このウィンドウでは、名前のマスクにより、スキャンからのオブジェクトの除外を設定できます。

除外を脅威名で設定する	［**除外を脅威名で設定する**］をクリックすると、［**脅威の名前による除外**］ウィンドウが表示されます。このウィンドウでは、脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。
グローバル除外リストを使用	チェックボックスは、本製品の実行中にグローバル例外で指定されたマウントポイントの除外を有効または無効にします。 チェックボックスをオンにすると、設定されたマウントポイントをスキャンから除外します。 既定では、このチェックボックスはオンです。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、スキャンからのオブジェクトの除外を設定できます。指定したマスクが名前に含まれるファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［脅威の名前による除外］ウィンドウ

脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。指定された脅威はブロックされません。既定では、脅威の名前のリストは空です。

脅威の名前は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した脅威が除外リストから削除されます。

このボタンは、少なくとも1つの脅威の名前をリストから選択している場合に使用できます。

表内の脅威の名前をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を編集できます。

［**追加**］をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を指定できます。

管理コンソールでのコンテナースキャン

管理コンソールでは、*コンテナスのキャンタスク*を使用してコンテナとイメージをスキャンできます。

コンテナースキャンのユーザータスクを作成し、実行できます。タスクの設定を編集してスキャン設定を管理できます。

［コンテナースキャン］タスクのプロパティの［**設定**］セクションでは、次の表に示す設定を構成できます。

コンテナのスキャンタスクの設定

設定	説明
スキャン	この設定グループには、［コンテナのスキャン設定］と［スキャンの全般設定］を設定できるウィンドウを開くボタンが含まれています。
脅威の検知時の処理	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**脅威の検知時の処理**］ウィンドウが表示され、検知された感染オブジェクトに対して実行する処理を設定できます。

タスクプロパティの［**除外**］セクションでは、コンテナースキャンタスクの除外をマスクや脅威の名前で設定することもできます。

［コンテナースキャン設定］ウィンドウ

このウィンドウでは、コンテナとイメージのスキャンを設定します。

コンテナとイメージのスキャン設定

設定	説明
コンテナースキャン	このチェックボックスでは、コンテナをスキャンするかどうかを選択します。チェックボックスがオンの場合、スキャン対象に含めるコンテナの名前または名前のマスクを指定できます。 既定では、このチェックボックスはオンです。
名前のマスク	スキャン対象に含めるコンテナの名前または名前のマスクを入力するフィールド。 既定では、「*」というマスクが指定されています。これは、すべてのコンテナがスキャン対象となります。
脅威の	ドロップダウンリストで、感染したオブジェクトの検知時にコンテナに対して実行する処理

検知時の処理	を選択します： • **コンテナをスキップ** – 感染したオブジェクトが検知されても、コンテナに対して何の処理も実行しません。 • **コンテナを停止** – 感染したオブジェクトが検知された場合、コンテナを停止します。 • **駆除できなかった場合はコンテナを停止**（既定値） – 感染したオブジェクトの駆除、または脅威の除去に失敗した場合はコンテナを停止します。 CRI-O 環境の仕組みにより、感染したオブジェクトは CRI-O 環境のコンテナ内で駆除または削除されません。［**コンテナを停止**］操作を選択することを推奨します。
イメージをスキャン	このチェックボックスでは、イメージをスキャンするかどうかを選択します。このチェックボックスをオンにすると、スキャン対象に含めるイメージの名前または名前のマスクを指定できます。 既定では、このチェックボックスはオンです。
名前のマスク	スキャン対象に含めるイメージの名前または名前のマスクを入力するフィールド。 既定では、「*」というマスクが指定されています。これは、すべてのイメージがスキャン対象となります。
脅威の検知時の処理	ドロップダウンリストで、感染したオブジェクトの検知時にイメージに対して実行する処理を選択します： • **イメージをスキップ**（既定値） – 感染したオブジェクトが検知されても、イメージに対して何の処理も実行しません。 • **イメージを削除** – 感染したオブジェクトの検知時に、イメージを削除します（推奨しないオプションです）。すべての依存関係も削除されます。実行中のコンテナは停止され、それから削除されます。
各レイヤーをスキャン	このチェックボックスでは、イメージと実行中のコンテナのすべてのレイヤーのスキャンを行うかどうかを選択できます。 既定では、このチェックボックスはオフです。

［スキャンの設定］ウィンドウ

このウィンドウでは、タスクのファイルスキャンを設定します。

スキャン設定

設定	説明
アーカイブをスキャン	このチェックボックスでは、アーカイブをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、アーカイブがスキャンされます。 アーカイブをスキャンするには、アーカイブを解凍する必要があるためスキャン速度が遅くなる可能性があります。［**スキャンの全般設定**］セクションの［**スキャン時間が次を超えたらファイルをスキップする（秒）**］および［**ファイルのサイズが次を超えたらスキップする（MB）**］を設定すると、アーカイブのスキャンの所要時間を減らすことができます。 このチェックボックスをオフにすると、アーカイブはスキャンされません。

	既定では、このチェックボックスはオンです。
SFX アーカイブをスキャン	このチェックボックスでは、*自己解凍アーカイブ*をスキャンするかどうかを選択します。自己解凍アーカイブとは、実行可能な展開モジュールを含むアーカイブです。 このチェックボックスをオンにすると、自己解凍アーカイブがスキャンされます。 このチェックボックスをオフにすると、自己解凍アーカイブはスキャンされません。 このチェックボックスは、［**アーカイブをスキャン**］がオフの場合に使用できます。 既定では、このチェックボックスはオンです。
メールデータベースをスキャン	このチェックボックスでは、Microsoft Outlook、Outlook Express などのメールアプリケーションのメールデータベースをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、メールデータベースはスキャンされます。 このチェックボックスをオフにすると、メールデータベースはスキャンされません。 既定では、このチェックボックスはオフです。
メール形式のファイルをスキャン	このチェックボックスでは、プレーンテキストのメールメッセージのファイルをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、プレーンテキストのメッセージがスキャンされます。 このチェックボックスをオフにすると、プレーンテキストのメッセージはスキャンされません。 既定では、このチェックボックスはオフです。
スキャン時間が次を超えたらファイルをスキップする（秒）	このフィールドでは、ファイルをスキャンする最大時間を秒単位で指定できます。指定した時間が経過した後、ファイルのスキャンは停止されます。 使用できる値：0 ～ 9999。値が 0 に設定されると、スキャン時間は制限されません。 既定値：0
ファイルのサイズが次を超えたらスキップする（MB）	このフィールドでは、スキャンするファイルの最大サイズをメガバイト単位で指定できます。 使用できる値：0 ～ 999999。値が 0 に設定されると、サイズにかかわらず、すべてのファイルがスキャンされます。 既定値：0
感染していないオブジェクトを記録する	このチェックボックスでは、*ObjectProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、スキャンされたすべてのオブジェクトの *ObjectProcessed* タイプのイベントをログに記録します。 このチェックボックスをオフにすると、スキャンされたオブジェクトの *ObjectProcessed* タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
処理されていないオブジェクトを記録する	このチェックボックスでは、スキャン中にファイルを処理できない場合、*ObjectNotProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、［*ObjectNotProcessed*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*ObjectNotProcessed*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
圧縮されたオブジェク	このチェックボックスでは、検出されたすべての圧縮されたオブジェクトに関する *PackedObjectDetected* タイプのイベントをログに記録するかどうかを選択します。

トを記録する	このチェックボックスをオンにすると、［*PackedObjectDetected*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*PackedObjectDetected*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
iChecker 技術を使用する	このチェックボックスでは、前回のファイルのスキャン以降の新しいファイルおよび変更されたファイルのみをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、前回のスキャン以降の新しいファイルおよび変更されたファイルのみがスキャンされます。 このチェックボックスをオフにすると、作成日または変更日に関係なくファイルがスキャンされます。 既定では、このチェックボックスはオンです。
ヒューリスティック分析を使用する	このチェックボックスでは、ファイルのスキャン中にヒューリスティック分析を使用するかどうかを選択します。 既定では、このチェックボックスはオンです。
ヒューリスティック分析のレベル	［**ヒューリスティック分析を使用する**］をオンにすると、ドロップダウンリストでヒューリスティック分析レベルを選択できます。 • **低**：スキャンの詳細レベルが最も低く、システム負荷は最小です。 • **中**：スキャンの詳細レベルは中程度で、システム負荷のバランスが取れています。 • **高**：スキャンの詳細レベルが最も高く、システム負荷は最大です。 • **推奨**（既定値）：カスペルスキーが推奨する、最適なレベルです。保護品質と保護対象デバイスの性能への影響の最適な組み合わせを保証します。

•

［脅威の検知時の処理］ウィンドウ

このウィンドウでは、検知された感染オブジェクトに対して実行する処理を設定できます：

脅威の検知時の処理

設定	説明
最初の処理	このドロップダウンリストでは、感染したオブジェクトの検知時に実行する最初の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています（既定値）。 • **スキップ**：オブジェクトをスキップします。

次の処理	このドロップダウンリストでは、感染したオブジェクトに対する最初の処理が成功しなかった場合に実行する次の処理を選択します： • **駆除**：オブジェクトを駆除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **削除**：オブジェクトを削除します。感染したオブジェクトのコピーがバックアップに移動されます。 • **推奨される処理を実行**：推奨される処理をオブジェクトに対して実行します。実行する処理は、ファイルの中で検知された脅威の危険度のデータと、駆除が可能かどうかに基づいています。 • **スキップ**：オブジェクトをスキップします（既定値）。

•

除外セクション

スキャンの除外の設定

設定のグループ	説明
マスクによる除外	この設定グループには［**設定**］が含まれています。クリックすると、［**マスクによる除外**］ウィンドウが表示されます。このウィンドウでは、名前のマスクにより、スキャンからのオブジェクトの除外を設定できます。
脅威の名前による除外	この設定グループには［**設定**］が含まれています。クリックすると、［**脅威の名前による除外**］ウィンドウが表示されます。このウィンドウでは、脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。
グローバル除外リストを使用	チェックボックスは、本製品の実行中にグローバル例外で指定されたマウントポイントの除外を有効または無効にします。 チェックボックスをオンにすると、設定されたマウントポイントをスキャンから除外します。 既定では、このチェックボックスはオンです。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、スキャンからのオブジェクトの除外を設定できます。指定したマスクが名前に含まれるファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［脅威の名前による除外］ウィンドウ

脅威の名前に基づいて、スキャンからのオブジェクトの除外を設定できます。指定された脅威はブロックされません。既定では、脅威の名前のリストは空です。

脅威の名前は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した脅威が除外リストから削除されます。

このボタンは、少なくとも1つの脅威の名前をリストから選択している場合に使用できます。

表内の脅威の名前をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を編集できます。

［**追加**］をクリックすると、［**脅威の名前**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する脅威の名前を指定できます。

コマンドラインでのコンテナースキャン

コマンドラインでは、次の方法でコンテナとイメージをスキャンできます：

- コンテナースキャンの事前定義済みタスク（*Container_Scan*）を使用します。このタスクを手動で開始または停止し、タスクの実行スケジュールを設定できます。このタスクの設定を編集することで、スキャン設定を構成できます。
- コンテナースキャンのユーザータスク（*ContainerScan* タイプのタスク）を使用します。ユーザータスクを手動で開始および停止し、タスクの実行スケジュールを設定できます。
- `kesl-control --scan-container` コマンドを使用すると、指定したコンテナとイメージのオブジェクトスキャンを実行できます。

コンテナースキャンタスクの設定

この表では、すべてのコンテナとイメージのスキャン設定のすべての設定と、その設定で使用可能なすべての値と既定値を説明します。

コンテナースキャンタスクの設定

設定	説明	値
ScanContainers	マスクで指定したコンテナースキャン ContainerNameMask の設定を使用してマスクを指定することができます。	Yes（既定値）- コンテナをマスクの定義に基づいてスキャンします。 No - コンテナをマスクの定義に基づいてスキャンしません。
ContainerNameMask	名前または名前のマスクを指定して、スキャン対象のコンテナを定義します。 マスクはコマンドシェル形式で指定されます。? および * の記号を使用することができます。 この設定を指定する前に、ScanContainers=Yes であることを確認してください。	既定値：*（すべてのコンテナをスキャン） 例： my_container という名前のコンテナをスキャンする場合： ContainerNameMask=my_container 名前が my_container で始まるすべてのコンテナをスキャンする場合： ContainerNameMask=my_container* 名前が my_ で始まり、その後に任意の 5 文字、_container の順に続き、任意の文字で名前が終わるすべてのコンテナをスキャンする場合： ContainerNameMask=my_?????_container*
ScanImages	マスクで指定したコンテナースキャン ImageNameMask の設定を使用してマスクを指定することができます。	Yes（既定値）- イメージをマスクの定義に基づいてスキャンします。 No - イメージをマスクの定義に基づいてスキャンしません。
ImageNameMask	名前または名前のマスクを指定して、スキャン対象のイメージを定義します。 この設定を指定する前に、ScanImages 設定が Yes に設定されていることを確認してください。 マスクはコマンドシェル形式で指定されます。 複数のマスクを指定する場合は、新しいインデックスを使用して新しい行に各マスクを指定する必要があります。	既定値：*（すべてのイメージをスキャン）。 例： 「my_image」という名前で、「latest」タグを持つイメージをスキャンする場合： ImageNameMask=my_image:latest 名前が「my_image_」で始まり、任意のタグを持つイメージをスキャンする場合： ImageNameMask=my_image*
DeepScan	すべてのイメージレイヤーを確認し、コンテナを実行します。	Yes - 全レイヤーをスキャンします。 No（既定値）- どのレイヤーもスキャンしません。
ContainerScanAction	感染したオブジェクトの検知時	StopContainerIfFailed（既定値）— ア

	に、コンテナに対して実行する処理。コンテナ内の感染したオブジェクトに対する処理について、下に記載しています。	プリケーションが感染したオブジェクトの駆除や削除ができなかった場合、コンテナを停止します。 CRI-O 環境の仕組みにより、感染したオブジェクトは CRI-O 環境のコンテナ内で駆除または削除されません。`StopContainer` 操作を選択することを推奨します。 `StopContainer` - 感染したオブジェクトが検知されると、本製品によってコンテナが停止されます。 `Skip` - 感染したオブジェクトの検知時に、コンテナに対する処理は実行されません。
`ImageAction`	悪意のあるオブジェクトが削除された時に、イメージに対して実行する処理を指定します。イメージ内の感染したオブジェクトに対する処理について、下に記載しています。	`Skip`（既定値） - 感染したオブジェクトの検知時に、イメージに対する処理は実行されません。 `Delete` - 感染したオブジェクトの検知時に、本製品によってイメージが削除されます（推奨しないオプションです）。 すべての依存関係も削除されます。実行中のコンテナは停止され、それから削除されます。

コンテナとイメージ内のオブジェクトに対して、下に記載された設定が適用されます。

コンテナースキャンタスクの設定

設定	説明	
`ScanArchived`	アーカイブ（自己解凍型アーカイブを含む）のスキャンを指定します。 アプリケーションは次のアーカイブをスキャンします：.zip、.7z*、.7-z、.rar、.iso、.cab、.jar、.bz、.bz2、.tbz、.tbz2、.gz、.tgz、.arj。サポートされているアーカイブ形式のリストは、使用されている製品データベースによって異なります。	`Yes`（既 ます。I 指定さ 応じて、 含むア `No` – ア
`ScanSfxArchived`	自己解凍型アーカイブ（実行可能な解凍モジュールを含むアーカイブ）のみのスキャンを指定します。	`Yes`（既 キャン `No` – 自 ません。
`ScanMailBases`	Microsoft Outlook、Outlook Express、およびその他のメールクライアントのメールデータベースのスキャンを指定します。	`Yes` – メ キャン `No`（既 ァイル
`ScanPlainMail`	プレーンテキストのメールメッセージのスキャンを指定します。	`Yes` – プ ジをス

		No（既 ルメッ
TimeLimit	オブジェクトの最大スキャン時間（秒単位）。この設定で指定された時間よりもスキャンの時間がかかる場合、そのオブジェクトのスキャンが停止されます。	0～999 0 – オフ です。 既定値
SizeLimit	スキャン対象のオブジェクトの最大サイズ（メガバイト単位）。指定された値よりもスキャン対象のオブジェクトのサイズが大きい場合、オブジェクトはスキップされます。	0 ～ 99 0 – スキ 無制限 既定値
FirstAction	感染したオブジェクトに対して実行される最初の処理の選択。	Disinf し、そ す。駆 別また 除でき 更され ［Disi ［Seco 処理を Remove アップ を削除 Recomm オブジ 報に基 に選択 の木馬 Security イの木 なく、 Skip – は削除 トに関 既定値
SecondAction	感染したオブジェクトに対して実行される次の処理の選択。最初の処理に失敗した場合に、次の処理を実行します。	Second FirstA Skip ま 選択さ はあり つの処 指定し 適用さ 既定値
UseExcludeMasks	ExcludeMasks.item_# 設定で指定されたオブジェクトのスキャン除外を使用します。	Yes – E された ます。 No（既 定で指 ら除外
ExcludeMasks.item_#	名前またはマスクにより、オブジェクトをスキャンから除外します。この設定を使用すると、指定されたスキャン範囲から名	既定値は

	前によって個別のファイルを除外したり、シェル形式でマスクを使用して複数のファイルを除外したりできます。	例： UseE Excl Excl
UseExcludeThreats	ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトのスキャン除外を使用します。	Yes – E 定され ンから No（既 設定で をスキ
ExcludeThreats.item_#	オブジェクト内で検知された脅威の名前によってスキャンからオブジェクトを除外します。この設定の値を指定する前に、UseExcludeThreats 設定が有効になっていることを確認します。 スキャンから単一オブジェクトを除外するには、このオブジェクト内で検知された脅威の完全な名前（このオブジェクトが感染していると判定した際に使用された名前の文字列）を指定します。 たとえば、ネットワークに関する情報を収集するユーティリティを使用している場合があります。これをブロックしないようにするには、スキャンから除外される脅威のリストに、製品で使用される脅威の完全な名前を追加します。 オブジェクトで検知された脅威のフルネームは、アプリケーションログや https://threats.kaspersky.com の Web サイトで確認することができます。	設定値 す。 既定値 例： UseE Excl Test Excl roja
UseGlobalExclusions	スキャンのグローバル除外を有効にします。	Yes（ ます。 No – グ
ReportCleanObjects	感染していないとレポートされたスキャン済みオブジェクトに関する情報のログへの記録を指定します。 この設定は、たとえば特定のオブジェクトがスキャン済みであることを確認するために有効にします。	Yes – る情報 No（既 クトに
ReportPackedObjects	複合オブジェクトの一部を構成するスキャン済みオブジェクトに関する情報のログへの記録を指定します。 この設定は、たとえばアーカイブ内のオブジェクトがスキャン済みであることを確認するために有効にします。	Yes – ェクト No（既 済みオ 録しま
ReportUnprocessedObjects	何らかの理由により処理されていないオブジェクトに関する情報のログへの記録を指定します。	Yes – する情 No（既 ェクト ん。
UseAnalyzer	ヒューリスティック分析を指定します。 ヒューリスティック分析により、新しい脅威がウイルスアナリストに知られるようになる前に検知することができます。	Yes（ を有効 No – ヒ ます。
HeuristicLevel	ヒューリスティック分析のレベルを指定します。	Light い、シ

	ヒューリスティック分析のレベルを指定できます。ヒューリスティック分析レベルは、脅威の検索範囲とオペレーティングシステムのリソースに対する負荷およびスキャンの所要時間のバランスを設定します。ヒューリスティック分析レベルが高いほど、スキャンに必要なリソースと時間が増加します。	Medium レベル が取れ Deep – ステム Recomm
UseIChecker	iChecker 技術の使用を指定します。	Yes（既 効にし No – iC す。

コンテナとイメージのオブジェクトスキャン

kesl-control --scan-container コマンドを使用すると、指定したコンテナとイメージのオブジェクトスキャンを実行できます。

オブジェクトスキャンは、事前定義済みのタスク *Custom_Container_Scan* (ID: 19) に保存された設定で実行されます。このタスクの設定を編集することで、カスタムコンテナースキャンの設定を構成できます。既定では、*Custom_Container_Scan* タスクの設定は *Container_Scan* タスク（ID: 18）と同じです。

コンテナのカスタムスキャンタスクを開始するには、次のコマンドを実行します：

```
kesl-control --scan-container <コンテナ / イメージ [:タグ]>
```

<コンテナ / イメージ [:タグ]> は、コンテナまたはイメージの名前または ID です。複数のオブジェクトをスキャンするには、マスクを使用できます。

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」

アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。

ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。

同名のエントリが複数ある場合は、それらすべてをスキャンします。

コマンド実行の結果、一時的なコンテナとイメージのスキャンタスクが作成され、完了後自動的に削除されます。この場合、スキャン結果はコンソールに出力されます。

例：
my_container という名前のコンテナをスキャンします：
`kesl-control --scan-container my_container`
my_image（すべてのタグ）という名前のイメージをスキャンします：

```
kesl-control --scan-container my_image*
```

Jenkins との連携

Kaspersky Endpoint Security は、Jenkins との連携をサポートしています。Jenkins Pipeline プラグインを使用して、様々な段階で Docker イメージをスキャンできます。たとえば、開発プロセス中や公開前に、リポジトリ内の Docker イメージをスキャンできます。

Kaspersky Endpoint Security を Jenkins と連携するには：

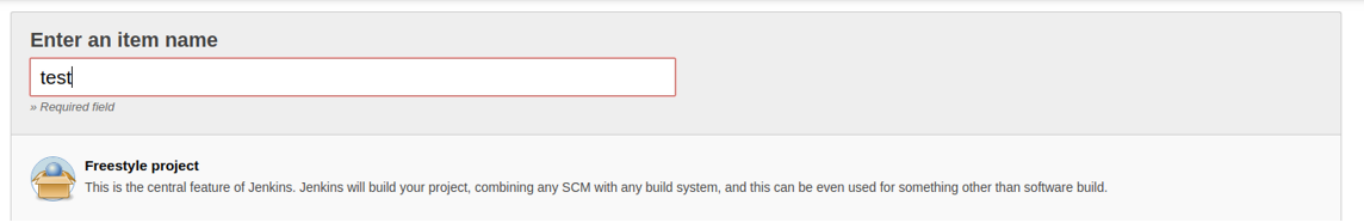
1. Jenkins ノードに Kaspersky Endpoint Security をインストールします。
2. Jenkins ノードに Docker Engine をインストールします。

   詳細は、Docker Engine のガイドを参照してください。
3. Kaspersky Endpoint Security の管理者権限を Jenkins ユーザーに付与します：

   `kesl-control --grant-role admin <Jenkins ユーザー名>`
4. Jenkins ユーザーを docker グループに追加します：

   `sudo usermod -aG docker <Jenkins ユーザー名>`

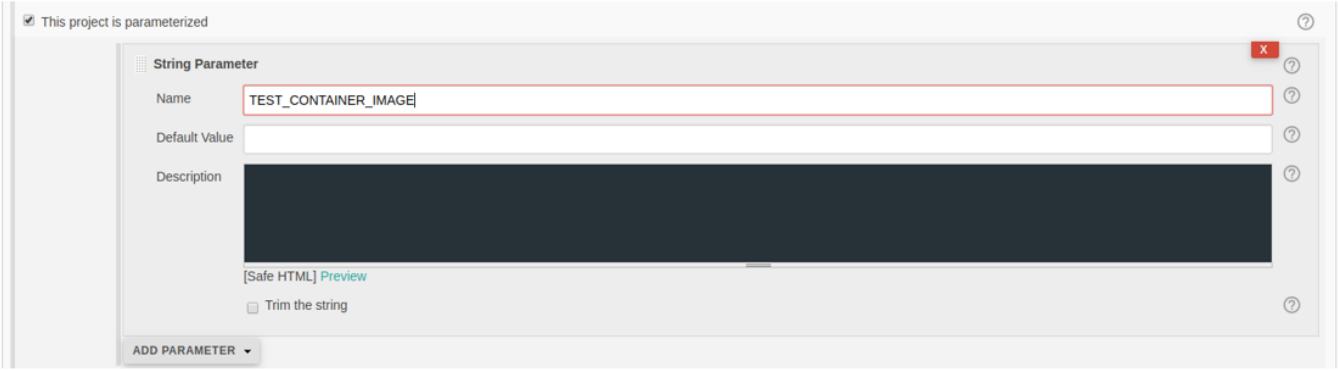
   通常、名前には jenkins が使用されます。
5. Jenkins で、名前に `test` を使用して新しいビルドジョブを作成します（［**新しいアイテム**］→［**アイテム名を入力**］）。



6. 必要に応じて、プロジェクトを設定します。結果として、スキャンする必要があるイメージや起動済みコンテナがあると仮定します。
7. Docker コンテナを起動するには、次のスクリプトを Jenkins のビルド手順に追加します。Jenkins プラグインを使用して、または別の方法で Docker コンテナを起動する場合は、実行中の Docker コンテナの ID をファイル /tmp/kesl_cs_info に保存して、さらにスキャンします：

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
echo "Start container from image: '${TEST_CONTAINER_IMAGE}'"
CONTAINER_ID=$(docker run -d -v /storage:/storage ${TEST_CONTAINER_IMAGE}
/storage/docker_process.sh)
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot start container from image ${TEST_CONTAINER_IMAGE}"
exit 1
fi
echo "${CONTAINER_ID}" > ${TMP_FILE}
```

```
exit ${EXIT_CODE}
```



8. アーティファクトをビルドしたら、Jenkins をビルドする手順に次のスクリプトを追加します。

   このスクリプトは、スキャンに対して1つのコンテナをサポートします。必要に応じて、スクリプトを編集します。

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
if [ ! -f "${TMP_FILE}" ] ; then
echo "Cannot find temporary file with container ID: '${TMP_FILE}'"
exit 1
fi
CONTAINER_ID=$(cat ${TMP_FILE})
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot find container ID in the temporary file: '${TMP_FILE}'"
exit 1
fi
echo "Start anti-virus scan for: '${CONTAINER_ID}'"
THREATS_AMOUNT=$(kesl-control --scan-container ${CONTAINER_ID}|grep 'Total detected objects'|awk '{print $5}')
if [ "${THREATS_AMOUNT}" != "0" ] ; then
echo "ATTENTION! ${THREATS_AMOUNT} threats detected at: '${CONTAINER_ID}'"
EXIT_CODE=1
else
echo "Not threats found"
fi
echo "Remove container: {${CONTAINER_ID}}"
docker kill ${CONTAINER_ID}
docker rm -f ${CONTAINER_ID}
rm -f ${TMP_FILE}
```

9. リポジトリから Docker イメージをスキャンするには、次のスクリプトを使用します：

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-dockerfile/master/Dockerfile
DOCKER_FILE_FETCHED=$$.Dockerfile
TEST_IMAGE_NAME=test_image
```

```
echo "Build image from ${DOCKER_FILE}"
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
echo "Dockerfile fetched: ${DOCKER_FILE_FETCHED}"
else
echo "Dockerfile not fetched"
exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME}
echo "Scan docker image"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container
${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

10. ビルドジョブを保存します。

ファイアウォール管理

ネットワーク（LAN）やインターネット上で使用されているデバイスは、ウイルスやその他のマルウェア、およびオペレーティングシステムやソフトウェアの脆弱性を悪用する様々な攻撃を受けます。オペレーティングシステムのファイアウォールは、デバイスがインターネットまたは LAN に接続されている時に、ほとんどの脅威をブロックすることによって、ユーザーデバイスに保存されているデータを保護します。

オペレーティングシステムのファイアウォールは、ユーザーデバイス上のすべてのネットワーク接続を検出し、その IP アドレスのリストを提供することができます。ファイアウォール管理コンポーネントでは、ネットワークパケットルールを設定することで、ネットワーク接続のステータスを設定できます。

この機能は、KESL コンテナではサポートされていません。

ネットワークパケットルールを使用して、すべてのアプリケーションのインターネットアクセスをブロックする設定から、無制限にアクセスを許可する設定まで、必要なレベルのデバイス保護を設定できます。ファイアウォール管理コンポーネントの対応するブロックルールが指定されている場合を除き、すべての送信接続が許可されます（既定の処理設定）。

ファイアウォール管理コンポーネントは既定で無効になっています。

ファイアウォール管理を有効にする前に、他のオペレーティングシステムのファイアウォール管理ツールを無効にしてください。

ファイアウォール管理コンポーネントを有効にすると、Kaspersky Endpoint Security は、オペレーティングシステムが提供するツールを使用してファイアウォールに設定されたすべてのカスタムルールを自動的に削除します。これらのルールは、コンポーネントが無効化された後は復元されません。必要に応じて、ファイアウォール管理コンポーネントを有効にする前に、カスタムファイアウォールルールを保存します。

ファイアウォール管理が有効になっている場合、Kaspersky Endpoint Security はオペレーティングシステムのファイアウォールをスキャンし、アプリケーションやユーティリティがファイアウォールルールを追加または削除しようとするなど、ファイアウォール設定を変更しようとする試みをブロックします。Kaspersky Endpoint Security はオペレーティングシステムのファイアウォールを 60 秒ごとにチェックし、必要に応じてアプリケーションを使用して作成されたファイアウォールのルールのセットを復元します。チェックの間隔は変更できません。

Red Hat Enterprise Linux および CentOS 8 オペレーティングシステムでは、Kaspersky Endpoint Security で作成されたファイアウォールルールは、管理コマンドを使用してのみ表示できます（`kesl-control -F --query` コマンド）。

Kaspersky Endpoint Security は、ファイアウォール管理を無効にしてもオペレーティングシステムのファイアウォールをスキャンします。これにより、本製品は動的ルールを復元できます。

ファイアウォール管理を有効または無効にしたり、次の設定を行うことができます：

- ネットワーク接続を確立しようとする試みが検出された場合に、Kaspersky Endpoint Security が適用するネットワークパケットルールのリストを設定します。ネットワークパケットルールを追加または削除したり、ネットワークパケットルールの実行優先度を変更できます。
- この接続タイプに他のネットワークパケットルールが適用されない場合に、着信接続とパケットに対して実行する既定の処理を選択します。

- ネットワークアドレスをプリセットされたネットワークゾーンにマッピングします。ネットワークゾーンに IP アドレスやサブネットを追加したり、ネットワークゾーンからアドレスを削除できます。

- このチェックボックスで、ネットワークエージェントのポートに対する許可ルールを自動的に追加するかどうかを選択します。

nftables を使用するシステムであり得る問題を回避するために、Kaspersky Endpoint Security はオペレーティングシステムのファイアウォールのルールを追加する時に、iptables および iptables-restore システムユーティリティを使用します。本製品は、kesl_bypass と呼ばれる許可ルールの特別なチェーンを作成し、それを iptables および ip6tables ユーティリティの mangle テーブルのリストの一番上に追加します。kesl_bypass チェーンのルールにより、Kaspersky Endpoint Security のスキャンからトラフィックを除外できます。このチェーンのルールは、オペレーティングシステムで変更できます。本製品が削除されると、空の場合にのみ kesl_bypass ルールチェーンが iptables および ip6tables から削除されます。

ネットワークパケットルールの概要

*ネットワークパケットルール*は、検知されたネットワーク接続の試行を許可または拒否するために Kaspersky Endpoint Security によって実行される処理です。

ネットワークパケットルールは、アプリケーションに関係なくネットワークパケットを制限します。このようなルールは、選択したデータプロトコルの特定のポートから送受信するネットワークトラフィックを制限します。

既定では、ファイアウォール管理の対応するブロックルールが指定されている場合を除き、すべての送信接続が許可されます（既定の処理設定）。既定の処理は、最も低い優先順位で実行されます。他のネットワークパケットルールが起動されていない場合、またはネットワークパケットルールが指定されていない場合、接続が許可されます。

既定では、ファイアウォール管理は特定のネットワークパケットルールを指定します。独自のネットワークパケットルールを作成して、ネットワークパケットルールごとに実行の優先度を指定できます。

動的ルールの概要

Kaspersky Endpoint Security を使用すると、*動的ルール*をファイアウォールに追加またはファイアウォールから削除して、アプリケーションが正しく動作するようにできます。たとえば、ネットワークエージェントは、本製品または Kaspersky Security Center が開始した Kaspersky Security Center への接続を許可する動的ルールを追加します。アンチクリプターのルールも動的です。

Kaspersky Endpoint Security が Light Agent モードで使用されている場合、SVM および Integration Server への接続を許可する動的ルールがファイアウォールに自動的に追加されます。

Kaspersky Endpoint Security は動的ルールを管理せず、製品コンポーネントのネットワークリソースへのアクセスをブロックしません。動的ルールは、ファイアウォール管理コンポーネントの状態（有効 / 無効）やコンポーネント操作の設定の変更には依存しません。ネットワークパケットルールよりも、動的ルールの実行が優先されます。たとえば、iptables ユーティリティを使用して動的ルールのセットのいずれかが削除された場合、そのセットを復元できます。

動的ルールのセットの表示（`kesl-control -F --query` コマンドを使用）はできますが、動的ルールの設定を変更することはできません。

事前に定義されたネットワークゾーン名の概要

*事前に定義されたネットワークゾーン*は、IP アドレスまたはサブネットの特定のグループです。事前に定義されたネットワークゾーンを使用することにより、IP アドレスやサブネットごとに別のルールを作成することなく、複数の IP アドレスやサブネットに対して同じルールを使用できます。ネットワークゾーンは、ネットワークパケットルールを作成する際に、「リモートアドレス」パラメータの値として使用できます。Kaspersky Endpoint Security には、固有の名前を持つ 3 つの事前定義されたネットワークゾーンがあります：

- **パブリック**：アンチウイルス製品、ファイアウォール、フィルターによって保護されないネットワーク（インターネットカフェのネットワークなど）にネットワークアドレスやサブネットを割り当てる場合は、ネットワークアドレスやサブネットをこのゾーンに追加します。
- **ローカル**：このデバイス上のファイルやプリンターにユーザーがアクセスすることを信頼するネットワーク（LAN やホームネットワークなど）にネットワークアドレスやサブネットを割り当てる場合は、ネットワークアドレスやサブネットをこのゾーンに追加します。
- **許可**：このゾーンは、デバイスが攻撃や不正なデータアクセスにさらされることのない安全なネットワーク用です。

ユーザーがネットワークゾーンを作成したり削除したりできません。ユーザーはネットワークゾーンに IP アドレスやサブネットを追加したり削除したりすることができます。

Web Console でのファイアウォール管理

Web コンソールでは、ポリシーのプロパティ（**製品設定 → 脅威対策 → ファイアウォール管理**）でファイアウォール管理設定を構成できます。

ファイアウォール管理の設定

設定	説明
ファイアウォール管理の有効化または無効化	この切り替えボタンでは、ファイアウォール管理を有効にするかどうかを選択します。 この切り替えボタンは既定でオフになっています。
ネットワークパケットルール	［**ネットワークパケットルールを設定する**］をクリックすると、［**ネットワークパケットルール**］ウィンドウが表示されます。このウィンドウでは、ネットワーク接続の試行を検知した場合にファイアウォール管理が適用するネットワークパケットルールのリストを編集できます。
使用可能なネットワーク	［**使用可能なネットワークを設定する**］をクリックすると、［**使用可能なネットワーク**］ウィンドウが表示されます。このウィンドウでは、ファイアウォール管理が監視するネットワークのリストを設定します。
受信接続	このドロップダウンリストでは、ネットワークの受信接続に対して実行する処理を選択します： • **許可**：ネットワーク接続を許可します（既定値）。 • **ブロック**：ネットワーク接続をブロックします。
受信パケット	このドロップダウンリストでは、受信パケットに対して実行する処理を選択します： • **許可**：受信パケットを許可します（既定値）。 • **ブロック**：受信パケットをブロックします。
ネットワークエージェントのポ	このチェックボックスでは、ネットワークエージェントのポートに対する許可ルールを自動的に追加するかどうかを選択します。

ートの許可ルールを常に追加する	既定では、このチェックボックスはオンです。

［ネットワークパケットルール］ウィンドウ

［**ネットワークパケットルール**］の表には、ファイアウォール管理がネットワーク活動の監視に使用するネットワークパケットルールが表示されています。ネットワークパケットルールの指定可能な設定について、以下の表で説明します。

ネットワークパケットルールの設定

設定	説明
名前	ネットワークパケットルールの名前
処理	ネットワーク活動の検出時にファイアウォール管理によって実行される処理。
ローカルアドレス	Kaspersky Endpoint Security がインストールされており、ネットワークパケットを送受信できるデバイスのネットワークアドレス。
リモートアドレス	ネットワークパケットを送受信できるリモートデバイスのネットワークアドレス。
Direction	ネットワーク活動を監視する通信方向。
プロトコル	ネットワーク動作を監視するデータ転送プロトコルの種別。
ローカルポート	接続を監視するローカルデバイスのポート番号。
リモートポート	接続を監視するリモートデバイスのポート番号。
ICMP タイプ	ICMP タイプ。ファイアウォール管理は、ホストまたはゲートウェイによって送信される指定されたタイプのメッセージを監視します。
ICMP コード	ICMP コード。ファイアウォール管理コンポーネントは、ホストまたはゲートウェイから送信された、**ICMP 種別**フィールドに指定された種別と **ICMP コード**フィールドに指定されたコードのメッセージを監視します。
ログ記録	この列は、ネットワークパケットルールの処理をログに記録すると表示されます。 値が **はい** の場合、ネットワークパケットルールの処理がログに記録されます。 値が **No** の場合、ネットワークパケットルールの処理はログに記録されません。

既定では、ネットワークパケットルールの表は空です。

表内のネットワークパケットルールに対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［ネットワークパケットルール］ウィンドウ

このウィンドウでは、ネットワークパケットルールを設定します。

ネットワークパケットルールの設定

設定	説明
ルール名	ネットワークパケットルールの名前を入力するフィールド。
処理	このドロップダウンリストでは、ネットワーク活動の検知時にファイアウォール管理によって実行される処理を選択します： • **ブロック**：ネットワーク活動をブロックします。 • **許可**：ネットワーク活動を許可します（既定値）。
プロトコル	このドロップダウンリストでは、ネットワーク活動を監視するデータ転送プロトコルの種別を選択します： • **すべて**（既定値） • GRE • ICMP • ICMPv6 • IGMP • TCP • UDP
ICMPタイプを	このチェックボックスでは、ICMP タイプを指定できます。ファイアウォール管理は、ホストまたはゲートウェイによって送信される指定されたタイプのメッセージを監視します。 このチェックボックスをオンにすると、ICMP タイプを入力するフィールドが表示されます。

指定する	このチェックボックスは、［**プロトコル**］ドロップダウンリストで［**ICMP**］または［**ICMPv6**］データ転送プロトコルが選択されている場合にのみ表示されます。 既定では、このチェックボックスはオフです。
ICMP コードを指定する	このチェックボックスでは、ICMP コードを指定できます。ファイアウォール管理コンポーネントは、ホストまたはゲートウェイから送信された、指定された種別（［**ICMP タイプの指定**］チェックボックスの下のフィールド）と指定されたコード（［**ICMP コードの指定**］チェックボックスの下のフィールド）のメッセージを監視します。 このチェックボックスをオンにすると、ICMP コードを入力するフィールドが表示されます。 このチェックボックスは、［**プロトコル**］ドロップダウンリストで［**ICMP**］または［**ICMPv6**］データ転送プロトコルが選択されている場合にのみ表示されます。［**ICMP タイプを指定する**］をオンにする場合にのみ使用できます。 既定では、このチェックボックスはオフです。
通信方向	このドロップダウンリストでは、監視対象のネットワーク活動の通信方向を指定できます： • **受信パケット**（既定値）：このオプションをオンにすると、ファイアウォール管理は受信パケットを監視します。 • **受信**：このオプションをオンにすると、ファイアウォール管理は受信するネットワーク活動を監視します。 • **送受信**：このオプションをオンにすると、ファイアウォール管理は受信するネットワーク活動と送信するネットワーク活動の両方を監視します。 • **送受信パケット**：このオプションをオンにすると、ファイアウォール管理は受信パケットと送信パケットの両方を監視します。 • **送信パケット**：このオプションをオンにすると、ファイアウォール管理は送信パケットを監視します。 • **送信**：このオプションをオンにすると、ファイアウォール管理は送信するネットワーク活動を監視します。
リモートアドレス	このドロップダウンリストでは、ネットワークパケットを送受信できるリモートデバイスのネットワークアドレスを指定します： • **すべてのアドレス**（既定値）：このオプションをオンにすると、任意の IP アドレスを持つリモートデバイスによって送受信されるネットワークパケットをネットワークルールが制御します。 • **すべてのサブネットアドレス**：このオプションを選択すると、選択されたネットワークの種別（**パブリックネットワーク**、**ローカルネットワーク**、または**許可するネットワーク**）に関連付けられた IP アドレスを持つリモートデバイスによって送受信されるネットワークパケットを、ネットワークルールが制御します。 • **指定のアドレス**：このオプションをオンにすると、［**アドレス**］フィールドで指定された IP アドレスを持つリモートデバイスによって送受信されるネットワークパケットを、ネットワークルールが制御します。
リモートポートを指定する	このチェックボックスでは、接続を監視する必要のあるリモートデバイスのポート番号を指定できます。 このチェックボックスをオンにすると、ポート番号を入力するフィールドが表示されます。 このチェックボックスは、［**プロトコル**］ドロップダウンリストで［**TCP**］または［**UDP**］データ転送プロトコルが選択されている場合にのみ表示されます。 既定では、このチェックボックスはオフです。

ローカルアドレス	このドロップダウンリストでは、Kaspersky Endpoint Security がインストールされてネットワークパケットを送受信できるデバイスのネットワークアドレスを指定します： • **すべてのアドレス**（既定値）：このオプションをオンにすると、Kaspersky Endpoint Security がインストール済みで任意の IP アドレスを持つデバイスによって送受信されるネットワークパケットを、ネットワークルールが制御します。 • **指定のアドレス**：このオプションをオンにすると、Kaspersky Endpoint Security がインストールされてネットワークパケットを送受信できるデバイスの、［**アドレス**］フィールドで指定されたネットワークアドレスを、ネットワークルールが制御します。
ローカルポートを指定する	このチェックボックスでは、接続を監視する必要のあるローカルデバイスのポート番号を指定できます。 このチェックボックスをオンにすると、ポート番号を入力するフィールドが表示されます。 このチェックボックスは、［**プロトコル**］ドロップダウンリストで［**TCP**］または［**UDP**］データ転送プロトコルが選択されている場合にのみ表示されます。 既定では、このチェックボックスはオフです。
イベントの記録	このチェックボックスでは、ネットワークルールの処理がレポートに記録されるかどうかを指定できます。 このチェックボックスをオンにすると、ネットワークルールの処理がレポートに記録されます。 このチェックボックスをオフにすると、ネットワークルールの処理はレポートに記録されません。 既定では、このチェックボックスはオフです。

［使用可能なネットワーク］ウィンドウ

［**使用可能なネットワーク**］の表には、ファイアウォール管理によって制御されるネットワークが表示されています。既定では、使用可能なネットワークの表は空です。

使用可能なネットワークの設定

設定	説明
IP アドレス	ネットワーク IP アドレス。
ネットワーク種別	ネットワーク種別（**パブリックネットワーク**、**ローカルネットワーク**、または**許可するネットワーク**）。

使用可能なネットワークは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［ネットワーク接続］ウィンドウ

このウィンドウでは、ファイアウォール管理が監視するネットワーク接続を設定します。

ネットワーク接続

設定	説明
IP アドレス	ネットワークの IP アドレスを入力するフィールド。
ネットワーク種別	ネットワークの種別を選択できます： • **パブリック** • **ローカル** • **許可**

管理コンソールでのファイアウォール管理

管理コンソールでは、ポリシーのプロパティ（製品設定 → **脅威対策** → **ファイアウォール管理**）でファイアウォール管理設定を構成できます。

ファイアウォール管理の設定

設定	説明
ファイアウォール管理を有効にする	このチェックボックスでは、ファイアウォール管理を有効にするかどうかを選択します。 既定では、このチェックボックスはオフです。
ネットワークパケットルール	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**ネットワークパケットルール**］ウィンドウが表示されます。このウィンドウでは、ネットワーク接続の試行を検知した場合にファイアウォール管理が適用するネットワークパケットルールを編集できます。
使用可能なネットワーク	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**使用可能なネットワーク**］ウィンドウが表示されます。このウィンドウでは、ファイアウォール管理が監視するネットワークのリストを設定します。
受信接続	このドロップダウンリストでは、ネットワークの受信接続に対して実行する処理を選択します： • **許可**：ネットワーク接続を許可します（既定値）。 • **ブロック**：ネットワーク接続をブロックします。
受信パケット	このドロップダウンリストでは、受信パケットに対して実行する処理を選択します： • **許可**：受信パケットを許可します（既定値）。 • **ブロック**：受信パケットをブロックします。

ネットワークエージェントのポートの許可ルールを常に追加する	このチェックボックスでは、ネットワークエージェントのポートに対する許可ルールを自動的に追加するかどうかを選択します。 既定では、このチェックボックスはオンです。

［ネットワークパケットルール］ウィンドウ

［**ネットワークパケットルール**］の表には、ファイアウォール管理がネットワーク活動の監視に使用するネットワークパケットルールが表示されています。ネットワークパケットルールの指定可能な設定について、以下の表で説明します。

ネットワークパケットルールの設定

設定	説明
名前	ネットワークパケットルールの名前
処理	ネットワーク活動の検出時にファイアウォール管理によって実行される処理。
ローカルアドレス	Kaspersky Endpoint Security がインストールされており、ネットワークパケットを送受信できるデバイスのネットワークアドレス。
リモートアドレス	ネットワークパケットを送受信できるリモートデバイスのネットワークアドレス。
ログ記録	この列は、ネットワークパケットルールの処理をログに記録すると表示されます。 値が **はい** の場合、ネットワークパケットルールの処理がログに記録されます。 値が **No** の場合、ネットワークパケットルールの処理はログに記録されません。

既定では、ネットワークパケットルールの表は空です。

表内のネットワークパケットルールに対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［ネットワークパケットルールの追加］ウィンドウ

このウィンドウでは、追加したネットワークパケットルールを設定します。

ネットワークパケットルールの設定

設定	説明
プロトコル	ネットワーク活動を監視するデータ転送プロトコルの種別を選択します： • **すべて**（既定値） • GRE • ICMP • ICMPv6 • IGMP • TCP • UDP
通信方向	監視するネットワーク活動の方向を指定します： • **受信パケット**：このオプションをオンにすると、ファイアウォール管理は受信パケットを監視します。 • **受信**：このオプションをオンにすると、ファイアウォール管理は受信するネットワーク活動を監視します。 • **送受信**：このオプションをオンにすると、ファイアウォール管理は受信するネットワーク活動と送信するネットワーク活動の両方を監視します。 • **送受信パケット**：このオプションをオンにすると、ファイアウォール管理は受信パケットと送信パケットの両方を監視します。 • **送信パケット**：このオプションをオンにすると、ファイアウォール管理は送信パケットを監視します。 • **送信**：このオプションをオンにすると、ファイアウォール管理は送信するネットワーク活動を監視します。
ICMP タイプ	ICMP タイプを指定します。ファイアウォール管理は、ホストまたはゲートウェイによって送信される指定されたタイプのメッセージを監視します。 **指定** オプションをオンにすると、ICMP タイプを入力するフィールドが表示されます。 このウィンドウは、［**プロトコル**］ドロップダウンリストで［**ICMP**］または［**ICMPv6**］データ転送プロトコルが選択されている場合に表示されます。
ICMP コード	ICMP コードを指定します。ファイアウォール管理コンポーネントは、ホストまたはゲートウェイから送信された、**ICMP 種別**フィールドに指定された種別と **ICMP コード**フィールドに指定されたコードのメッセージを監視します。 **指定** オプションをオンにすると、ICMP コードを入力するフィールドが表示されます。

	このウィンドウは、［**プロトコル**］ドロップダウンリストで［**ICMP**］または［**ICMPv6**］データ転送プロトコルが選択されている場合に表示されます。
リモートポート	接続を監視するリモートデバイスのポート番号を指定します。 **指定** オプションをオンにすると、ポート番号を入力するフィールドが表示されます。 このウィンドウは、［**プロトコル**］ドロップダウンリストで［**TCP**］または［**UDP**］データ転送プロトコルが選択されている場合にのみ表示されます。
ローカルポート	接続を監視するローカルデバイスのポート番号を指定します。 **指定** オプションをオンにすると、ポート番号を入力するフィールドが表示されます。 このウィンドウは、［**プロトコル**］ドロップダウンリストで［**TCP**］または［**UDP**］データ転送プロトコルが選択されている場合にのみ表示されます。
リモートアドレス	ネットワークパケットを送受信できるリモートデバイスのネットワークアドレスを指定します： • **すべてのアドレス**（既定値）：この項目をオンにすると、任意の IP アドレスを持つリモートデバイスによって送受信されるネットワークパケットを、ネットワークルールが制御します。 • **指定のアドレス**：この項目をオンにすると、下のフィールドで指定された IP アドレスを持つリモートデバイスによって送受信されるネットワークパケットを、ネットワークルールが制御します。 • **ネットワーク種別**：この項目をオンにすると、選択されたネットワークの種別（**パブリックネットワーク**、**ローカルネットワーク**、または**許可するネットワーク**）に関連付けられた IP アドレスを持つリモートデバイスによって送受信されるネットワークパケットを、ネットワークルールが制御します。
ローカルアドレス	Kaspersky Endpoint Security がインストールされており、ネットワークパケットを送受信できるデバイスのネットワークアドレスを指定します。 • **すべてのアドレス**（既定値）：このオプションをオンにすると、Kaspersky Endpoint Security がインストール済みで任意の IP アドレスを持つデバイスによって送受信されるネットワークパケットを、ネットワークルールが制御します。 • **指定のアドレス**：このオプションをオンにすると、Kaspersky Endpoint Security がインストールされてネットワークパケットを送受信できるデバイスのネットワークアドレスを、ネットワークルールが制御します。これらのネットワークアドレスは、以下のフィールドで指定されます。
処理	ネットワーク活動の検知時にファイアウォール管理によって実行される処理を選択します： • **ブロック**：ネットワーク活動をブロックします。 • **許可**：ネットワーク活動を許可します（既定値）。
ログ記録	ネットワークルールの処理をレポートに記録するかどうかを指定します。
ルール名	ネットワークパケットルールの名前を入力するフィールド。

［使用可能なネットワーク］ウィンドウ

［**使用可能なネットワーク**］の表には、ファイアウォール管理によって制御されるネットワークが表示されています。既定では、使用可能なネットワークの表は空です。

使用可能なネットワークの設定

設定	説明
IP アドレス	ネットワーク IP アドレス。
ネットワーク種別	ネットワーク種別（**パブリックネットワーク**、**ローカルネットワーク**、または**許可するネットワーク**）。

使用可能なネットワークは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［ネットワーク接続］ウィンドウ

このウィンドウでは、ファイアウォール管理が監視するネットワーク接続を設定します。

ネットワーク接続

設定	説明
IP アドレス	ネットワークの IP アドレスを入力するフィールド。
ネットワーク種別	ネットワークの種別を選択できます： • **パブリック** • **ローカル** • **許可**

コマンドラインでのファイアウォール管理

コマンドラインでは、ファイアウォール管理の事前定義済みタスク（*Firewall_Management*）を使ってファイアウォール管理を設定できます。

既定では、ファイアウォール管理は実行されません。このタスクは、手動で開始および停止できます。

タスク設定を管理するコマンドを使用して、事前定義済みのタスクの設定を編集することで、ファイアウォール管理を設定できます。

ファイアウォール管理コマンドを使用して、ファイアウォール管理の設定を構成できます：

- ネットワークパケットルールの作成と削除、実行優先度の変更。
- ネットワークゾーンのIPアドレスまたはサブネットのリストを作成します。
- Kaspersky Endpoint Security で作成されたファイアウォールルールを表示するには、`kesl-control -F --query` コマンドを使用します。

ファイアウォール管理タスクの設定

設定	説明	値
`DefaultIncomingAction`	この接続種別に適用するネットワークルールがない場合、受信接続に対して実行する既定の処理。	`Allow`（既定値）– 受信接続を許可します。 `Block` – 受信接続をブロックします。
`DefaultIncomingPacketAction`	この接続種別に適用するネットワークパケットルールがない場合、受信パケットに対して実行する既定の処理。	`Allow`（既定値）– 受信パケットを許可します。 `Block` – 受信パケットをブロックします。
`OpenNagentPorts`	ネットワークエージェントの動的ルールをネットワークパケットルールに追加するかどうかを指定します。	`Yes`（既定値）– ネットワークエージェントの動的ルールをネットワークパケットルールに追加します。 `No` – ネットワークエージェントの動的ルールをネットワークパケットルールに追加しません。
[PacketRules.item_#] セクションには、ファイアウォール管理タスクのネットワークパケットルールが含まれます。複数の `[PacketRules.item_#]` セクションを、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。 `[PacketRules.item_#]` の各セクションには、次の設定が含まれています：		
`Name`	ネットワークパケットルールの名前。	既定値：`Packet rule #<n>`（n はインデックス）
`FirewallAction`	このネットワークパケットルールで指定される接続に対して実行する処理。	`Allow`（既定値）– ネットワーク接続を許可します。 `Block` – ネットワーク接続をブロックします。

`Protocol`	監視するネットワーク活動のデータ転送プロトコルの種別。	`Any`（既定値）– ファイアウォール管理タスクはすべてのネットワーク活動を監視します。
		`TCP`
		`UDP`
		`ICMP`
		`ICMPv6`
		`IGMP`
		`GRE`

`RemotePorts`	接続を監視するリモートデバイス	`Any`（既定値）– すべての

	のポート番号。この値に対して、整数または範囲を指定できます。 この設定は、**Protocol** の設定値が **TCP** または **UDP** に設定された場合にのみ指定できます。	リモートポートを監視します。 **0 – 65535**
LocalPorts	接続を監視するローカルデバイスのポート番号。この値に対して、整数または範囲を指定できます。 この設定は、**Protocol** の設定値が **TCP** または **UDP** に設定された場合にのみ指定できます。	**Any**（既定値） – すべてのローカルポートを監視します。 **0 – 65535**
ICMPType	ICMP パケットの種別。 この設定は、**Protocol** の設定値が **ICMP** または **ICMPv6** に設定された場合にのみ指定できます。	**Any**（既定値） – すべての ICMP パケット種別を監視します。 データ転送プロトコルの仕様に応じた整数。
ICMPCode	ICMP パケットのコード。 この設定は、**Protocol** の設定値が **ICMP** または **ICMPv6** に設定された場合にのみ指定できます。	**Any**（既定値） – すべての ICMP パケットコードを監視します。 データ転送プロトコルの仕様に応じた整数。
Direction	ネットワーク活動を監視する通信方向。	**IncomingOutgoing** または **InOut**（既定値） – 受信と送信の両方の接続を監視します。 **Incoming** または **In** – 受信接続を監視します。 **Outgoing** または **Out** – 送信接続を監視します。 **IncomingPacket** または **InPacket** – 受信パケットを監視します。 **OutgoingPacket** または **OutPacket** – 送信パケットを監視します。 **IncomingOutgoingPacket** または **InOutPacket** – 受信と送信の両方の接続を監視します。
RemoteAddress	ネットワークパケットを送受信できるリモートデバイスのネットワークアドレス。	**Any**（既定値）- すべての IP アドレスのリモートデバイスによって送受信されるネットワークパケットを監視します。 **Trusted** – 許可するネットワーク用の事前定義されたネットワークゾーン。 **Local** – ローカルネットワーク用の事前定義されたネットワークゾーン。

		Public – パブリックネットワーク用の事前定義されたネットワークゾーン。 d.d.d.d – IPv4 アドレス、d は 10 進数の 0 – 255。 d.d.d.d/p – IPv4 のサブネットアドレス、p は数値 0 – 32。 x:x:x:x:x:x:x:x – IPv6 アドレス、x は 16 進数の 0 – ffff。 x:x:x:x::0/p – IPv6 のサブネットアドレス、p は数値 0 – 64。
LocalAddress	Kaspersky Endpoint Security がインストールされており、ネットワークパケットを送受信できるデバイスのネットワークアドレス。	Any（既定値）- すべての IP アドレスのローカルデバイスによって送受信されるネットワークパケットを監視します。 d.d.d.d - IPv4 アドレス、d は 10 進数の 0 - 255。 d.d.d.d/p – IPv4 のサブネットアドレス、p は数値 0 – 32。 x:x:x:x:x:x:x:x – IPv6 アドレス、x は 16 進数の 0 – ffff。 x:x:x:x::0/p - IPv6 のサブネットアドレス、p は数値 0 - 64。
LogAttempts	ネットワークルール処理の記録をレポートに含めます。	Yes – レポートに処理を記録します。 No（既定値）- レポートに処理を記録しません。
[NetworkZonesPublic] セクションには、パブリックネットワークに関連付けられたネットワークアドレスが含まれます。複数の IP アドレスまたは IP アドレスのサブネットを指定できます。		
Address.item_#	IP アドレスまたは IP アドレスのサブネットを指定します。	d.d.d.d - IPv4 アドレス、d は 10 進数の 0 - 255。 d.d.d.d/p – IPv4 のサブネットアドレス、p は数値 0 – 32。 x:x:x:x:x:x:x:x – IPv6 アドレス、x は 16 進数の 0 – ffff。 x:x:x:x::0/p - IPv6 のサブネットアドレス、p は数値 0 - 64。 既定値：""（このゾーンのネットワークアドレスはありません）
[NetworkZonesLocal] セクションには、ローカルネットワークに関連付けられたネットワークアドレ		

スが含まれます。複数の IP アドレスまたは IP アドレスのサブネットを指定できます。		
`Address.item_#`	IP アドレスまたは IP アドレスのサブネットを指定します。	`d.d.d.d` - IPv4 アドレス、d は 10 進数の 0 - 255。 `d.d.d.d/p` – IPv4 のサブネットアドレス、p は数値 0 – 32。 `x:x:x:x:x:x:x:x` – IPv6 アドレス、x は 16 進数の 0 – ffff。 `x:x:x:x::0/p` - IPv6 のサブネットアドレス、p は数値 0 - 64。 既定値：`""`（このゾーンのネットワークアドレスはありません）
[NetworkZonesTrusted] セクションには、許可するネットワークに関連付けられたネットワークアドレスが含まれます。複数の IP アドレスまたは IP アドレスのサブネットを指定できます。		
`Address.item_#`	IP アドレスまたは IP アドレスのサブネットを指定します。	`d.d.d.d` - IPv4 アドレス、d は 10 進数の 0 - 255。 `d.d.d.d/p` – IPv4 のサブネットアドレス、p は数値 0 – 32。 `x:x:x:x:x:x:x:x` – IPv6 アドレス、x は 16 進数の 0 – ffff。 `x:x:x:x::0/p` - IPv6 のサブネットアドレス、p は数値 0 - 64。 既定値：`""`（このゾーンのネットワークアドレスはありません）

コマンドラインでネットワークパケットルールのリストの設定

ネットワークパケットルールを追加するには、次のコマンドを実行します：

`kesl-control --add-rule [--name <`ルールの名前`>] [--action <`処理`>] [--protocol <`プロトコル`>] [--direction <`通信方向`>] [--remote <`アドレスの削除`>[:<`ポートの範囲`>]] [--local <`ローカルアドレス`>[:<`ポートの範囲`>]] [--at <`インデックス`>]`

説明：

- `--name <`ルールの名前`>` は、ネットワークパケットルールの名前です。
- `--action <`処理`>` は、ネットワークパケットルールで指定された接続に対して実行される処理です。
- `--protocol <`プロトコル`>` は、ネットワークアクティビティを監視したいデータ転送プロトコルの種別です。

- `--direction <通信方向>` は、監視するネットワークアクティビティの通信方向です。
- `--remote <リモートアドレス [:<ポートの範囲>]>` はリモートデバイスのネットワークアドレスです。定義済みのネットワークゾーンの名前をリモートアドレスとして指定できます。
- `--local <ローカルアドレス [:<ポートの範囲>]>` は、Kaspersky Endpoint Securityがインストールされているデバイスのネットワークアドレスです。
- `--at <インデックス>` は、ネットワークパケットルールのリスト中のルールのインデックスです。`--at` ライセンスが指定されていない場合、または値がリストのルールの数より大きい場合、新しいルールがリストの最後に追加されます。

コマンドで値を指定しなかったパラメータは、既定値に設定されます。

例：
すべての受信および TCP ポート 23 に対して確立された接続をブロックするルールを作成するには、次のコマンドを実行します：
```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol
TCP --local any:23 --remote any
```
パブリックネットワークゾーンについての受信および TCP ポート 23 を使用して確立された接続をブロックするルールを作成するには、次のコマンドを実行します：
```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol
TCP --local any:23 --remote Public
```

ネットワークパケットルールを削除するには、次のコマンドのいずれかを実行します：

- `kesl-control --del-rule --name <ルール名>`
- `kesl-control --del-rule --index <インデックス>`

説明：

- `--name <ルールの名前>` は、ネットワークパケットルールの名前です。
- `--index <インデックス>` は、ネットワークパケットルールのリスト中のルールの現在のインデックスです。

ネットワークパケットルールのリストに同じ名前のルールが複数含まれている、または指定された名前やインデックスを持つルールが含まれていない場合、エラーが発生します。

ネットワークパケットルールの実行の優先度を変更するには、次のいずれかのコマンドを実行します：

- `kesl-control --move-rule --name <ルール名> --at <インデックス>`
- `kesl-control --move-rule --index <インデックス> --at <インデックス>`

説明：

- `--name <ルールの名前>` は、ネットワークパケットルールの名前です。
- `--index <インデックス>` は、ネットワークパケットルールのリスト中のルールの現在のインデックスです。
- `--at <インデックス>` は、ネットワークパケットルールのリスト中のルールの新しいインデックスです。

コマンドラインでのネットワークゾーンの設定

ネットワークアドレスをゾーンに追加するには、次のコマンドを実行します：

```
kesl-control --add-zone --zone <ゾーン> --address <アドレス>
```

説明：

- `--zone <zone>` は、ネットワークゾーンの事前定義済みの名前です。可能な値：`Public`、`Local`、`Trusted`。
- `--address <address>` はネットワークアドレスまたはサブネットです。

ネットワークアドレスをゾーンから削除するには、次のいずれかのコマンドを実行します：

- `kesl-control --del-zone --zone <ゾーン> --address <アドレス>`
- `kesl-control --del-zone --zone <ゾーン> --index <ゾーン内のアドレスインデックス>`

同じネットワークアドレスの複数のアイテムが1つのゾーンに含まれている場合、`--del-zone` コマンドは実行されません。

指定したネットワークアドレスまたはインデックスが存在しない場合、エラーメッセージが表示されます。

ウェブ脅威対策

ウェブ脅威対策コンポーネントを使用すると、HTTP、HTTPS、FTP 経由の受信トラフィック、Web サイト、および IP アドレスをスキャンし、インターネットからの悪意のあるファイルのダウンロードを防止し、フィッシング、アドウェア、その他の悪意のある Web サイトへのアクセスをブロックできます。

この機能は、KESL コンテナではサポートされていません。

ネットワーク脅威対策が有効になっている場合、インターセプトされた TCP ポートの現在の接続はリセットされます。

既定では、ウェブ脅威対策タスクは無効です。ただし、デバイスでウェブ脅威対策設定のローカル管理が許可されており（ポリシーが適用されていないか、ポリシーのプロパティで「ロック」に設定されていない）、スナップ形式を含む次のブラウザーの実行ファイルのいずれかがシステム上で検知されている場合、この機能は自動的に有効になります。

- chrome
- chromium
- chromium-browser
- firefox
- firefox-esr
- google-chrome
- opera
- yandex-browser

ウェブ脅威対策を有効または無効にしたり、次の保護設定を行うことができます：

- 危険なオブジェクトが検知された Web リソースに対して本製品が実行する処理を選択します。
- 信頼する URL のリストを設定します。本製品は、このリストに含まれる URL の Web サイトのコンテンツをスキャンしません。
- アプリケーションが受信トラフィックをスキャンするときに検知するオブジェクトを選択します。
- HTTPS トラフィックをスキャンするように暗号化された接続スキャンを設定します。

  FTP トラフィックをスキャンするには、暗号化された接続スキャンの設定ですべてのネットワークポートの管理を設定する必要があります。

Web サイトが開かれると、アプリケーションは次の処理を実行します：

1. Web サイトのセキュリティを、ダウンロード済みの定義データベースを使用してチェックします。
2. Web サイトのセキュリティを、ヒューリスティック分析（有効に設定されている場合）を使用してチェックします。

ヒューリスティック分析中、オペレーティングシステムのアプリケーションの動作が分析されます。ヒューリスティック分析により、現在 Kaspersky Endpoint Security のデータベースに記録がない危険なオブジェクトを検知することができます。

3. Kaspersky Security Network の使用が有効になっている場合、Kasperskyのレピュテーションデータベースを使用して、Web サイトの信頼性をチェックします。

ウェブ脅威対策の効果を高めるために、Kaspersky Security Network の使用を有効にすることを推奨します。

4. Web サイトをブロックするか、開くことを許可します。

危険な Web サイトを開こうとした時は、次の処理が実行されます：

- HTTP または FTP トラフィックの場合、アクセスをブロックして警告メッセージを表示します。
- HTTPS トラフィックの場合、ブラウザーにエラーページが表示されます。

アプリケーション証明書を削除すると、Web 脅威対策コンポーネントが正しく機能しなくなる可能性があります。

Kaspersky Endpoint Security は、許可ルール（kesl_bypass）の特別なチェーンを、iptables および ip6tables ユーティリティの mangle テーブルのリストに追加します。この許可ルールのチェーンにより、製品のスキャンからトラフィックを除外できます。トラフィック除外ルールがチェーンに設定されている場合、ウェブ脅威対策コンポーネントの動作に影響を与えます。

Web コンソールでのウェブ脅威対策の設定

Web コンソールでは、ポリシーのプロパティ内でウェブ脅威対策設定を行うことができます（**アプリケーション設定 → 脅威対策 → ウェブ脅威対策**）。

ウェブ脅威対策コンポーネントの設定

設定	説明
ウェブ脅威対策の有効化 / 無効化	この切り替えボタンでは、ウェブ脅威対策を有効にするかどうかを選択します。 この切り替えボタンは既定でオフになっています。
脅威の検知時の処理	このセクションでは、危険なオブジェクトが検知された Web リソースで実行する処理を指定できます： • **通知する**：危険なオブジェクトが Web トラフィックで検知された時にユーザーに通知します。ウェブ脅威対策は、このオブジェクトのデバイスへのダウンロードを許可します。その際、アプリケーションは危険なオブジェクトに関する情報を記録し、アクティブな脅威のリストに追加します。 • **ブロック**：Web トラフィックで検知された危険なすべてのオブジェクトへのアクセスをブロックし、アクセスがブロックされたことを通知で表示します。また、危険なオブジェクトに関する情報をログに記録します（既定値）。

悪意のあるオブジェクトを検知する	このチェックボックスでは、悪意のあるURLのデータベースにリンク先が登録されていないかどうかのチェックを有効または無効にします。 既定では、このチェックボックスはオンです。
フィッシングリンクを検知する	このチェックボックスでは、リンク先がフィッシングサイトのURLのデータベースにリンク先が登録されていないかどうかのチェックを有効または無効にします。 既定では、このチェックボックスはオンです。
フィッシングリンク検知用のヒューリスティック分析を使用する	このチェックボックスでは、フィッシングリンクの検知にヒューリスティック分析を使用するかどうかを選択します。 このチェックボックスは［**フィッシングリンクを検知する**］がオンの場合に使用でき、既定で選択されています。
アドウェアを検知する	このチェックボックスでは、アドウェアに関連するURLのデータベースにリンク先が登録されていないかどうかのチェックを有効または無効にします。 既定では、このチェックボックスはオフです。
ユーザーに損害を与える目的で悪用される可能性がある正規のアプリケーションを検知するします。	このチェック ボックスでは、侵入者がデバイスやデータを侵害するために使用できる正規のアプリケーションのデータベースに対するリンクのチェックを有効または無効にします。 既定では、このチェックボックスはオフです。
信頼するURL	この表には、コンテンツを信頼するWebページのURLが表示されます。 信頼するURLのリストには、HTTP / HTTPSプロトコルのURLのみを追加できます。 URLの指定にマスクを使用できます。IPアドレスの指定は、マスクをサポートしていません。 アドレスマスクを作成する場合は、アスタリスク記号（*）を1文字以上の文字列を表すプレースホルダーとして使用します。URLのマスクとして「*abc*」と入力した場合、「abc」という文字の並びを含むすべてのURLに適用されます（例：www.virus.com/download_virus/page_0-9abcdef.html）。アスタリスクをマスクとしての用途ではなく、通常の文字としてURLマスク中で使用する場合は、「*」を2個続けて入力します（例：「www.virus.com/**/page_0-9abcdef.html」と入力すると、「www.virus.com/*/page_0-9abcdef.html」と解釈されます）。 既定では、この表は空です。 表内のURLは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［URL］ウィンドウ

このウィンドウで、信頼する URL のリストに URL または URL のマスクを追加できます。

信頼する URL のリストには、HTTP/HTTPS プロトコルの URL のみを追加できます。URL の指定にマスクを使用できます。IP アドレスの指定は、マスクをサポートしていません。

アドレスマスクを作成する場合は、アスタリスク記号（*）を 1 文字以上の文字列を表すプレースホルダーとして使用します。URL のマスクとして「*abc*」と入力した場合、「abc」という文字の並びを含むすべての URL に適用されます（例：www.virus.com/download_virus/page_0-9abcdef.html）。アスタリスクをマスクとしての用途ではなく、通常の文字として URL マスク中で使用する場合は、「*」を 2 個続けて入力します（例：「www.virus.com/**/page_0-9abcdef.html」と入力すると、「www.virus.com/*/page_0-9abcdef.html」と解釈されます）。

管理コンソールでのウェブ脅威対策の設定

管理コンソールでは、ポリシーのプロパティ内でウェブ脅威対策設定を行うことができます（**脅威対策 → ウェブ脅威対策**）。

ウェブ脅威対策コンポーネントの設定

設定	説明
ウェブ脅威対策を有効にする	このチェックボックスでは、ウェブ脅威対策を有効にするかどうかを選択します。 既定では、このチェックボックスはオフです。
信頼する URL	この設定グループには、［**設定**］が含まれています。クリックすると、［**信頼する URL**］ウィンドウが表示され、信頼する URL のリストを指定できます。本製品は、このリストに含まれる URL の Web サイトのコンテンツをスキャンしません。
脅威の検知時の処理	危険なオブジェクトが検知された Web リソースに対して本製品が実行する処理： • **ブロック**：Web トラフィックで検知された危険なすべてのオブジェクトへのアクセスをブロックし、アクセスがブロックされたことを通知で表示します。また、危険なオブジェクトに関する情報をログに記録します（既定値）。 • **通知する**：危険なオブジェクトが Web トラフィックで検知された時にユーザーに通知します。ウェブ脅威対策は、このオブジェクトのデバイスへのダウンロードを許可します。その際、アプリケーションは危険なオブジェクトに関する情報を記録し、アクティブな脅威のリストに追加します。
スキャン設定	この設定グループには、［**設定**］が含まれています。クリックすると、［**スキャン設定**］ウィンドウが表示され、受信トラフィックのスキャンを設定できます。

［信頼する URL］ウィンドウ

このウィンドウでは、コンテンツが信頼できると思われる URL と Web ページを追加します。

信頼する URL のリストには、HTTP / HTTPS プロトコルの URL のみを追加できます。URL の指定にマスクを使用できます。IP アドレスの指定は、マスクをサポートしていません。既定では、このリストは空です。

URL のマスクを作成する場合は、アスタリスク記号（*）を 1 文字以上の文字列を表すワイルドカードとして使用します。URL のマスクとして「*abc*」と入力した場合、「abc」という文字の並びを含むすべての URL に適用されます（例：www.virus.com/download_virus/page_0-9abcdef.html）。アスタリスクをマスクとしての用途ではなく、通常の文字として URL マスク中で使用する場合は、「*」を 2 個続けて入力します（例：「www.virus.com/**/page_0-9abcdef.html」と入力すると、「www.virus.com/*/page_0-9abcdef.html」と解釈されます）。

URL は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［URL］ウィンドウ

このウィンドウで、信頼する URL のリストに URL または URL のマスクを追加できます。

信頼する URL のリストには、HTTP/HTTPS プロトコルの URL のみを追加できます。URL の指定にマスクを使用できます。IP アドレスの指定は、マスクをサポートしていません。

アドレスマスクを作成する場合は、アスタリスク記号（*）を 1 文字以上の文字列を表すプレースホルダーとして使用します。URL のマスクとして「*abc*」と入力した場合、「abc」という文字の並びを含むすべての URL に適用されます（例：www.virus.com/download_virus/page_0-9abcdef.html）。アスタリスクをマスクとしての用途ではなく、通常の文字として URL マスク中で使用する場合は、「*」を 2 個続けて入力します（例：「www.virus.com/**/page_0-9abcdef.html」と入力すると、「www.virus.com/*/page_0-9abcdef.html」と解釈されます）。

［スキャンの設定］ウィンドウ

このウィンドウでは、ウェブ脅威対策の動作中に受信トラフィックのスキャンの設定ができます。

ウェブ脅威対策の設定

設定	説明
悪意のあるオブジェクトを検知する	このチェックボックスでは、悪意のある URL のデータベースにリンク先が登録されていないかどうかのチェックを有効または無効

	にします。 既定では、このチェックボックスはオンです。
フィッシングリンクを検知する	このチェックボックスでは、リンク先がフィッシングサイトの URL のデータベースにリンク先が登録されていないかどうかのチェックを有効または無効にします。 既定では、このチェックボックスはオンです。
フィッシングリンク検知用のヒューリスティック分析を使用する	このチェックボックスでは、フィッシングリンクの検知にヒューリスティック分析を使用するかどうかを選択します。 このチェックボックスは［**フィッシングリンクを検知する**］がオンの場合に使用でき、既定で選択されています。
アドウェアを検知する	このチェックボックスでは、アドウェアに関連する URL のデータベースにリンク先が登録されていないかどうかのチェックを有効または無効にします。 既定では、このチェックボックスはオフです。
ユーザーに損害を与える目的で悪用される可能性がある正規のアプリケーションを検知するします。	このチェック ボックスでは、侵入者がデバイスやデータを侵害するために使用できる正規のアプリケーションのデータベースに対するリンクのチェックを有効または無効にします。 既定では、このチェックボックスはオフです。

コマンドラインでのウェブ脅威対策の設定

コマンドラインでは、ウェブ脅威対策の事前定義済みタスク（*Web_Threat_Protection*）を使用してウェブ脅威対策を管理できます。

このタスクは、対応しているいずれかのブラウザがシステムで検出され、デバイスでウェブ脅威対策設定のローカル管理が許可されている場合（ポリシーが適用されていないか、ポリシーのプロパティで「ロック」に設定されていない場合）に自動的に開始されます。

タスクは、手動で開始および停止できます。ウェブ脅威対策の設定は、ウェブ脅威対策の事前定義済みタスクの設定を編集することで構成できます。

ウェブ脅威対策タスクの設定

設定	説明	値
`ActionOnDetect`	Web トラフィック中の感染したオブジェクトの検知時に実行する処理を指定します。	`Inform` - 検知されたオブジェクトのダロードを許可し、ブロックされたアクセ試行について通知を表示し、感染したオジェクトに関する情報をログに記録します。 `Block`（既定値） - 検知されたオブジェトへのアクセスをブロックし、ブロックれたアクセス試行について通知を表示し感染したオブジェクトに関する情報をロに記録します。
`CheckMalicious`	悪意のある URL のデータベースにリンク先が登録されていないかどうかのチェックを有効または無効にします。	`Yes`（既定値） - リンクが悪意のあるリクのデータベースに存在するかどうかをェックします。 `No` - リンクが悪意のあるリンクのデースに存在するかどうかをチェックしまん。

CheckPhishing	フィッシング URL のデータベースにリンク先が登録されていないかどうかのチェックを有効または無効にします。	Yes（既定値）- リンクがフィッシングンクのデータベースに存在するかどうかチェックします。 No - リンクがフィッシングリンクのデベースに存在するかどうかをチェックしせん。
UseHeuristicForPhishing	Web ページのフィッシングリンクのスキャンにヒューリスティック分析を使用するかどうかを設定します。	Yes（既定値）- フィッシングリンクの知にヒューリスティック分析を使用しす。この値を指定すると、ヒューリステック分析のレベルが Light に設定され（徹底度が最も低いスキャンを行い、システムへの負荷は最小です）。ウェブ脅威策のヒューリスティック分析のレベルは更できません。 No - フィッシングリンク検知用のヒュースティック分析を使用しません。
CheckAdware	アドウェア URL のデータベースにリンク先が登録されていないかどうかのチェックを有効または無効にします。	Yes - リンクがアドウェアリンクのデベースに存在するかどうかをチェックします。 No（既定値）- リンクがアドウェアリンのデータベースに存在するかどうかをチックしません。
CheckOther	侵入者がデバイスやデータを侵害するために使用できる正規のアプリケーションを含む URL のデータベースに対するリンクのスキャンを有効または無効にします。	Yes - デバイスやデータに損害を与える的で悪用される可能性がある正規のアケーションを含む URL のデータベースンクが登録されているかをチェックします。 No（既定値）- デバイスやデータに損害与える目的で悪用される可能性がある正のアプリケーションを含む URL のデースにリンクが登録されているかをチェクしません。
UseTrustedAddresses	信頼する URL のリストの使用を有効または無効にします。このアプリケーションは、信頼できる URL をスキャンしてウイルスやその他の悪意のあるオブジェクトを検出することはありません。TrustedAddresses.item_# パラメータを使用して、信頼する URL を指定できます。	Yes（既定値）- 信頼する URL のリスト使用します。 No - 信頼する URL のリストを使用しません。
TrustedAddresses.item_#	信頼する URL を指定します。	既定値は定義されていません。 URL の指定にマスクを使用できます。

		アドレスマスクを作成する場合は、アスタリスク記号（*）を1文字以上の文字列を表すプレースホルダーとして使用します。URL のマスクとして「*abc*」と入力した場合、「abc」という文字の並びを含むすべての URL に適用されます（例：www.virus.com/download_virus/page_0-9abcdef.html）。アスタリスクをマスクとしての用途ではなく、通常の文字として URL マスク中で使用する場合は、「*」を 2 個続けて入力します（例：「www.virus.com/**/page_0-9abcdef.html」と入力すると、「www.virus.com/*/page_0-9abcdef.html」と解釈されます）。 IP アドレスの指定は、マスクをサポートしていません。

暗号化された接続のスキャン

暗号化された接続スキャンの設定は、ウェブ脅威対策およびウェブコントロールコンポーネントの操作に使用されます。ウェブ脅威対策コンポーネントは、安全な接続を介して送信されたネットワークトラフィックを復号化し、検査できます。暗号化接続スキャンは既定で有効になっています。

暗号化接続スキャンを有効または無効にしたり、スキャン設定を構成することができます：

- 信頼されない証明書の検知時に実行される処理を選択します。
- 暗号化された接続のスキャンエラーが Web サイトで発生した場合に実行する処理を選択します。
- 証明書の検証にインターネットを使用することを有効または無効にします。
- 信頼済みドメインのリストを表示し、設定します。指定したドメインへのアクセス時に確立された、暗号化された接続をスキャンしません。
- 暗号化された接続スキャンを実行する際に、アプリケーションが信頼済みとみなす証明書のリストを構成します。
- アプリケーションで監視するネットワークポートのリストを設定します。監視するネットワークポートまたはネットワークポートの範囲を指定できます。

暗号化された接続のスキャン設定が変更された場合は、*NetworkSettingsChanged* イベントがログファイルに記録されます。

Web コンソールでの暗号化された接続スキャンの設定

Web コンソールでは、ポリシーのプロパティで暗号化された接続スキャンの設定を構成できます（**製品設定 → 全般設定 → ネットワーク設定**）。

暗号化された接続のスキャン設定

設定	説明
暗号化された接続のスキャンが有効または無効です	この切り替えボタンでは、暗号化された接続のスキャンを実行するかどうかを選択します。 この切り替えボタンは既定でオンになっています。
信頼するルート証明書	**信頼するルート証明書を管理**をクリックすると、**信頼するルート証明書**ウィンドウが開き、信頼する証明書のリストを設定できます。信頼する証明書は、暗号化された接続をスキャンする時に使用されます。
信用できない証明書を持つドメインへの訪問	信頼する証明書を持つドメインにアクセスしたときにアプリケーションが実行する処理を選択できます： • **許可**（既定値）- 信頼できない証明書を使用してドメインに接続できるようにします。 • **ブロック**：信頼できない証明書を持つドメインへの接続をブロックします。
暗号化された接続のスキャンでエラーが	暗号化された接続のスキャンエラーが発生したドメインにアクセスしたときにアプリケーションが実行する処理を選択できます。

発生するドメインへのアクセス	• **ドメインを許可および除外に追加**（既定値）- エラーの発生したドメインをスキャンエラーが発生したドメインのリストに追加し、このドメインへのアクセス時には暗号化されたネットワークトラフィックをスキャンしないように設定します。 • **ブロック** - スキャンエラーのあるドメインへの接続をブロックします。
証明書検証ポリシー	証明書を検証する方法を選択できます： • **ローカルチェック**：証明書の検証にインターネットを使用しません。 • **完全チェック**（既定値）- 証明書の検証にインターネットを使用し、証明書の検証に必要だが存在しないチェーンをダウンロードします。
信頼するドメイン	**信頼するドメインの設定**をクリックすると、**信頼するドメイン**ウィンドウが開き、信頼するドメイン名のリストを設定できます。
すべてのネットワークポートを監視する	このオプションをオンにすると、すべてのネットワークポートを監視します。
選択したネットワークポートのみを監視する	このオプションをオンにすると、**監視対象ポート**ウィンドウで指定されたネットワークポートのみを監視します。 既定では、このオプションがオンです。
監視対象ポート	**ネットワークポートの設定**をクリックすると**ネットワークポート**ウィンドウが表示され、本製品が監視するネットワークポートを指定することができます。

［信頼する証明書］ウィンドウ

Kaspersky Endpoint Security が信頼できるとみなす証明書のリストを設定できます。信頼する証明書のリストは、暗号化された接続をスキャンする時に使用されます。

証明書ごとに次の情報が表示されます：

- 証明書のサブジェクト
- シリアル番号
- 証明書の発行者
- 証明書の開始日
- 証明書の有効期間が終了する日
- SHA256 証明書のフィンガープリント

既定では、証明書のリストは空です。

証明書は、追加、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

［信頼する証明書の追加］ウィンドウ

このウィンドウでは、Kaspersky Endpoint Security で信頼する証明書を追加できます。

［**証明書を追加する**］をクリックすると、標準のファイル選択ウィンドウが表示されます。証明書を含むファイル（DER または PEM 形式）へのパスを指定します。

証明書ファイルを選択すると、ウィンドウに証明書情報とそのファイルのパスが表示されます。

［信頼するドメイン］ウィンドウ

このリストには、暗号化された接続のスキャンから除外されるドメイン名とドメイン名のマスクが表示されます。

例：`*example.com`。たとえば、`*example.com/*` は、Web ページではなくドメインアドレスを指定する必要があるため、正しくありません。

既定では、このリストは空です。

信頼するドメインのリストでドメインを追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

監視対象ポート

この表には、**ネットワーク設定**ウィンドウの**監視対象ポート**で**選択したネットワークポートのみを監視する**オプションが選択されている場合に、アプリケーションが監視する必要のあるネットワークポートが含まれています。

このリストには 2 つの列があります：

- **ポート** - 監視対象のポートです。
- **説明** - 監視対象ポートの説明です。

既定では、メールとネットワークトラフィックの送受信で通常使用されるネットワークポートのリストを表示します。このネットワークポートのリストは、本製品のパッケージに含まれています。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

管理コンソールでの暗号化された接続スキャンの設定

管理コンソールでは、ポリシーのプロパティで暗号化された接続スキャンの設定を構成できます（**全般設定 → ネットワーク設定**）。

暗号化された接続のスキャン設定

設定	説明
暗号化された接続のスキャンの有効化	このチェックボックスでは、暗号化された接続のスキャンを実行するかどうかを選択します。 既定では、このチェックボックスはオンです。
信用できない証明書を持つドメインへの訪問	ドロップダウンリストでは、信頼できない証明書を持つドメインにアクセスしたときにアプリケーションが実行する処理を選択できます： • **許可**（既定値）- 信頼できない証明書を使用してドメインに接続できるようにします。 • **ブロック**：信頼できない証明書を持つドメインへの接続をブロックします。
暗号化された接続のスキャンでエラーが発生するドメインへのアクセス	ドロップダウンリストでは、暗号化された接続のスキャンエラーが発生したドメインにアクセスしたときにアプリケーションが実行する処理を選択できます： • **ドメインを許可および除外に追加**（既定値）- エラーの発生したドメインをスキャンエラーが発生したドメインのリストに追加し、このドメインへのアクセス時には暗号化されたネットワークトラフィックをスキャンしないように設定します。 • **ブロック** - スキャンエラーのあるドメインへの接続をブロックします。
証明書検証ポリシー	このドロップダウンリストでは、証明書を検証する方法を選択できます： • **ローカルチェック**：証明書の検証にインターネットを使用しません。 • **完全チェック**（既定値）- 証明書の検証にインターネットを使用し、証明書の検証に必要だが存在しないチェーンをダウンロードします。
信頼するドメイン	この設定グループには、**設定**が含まれています。クリックすると、**信頼するドメイン**ウィンドウが表示され、信頼するドメインのリストを設定できます。
信頼するルート証明書	この設定グループには、**設定**が含まれています。クリックすると、**信頼するルート証明書**ウィンドウが表示され、信頼するルート証明書のリストを設定でき

	ます。信頼する証明書は、暗号化された接続をスキャンする時に使用されます。
ネットワークポートの設定	この設定グループには、**設定**が含まれています。このボタンをクリックすると、**監視対象ポート**ウィンドウが表示されます。

［信頼するドメイン］ウィンドウ

このリストには、暗号化された接続のスキャンから除外されるドメイン名とドメイン名のマスクが表示されます。

例：*example.com。たとえば、*example.com/* は、Web ページではなくドメインアドレスを指定する必要があるため、正しくありません。

既定では、このリストは空です。

信頼するドメインのリストでドメインを追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［信頼する証明書］ウィンドウ

Kaspersky Endpoint Security が信頼できるとみなす証明書のリストを設定できます。信頼する証明書のリストは、暗号化された接続をスキャンする時に使用されます。

証明書ごとに次の情報が表示されます：

- **主体者** - 証明書のサブジェクト
- **シリアル番号** – 証明書のシリアル番号
- **発行者** – 証明書の発行者
- **有効期間の開始日** – 証明書の開始日
- **有効期限** – 証明書の終了日
- **SHA256 フィンガープリント**は、SHA256 証明書のフィンガープリントです。

既定では、証明書のリストは空です。

証明書は、追加、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

証明書ウィンドウの追加

このウィンドウでは、次のいずれかの方法で、証明書を信頼する証明書リストに追加できます：

- 証明書ファイルへのパスを指定します。［**参照**］をクリックすると、標準のファイル選択ウィンドウが表示されます。証明書を含むファイル（DER または PEM 形式）へのパスを指定します。
- ［**証明書の詳細を入力**］フィールドに証明書ファイルの内容をコピーします。

監視対象ポート

ネットワークポートの設定

設定	説明
すべてのネットワークポートを監視する	このオプションをオンにすると、すべてのネットワークポートを監視します。
選択したネットワークポートのみを監視する	このオプションをオンにすると、表で指定したネットワークポートのみが監視されます。 既定では、このオプションがオンです。
ネットワークポートの設定	この表には、［**指定したポートのみを監視する**］がオンの場合に監視されるネットワークポートが表示されます。このリストには 2 つの列があります： • **ポート** - 監視対象のポートです。 • **説明** - 監視対象ポートの説明です。 既定では、メールとネットワークトラフィックの送受信で通常使用されるネットワークポートのリストを表示します。このネットワークポートのリストは、本製品のパッケージに含まれています。 表内の項目は、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

コマンドラインでの暗号化された接続スキャンの設定

暗号化された接続スキャンの設定を管理するための特別な管理コマンドがコマンドラインで提供されます。暗号化された接続スキャンの設定を管理するコマンドを使用すると、次の操作が可能になります：

- 暗号化された接続スキャンの設定を構成。
- 暗号化された接続のスキャンからの除外を表示。
- アプリケーションがスキャンから自動的に除外したドメインのリストを消去。
- アプリケーションが信頼できると見なす証明書のリストを管理。

暗号化された接続スキャンの設定の表示および編集

特別な管理コマンドを使用して、暗号化された接続スキャンの設定を表示および編集できます。

- 暗号化された接続スキャンの設定の現在の値をコンソールまたは設定情報ファイルに出力できます。このファイルを使用して設定を編集できます。
- 設定を含む設定情報ファイルを使用して、暗号化された接続スキャンのすべての設定を編集できます。暗号化された接続スキャンの設定を表示するコマンドを使用して設定情報ファイルを取得できます。
- コマンドラインキーを使用して、< 設定名 >=< 設定値 > の形式で個々の設定を編集できます。暗号化された接続スキャンの設定を表示するコマンドを使用して、設定の現在の値を取得できます。

暗号化された接続スキャンの設定の現在の値をコンソールに出力するには、次のコマンドを実行します：

```
kesl-control --get-net-settings [--json]
```

`--json` を指定すると、設定はJSON形式で出力されます。もし `--json` キーが指定されなければ、設定はINI形式でインポートされます。

暗号化された接続スキャンの設定の現在の値をファイルに出力するには、次のコマンドを実行します：

```
kesl-control --get-net-settings --file <設定情報ファイルの絶対パス> [--json]
```

説明：

- `--file` < 設定情報ファイルへのパス > は、暗号化された接続スキャンの設定が保存される設定情報ファイルへのパスです。パスを指定しないでファイルの名前を指定した場合、そのファイルは現在のディレクトリに作成されます。指定された名前のファイルが指定されたパスに既に存在する場合は、上書きされます。指定されたディレクトリがディスクに見つからない場合、ファイルは作成されません。
- `--json` を指定すると、設定はJSON形式で出力されます。もし `--json` キーが指定されなければ、設定はINI形式でインポートされます。

設定情報ファイルを使用して暗号化された接続スキャンの設定値を編集するには、次の手順を実行します。

1. 上で説明したように、アプリケーションの全般設定を設定情報ファイルに出力します。
2. ファイル内の必要なパラメータの値を編集し、変更を保存します。
3. コマンドを実行します：

   `kesl-control --set-net-settings --file <` 設定情報ファイルの絶対パス `> [--json]`

   説明：

   - `--file <` 設定情報ファイルへのパス `>` は、暗号化された接続スキャンの設定が含まれる設定情報ファイルへの絶対パスです。
   - `--json` を指定すると、設定情報ファイルの設定を JSON 形式で本製品にインポートします。`--jason` のライセンスが指定されていない場合、設定は INI ファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

   ファイル内で定義されている暗号化された接続スキャンの設定のすべての値がアプリケーションにインポートされます。

コマンドラインを使用して暗号化された接続スキャンの設定値を編集するには、次のコマンドを実行します：

`kesl-control --set-net-settings <` 設定名 `>=<` 設定値 `> [<` 設定名 `>=<` 設定値 `>]`

`<` 設定名 `>=<` 設定値 `>` は、暗号化された接続スキャンの設定の 1 つの名前と値です。

暗号化された接続のスキャンに指定された設定値が変更されます。

暗号化接続スキャンからの除外の表示

暗号化された接続のスキャンから除外されるリストは次のとおりです：

- ユーザーが追加した除外項目のリスト
- 本製品によって追加された除外項目のリスト
- 本製品のデータベースから受信した除外項目のリスト

ユーザーが追加した、安全な接続のスキャンの除外リストを表示するには、次のコマンドを実行します：

```
kesl-control -N --query user
```

ユーザーが追加した、安全な接続のスキャンの除外リストを表示するには、次のコマンドを実行します：

```
kesl-control -N --query auto
```

本製品のデータベースから受け取った、安全な接続のスキャンの除外リストを表示するには、次のコマンドを実行します：

```
kesl-control -N --query kl
```

本製品が自動的にスキャン対象から除外するドメインのリストをクリアするには、次のコマンドを実行します：

```
kesl-control -N --clear-web-auto-excluded
```

信頼する証明書のリストの管理

信頼する証明書のリストに証明書を追加するには、次のコマンドを実行します：

```
kesl-control --add-certificate <path to certificate>
```

説明：

< 証明書のパス > は、追加する証明書ファイルへのパスです（PEM または DER 形式）。

信頼する証明書のリストから証明書を削除するには、次のコマンドを実行します：

```
kesl-control --remove-certificate <certificate subject>
```

信頼する証明書のリストを表示するには、次のコマンドを実行します：

```
kesl-control --list-certificates
```

証明書ごとに次の情報が表示されます：

- 証明書のサブジェクト
- シリアル番号
- 証明書の発行者
- 証明書の開始日
- 証明書の有効期間が終了する日
- SHA256 証明書のフィンガープリント

ネットワーク脅威対策

ネットワーク脅威対策は、受信ネットワークトラフィックにネットワーク攻撃に特有の動作が含まれていないかどうかスキャンします。

この機能は、KESL コンテナではサポートされていません。

Kaspersky Endpoint Security は、現在の定義データベースから TCP ポートの番号を取得し、これらのポートの受信トラフィックをスキャンします。

ネットワークトラフィックをスキャンするために、ネットワーク脅威対策タスクは定義データベースからポート番号を取得し、これらすべてのポートを経由する接続を受け入れます。ネットワークスキャンプロセス中に、システム上のアプリケーションがこのポートをリッスンしていなかったとしても、デバイスのポートが開いているように見える場合があります。未使用のポートはファイアウォールで閉じておくことを推奨します。

ネットワーク脅威対策が有効になっている場合、インターセプトされた TCP ポートの現在の接続はリセットされます。

ネットワーク脅威対策が有効になっている場合、保護対象デバイスに対するネットワーク攻撃の試みが検知されると、アプリケーションは攻撃デバイスからのネットワークアクティビティをブロックし、*ネットワーク攻撃検知イベント*を作成します。イベントには、攻撃デバイスに関する情報が含まれています。

既定では、攻撃デバイスからのネットワークトラフィックは 1 時間ブロックされます。ブロック時間が経過すると、アプリケーションはデバイスのブロックを解除します。

ネットワーク脅威対策は、デバイス上のネットワーク脅威対策設定がポリシーで定義されている場合に、既定で有効になっています。ローカルで構成された設定がデバイスに適用されている場合、ネットワーク脅威対策は既定で無効になります。

ネットワーク脅威対策を有効または無効にしたり、次の保護設定を行うことができます：

- ネットワーク攻撃に典型的なネットワークアクティビティの検知時にアプリケーションが実行する処理を選択します。
- ネットワーク攻撃の試行の検知時に、ネットワーク活動のブロックを有効または無効にします。
- 攻撃元のデバイスをブロックする期間を設定します。
- 本製品がそのネットワーク活動をブロックしない IP アドレスのリストを構成します。

コマンドラインでブロックされたデバイスを管理するコマンドを使用して、ブロックされたデバイスのリストを表示し、これらのデバイスのブロックを手動で解除することができます。Kaspersky Security Center には、*ネットワーク攻撃が検知された*イベントを除き、ブロックされたデバイスを監視および管理するためのツールはありません。

Kaspersky Endpoint Security は、許可ルール（kesl_bypass）の特別なチェーンを、iptables および ip6tables ユーティリティの mangle テーブルのリストに追加します。この許可ルールのチェーンにより、製品のスキャンからトラフィックを除外できます。トラフィック除外ルールがチェーンに設定されている場合、ネットワーク脅威対策タスクの動作に影響を与えます。たとえば、送信 HTTP トラフィックを除外するには、コマンド `iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT` を追加する必要があります。

Web コンソールでのネットワーク脅威対策の設定

Web コンソールでは、ポリシーのプロパティ内でネットワーク脅威対策設定を行うことができます（**アプリケーション設定 → 脅威対策 → ネットワーク脅威対策**）。

ネットワーク脅威対策コンポーネントの設定

設定	説明
ネットワーク脅威対策の有効化 / 無効化	この切り替えボタンでは、ネットワーク脅威対策を有効にするかどうかを選択します。 この切り替えボタンは既定でオンになっています。
脅威の検知時の処理	ネットワーク攻撃に典型的なネットワーク活動の検知時に実行する処理。 • ユーザーに**通知**します。ネットワーク活動を許可し、検知したネットワーク活動に関する情報をログに記録します。 • 攻撃元デバイスからのネットワーク活動を**ブロック**し、検知したネットワーク活動（既定値）に関する情報をログに記録します。
攻撃元コンピューターのブロックの有効化 / 無効化	この切り替えボタンは、ネットワーク攻撃の試行の検知時に、ネットワーク活動をブロックするかどうかを選択します。 この切り替えボタンは既定でオンになっています。
攻撃元デバイスをブロックする時間（分）	このフィールドでは、攻撃元ホストがブロックされる時間を分単位で指定します。指定された時間が経過すると、対象のホストからのネットワーク活動を許可します。 取りうる値：1～32768 の整数。 既定値：60
除外	この表には、IP アドレスのリストが表示されます。ここで設定したアドレスからのネットワーク攻撃は、ブロックされません。既定では、このリストは空です。 表内の IP アドレスは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［IP アドレス］ウィンドウ

このウィンドウでは、IP アドレスの追加や編集ができます。ここで設定した IP アドレスからのネットワーク攻撃は、ブロックされません。

IP アドレス

設定	説明
IP アドレスを入力	IP アドレスの入力フィールド。 IPv4 または IPv6 形式の IP アドレスを指定できます。

管理コンソールでのネットワーク脅威対策の設定

管理コンソールでは、ポリシーのプロパティ内でネットワーク脅威対策設定を行うことができます（**脅威対策 → ネットワーク脅威対策**）。

ネットワーク脅威対策コンポーネントの設定

設定	説明
ネットワーク脅威対策を有効にする	このチェックボックスでは、ネットワーク脅威対策を有効にするかどうかを選択します。 既定では、このチェックボックスはオンです。
脅威の検知時の処理	ネットワーク攻撃に典型的なネットワーク活動の検知時に実行する処理。 • ユーザーに**通知**します。ネットワーク活動を許可し、検知したネットワーク活動に関する情報をログに記録します。 • 攻撃元デバイスからのネットワーク活動を**ブロック**し、検知したネットワーク活動（既定値）に関する情報をログに記録します。
デバイスへの攻撃をブロックする	このチェックボックスは、ネットワーク攻撃の試行の検知時に、ネットワーク活動をブロックするかどうかを選択します。 既定では、このチェックボックスはオンです。
攻撃元デバイスをブロックする時間（分）	このフィールドでは、攻撃元ホストがブロックされる時間を分単位で指定します。指定された時間が経過すると、対象のホストからのネットワーク活動を許可します。 取りうる値：1～32768 の整数。 既定値：60
除外	この設定グループには、［**設定**］が含まれています。クリックすると、［**除外**］ウィンドウが表示され、IP アドレスのリストを指定できます。ここで設定した IP アドレスからのネットワーク攻撃は、ブロックされません。

［除外］ウィンドウ

このウィンドウでは、ネットワーク攻撃がブロックされない IP アドレスを追加できます。

既定では、このリストは空です。

リスト内の IP アドレスは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［IP アドレス］ウィンドウ

このウィンドウでは、IP アドレスの追加や編集ができます。ここで設定した IP アドレスからのネットワーク攻撃は、ブロックされません。

IP アドレス

設定	説明
IP アドレスを入力	IP アドレスの入力フィールド。 IPv4 または IPv6 形式の IP アドレスを指定できます。

コマンドラインでのネットワーク脅威対策の設定

コマンドラインでは、ネットワーク脅威対策の事前定義済みタスク（*Network_Threat_Protection*）を使用してネットワーク脅威対策を管理できます。

既定では、ネットワーク脅威対策タスクは実行されません。タスクは、手動で開始および停止できます。

ネットワーク脅威対策の設定は、ネットワーク脅威対策の事前定義済みタスクの設定を編集することで構成できます。

ネットワーク脅威対策タスクの設定

設定	説明	値
`ActionOnDetect`	ネットワーク攻撃に典型的なネットワーク活動の検知時に実行する処理。 この設定の値を `Block` から `Notify` に変更すると、ブロックされたデバイスのリストがクリアされます。	`Notify` - ネットワーク活動を許可し、検知したネットワーク活動の情報をログに記録します。この値が指定されている場合、`Block AttackingHosts` パラメータの値は無視されます。 `Block`（既定値） - ネットワーク活動をブロックし、その情報をログに記録します。
`BlockAttackingHosts`	攻撃元デバイスのネットワーク活動をブロックします。	`Yes`（既定値）— 攻撃元デバイスのネットワーク動作をブロックします。

		No – 攻撃元デバイスのネットワーク動作をブロックしません。この値が指定され、ActionOnDetect パラメータが Block に設定されている場合、アプリケーションは攻撃元デバイスからのネットワーク動作をブロックしますが、ブロックされたデバイスのリストにはデバイスを追加しません。
BlockDurationMinutes	攻撃元デバイスをブロックする期間を指定します（分）。	1～32768 既定値：60
UseExcludeIPs	ネットワーク攻撃の検知時にネットワーク活動をブロックしない IP アドレスのリストの使用。本製品が危険な動作の情報を記録する対象は、これらのデバイスのみです。 ExcludeIPs.item_# 設定を使用して、IP アドレスを除外リストに追加できます。	Yes – 除外された IP アドレスのリストを使用します。 No（既定値） – 除外された IP アドレスのリストを使用しません。
ExcludeIPs.item_#	本製品がそのネットワーク活動をブロックしない IP アドレスを指定します。既定では、このリストは空です。	d.d.d.d – IPv4 アドレス、d は 10 進数の 0 - 255。 d.d.d.d/p – IPv4 のサブネットアドレス、p は数値 0 – 32。 x:x:x:x:x:x:x:x – IPv6 アドレス、x は 16 進数の 0 – ffff。 x:x:x:x::0/p – IPv6 のサブネットアドレス、p は数値 0 - 64。 既定値は定義されていません。

悪質なリモート暗号化に対する保護

アンチクリプターコンポーネントは、SMB / NFS プロトコルでネットワークアクセスされるローカルディレクトリのファイルを悪意のあるリモートでの暗号化から保護します。

このコンポーネントを使用するには、対応する機能を含むライセンスが必要です。

この機能は、KESL コンテナではサポートされていません。

アンチクリプターが有効な場合、Kaspersky Endpoint Security は、保護対象デバイスの共有ネットワークディレクトリにあるファイルリソースを使用して、悪意のある暗号化の有無をリモートデバイスの処理でスキャンします。共有ネットワークリソースにアクセスするリモートデバイスの処理が悪意のある暗号化であるとアプリケーションが判断した場合、アプリケーションはオペレーティングシステムのファイアウォールに対して、侵害されたデバイスからのネットワークトラフィックをブロックするルールを作成し、有効にします。侵入されたデバイスは、信頼できないデバイスのリストに追加され、すべての信頼できないデバイスに対して、共有ネットワークディレクトリへのアクセスがブロックされます。アプリケーションは、侵入されたデバイスに関する情報を含む*暗号化の検知*イベントを作成する。

既定では、信頼されないデバイスのネットワークファイルリソースへのアクセスを 30 分間ブロックします。ブロック時間が終了すると、アプリケーションは信頼できないデバイスのリストから危険なデバイスを削除し、デバイスのネットワークファイルリソースへのアクセスは自動的に回復されます。

アンチクリプターコンポーネントによって作成されたファイアウォールのルールは、iptables ユーティリティを使用して削除することはできません。本製品は 1 分ごとにルールのセットを復元します。

リモートの悪意のある暗号化に対する保護は、既定では無効になっています。

悪意のある暗号化（アンチクリプター）に対する保護を有効または無効にしたり、保護設定を構成したりすることができます：

- 暗号化が検出されたときに本製品が実行する処理を選択します。ユーザーに通知するか、悪意のある暗号化を実行しているデバイスをブロックします。

  *通知*処理を選択した場合でも、アンチクリプターが有効になっているときは、ネットワークファイル共有上のリモートデバイスの処理をスキャンして、悪意のある暗号化がないか確認します。悪意のある処理が検知された場合、*暗号化の検知*イベントが作成されますが、デバイスの侵入はブロックされません。

- 信頼できないデバイスをブロックする期間を設定します。

- アプリケーションが悪意のある暗号化から保護するファイルとディレクトリを指定します。

- 悪意のある暗号化からの保護から除外するファイルとディレクトリを指定します。

  本製品は、暗号化の保護（アンチクリプター）から除外されたディレクトリで暗号化動作が検知された場合、その動作を暗号化であると認識しません。

コマンドラインでブロックされたデバイスを管理するコマンドを使用して、ブロックされたデバイスのリストを表示し、これらのデバイスのブロックを手動で解除することができます。Kaspersky Security Center には、*暗号化が検知された*イベントを除き、ブロックされたデバイスを監視および管理するためのツールはありません。

アンチクリプターが正常に動作するには、少なくとも1つのサービス（Samba または NFS）がオペレーティングシステムにインストールされている必要があります。NFS サービスでは、rpcbind パッケージがインストールされている必要があります。

アンチクリプターコンポーネントは、SMB1、SMB2、SMB3、NFS3、TCP / UDP、および IP / IPv6 のプロトコルにおいて適切に動作します。NFS2 プロトコルと NFS4 プロトコルでの動作はサポートされていません。リソースのマウントに NFS2 プロトコルと NFS4 プロトコルを使用できないよう、サーバー設定を構成してください。

Kaspersky Endpoint Security では、デバイスの動作に悪意があると識別されるまでは、ネットワークファイルリソースへのアクセスをブロックしません。このため、悪意のある処理が検知されるまで、少なくとも1つのファイルが暗号化されます。

Web コンソールでのアンチクリプターの設定

Web コンソールでは、ポリシーのプロパティ（**製品設定 → 先進の脅威対策 → アンチクリプター**）でアンチクリプター設定を構成できます。

アンチクリプターコンポーネントの設定

設定	説明
アンチクリプターによる保護の有効化 / 無効化	この切り替えボタンは、リモートでの悪意のある暗号化から、SMB / NFS プロトコルでネットワークアクセスされるローカルディレクトリ内のファイルの保護を有効にするかどうかを選択します。 この切り替えボタンは既定でオフになっています。
保護範囲	［**保護範囲を設定する**］をクリックすると、［**保護範囲**］ウィンドウが表示されます。
暗号化の検知時の処理	悪意のある暗号化を検知した際に、Kaspersky Endpoint Security が実行する処理です。 • ユーザーに**通知**します。Kaspersky Endpoint Security は暗号化を実行するデバイスをブロックしません。悪意のある暗号化の検知に関するイベントをイベントログに記録するだけです。 • 暗号化を実行するデバイスを**ブロック**します（既定値）。
ブロックする時間（分）	このフィールドでは、信頼しないデバイスのブロック期間を分単位で指定します。 侵入されたホストがブロックされ、この設定値を変更すると、このホストのブロック時間は変更されません。ブロックの時間は動的な値ではなく、ブロックの瞬間に計算されます。 使用できる値：1～4294967295 の整数。 既定値：30
除外	［**除外リストを設定する**］をクリックすると、［**除外範囲**］ウィンドウが表示されます。
マスクによる除外	［**除外をマスクで設定する**］をクリックすると、［**マスクによる除外**］ウィンドウが表示されます。

［保護範囲］ウィンドウ

この表には、アンチクリプターコンポーネントの保護範囲が表示されます。表で指定されたパス内のファイルとディレクトリをすべてスキャンします。表には既定で、ローカルファイルシステムのすべてのディレクトリを対象とする1つのスキャン範囲が表示されています。

保護範囲設定

設定	説明
範囲名	保護範囲名。
パス	保護されるディレクトリのパス。
ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、保護範囲の表の並び順で保護されます。必要に応じて、サブディレクトリを親ディレクトリよりもリストの上に配置し、親ディレクトリとは異なるセキュリティ設定をサブディレクトリに設定します。

［保護範囲の追加］ウィンドウ

このウィンドウでは、アンチクリプターの保護範囲の追加や設定ができます。

保護範囲設定

設定	説明
範囲名	保護範囲の名前を入力するフィールド。この名前は、［**保護範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。

この範囲を使用する	このチェックボックスでは、製品がこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、コンポーネントの動作中にこの保護範囲が処理されます。 このチェックボックスをオフにすると、コンポーネントの動作中にこの保護範囲は処理されません。このチェックボックスをオンにすることにより、後からこの範囲をコンポーネントの動作設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	ドロップダウンリストからファイルシステムの種別を選択できます： • **Local**（既定値）：ローカルディレクトリ。 • **Shared**：Samba または NFS プロトコルでアクセス可能なサーバーファイルシステムリソースを表示します。 • **共有済みのすべての場所**：Samba および NFS プロトコルでアクセス可能なすべてのサーバーファイルシステムリソースを表示します。
アクセスプロトコル	ドロップダウンリストからリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 このドロップダウンリストは、ファイルシステムのドロップダウンリストから［**Shared**］を選択した場合に使用できます。
パス	保護範囲に含めるディレクトリのパスを指定するための入力フィールドです。パスの指定にマスクを使用できます。 アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「`/dir/*/file`」または「`/dir/*/*/file`」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「`/dir/**/file*/`」または「`/dir/file**/`」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「`/dir/**/**/file`」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、**?** 文字を使用して任意の文字を表示できます。 このフィールドは、ファイルシステムのドロップダウンリストから［**Local**］を選択した場合に使用できます。 このフィールドを空白のままにすることはできません。 既定では、「**/**」パスが指定されています（ルートディレクトリ）。
マスク	このリストには、アンチクリプターコンポーネントの動作中にスキャンするオブジェ

クト名のマスクが含まれます。
既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。
マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲］ウィンドウ

この表には、スキャンの除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	スキャンから除外されるディレクトリのパス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲の追加］ウィンドウ

このウィンドウでは、除外範囲の追加や設定ができます。

除外範囲の設定

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品の実行時にこの範囲を除外するかどうかを選択します。 チェックボックスをオンにすると、動作中にこの範囲がスキャンや保護の対象から除外されます。 チェックボックスをオフにすると、動作中にこの範囲がスキャンや保護の対象に含まれます。チェックボックスをオンにすることにより、この範囲をスキャンや保護の対象から後で除外できます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	このドロップダウンリストでは、スキャンの除外に追加するディレクトリがあるファイルシステムの種別を選択できます： • **Local**：ローカルディレクトリ。 • **Mounted** - デバイスにマウントされるリモートディレクトリ。 • **リモートでマウント済みのすべての場所** - Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。
アクセスプロトコル	ドロップダウンリストからリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。 このドロップダウンリストは、ファイルシステムのドロップダウンリストから［**Mounted**］を選択した場合に使用できます。
パス	除外範囲に追加するディレクトリのパスの入力フィールドです。パスの指定にマスクおよびタグを使用できます。

特別なタグを使用してコンテナまたはイメージを指定できます：

- [container-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>]/<ローカルディレクトリへのパス>
- [image-id:<識別子>]/<ローカルディレクトリへのパス>
- [image-name:<名前>]/<ローカルディレクトリへのパス>

[container-id:<識別子>]、[container-name:<名前>]、[image-id:<識別子>]、および [image-name:<名前>]/<ローカルディレクトリ> タグの一意の組み合わせを使用することもできます。

1つのエリア内で1～4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。

例：

- [container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>

名前と識別子にはマスク（? および * 記号）を使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。 マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。 ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。 このフィールドは、ファイルシステムのドロップダウンリストから［**Local**］を選択した場合に使用できます。
共有リソース名	除外範囲に追加するディレクトリがある、ファイルシステム共有リソースの名前を入力するためのフィールドです。 このフィールドは、［ファイルシステム］ドロップダウンリストで［**Mounted**］が選択され、［**アクセスプロトコル**］ドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。
マスク	このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。マスクは、［**パス**］フィールドに指定されたディレクトリ内のオブジェクトにのみ適用されます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。 このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。 マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、スキャンからのオブジェクトの除外を設定できます。指定したマスクが名前に含まれるファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

管理コンソールでのアンチクリプターの設定

管理コンソールでは、ポリシーのプロパティ（**先進の脅威対策 → アンチクリプター**）でアンチクリプター設定を構成できます。

アンチクリプターコンポーネントの設定

設定	説明

アンチクリプターによる保護を有効にする	このチェックボックスでは、リモートでの悪意のある暗号化から、SMB / NFS プロトコルでネットワークアクセスされるローカルディレクトリ内のファイルの保護を有効にするかどうかを選択します。 既定では、このチェックボックスはオフです。
保護範囲	この設定グループには、スキャン範囲と保護設定を指定できるウィンドウを開くボタンが含まれています。
除外	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**除外範囲**］ウィンドウが表示されます。このウィンドウでは、スキャンから除外する範囲のリストを指定できます。
マスクによる除外	この設定グループには［**設定**］が含まれています。クリックすると、［**マスクによる除外**］ウィンドウが表示されます。このウィンドウでは、名前のマスクにより、スキャンからのオブジェクトの除外を設定できます。

［スキャン範囲］ウィンドウ

この表にはスキャン範囲が含まれます。表で指定されたパス内のファイルとディレクトリをすべてスキャンします。表には既定で、ローカルファイルシステムのすべてのディレクトリを対象とする1つのスキャン範囲が表示されています。

スキャン範囲設定

設定	説明
範囲名	スキャン範囲名。
パス	スキャンするディレクトリのパス。
ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、範囲の表の並び順でスキャンされます。必要に応じて、サブディレクトリを親ディレクトリよりもリストの上に配置し、親ディレクトリとは異なるセキュリティ設定をサブディレクトリに設定します。

［<新しいスキャン範囲>］ウィンドウ

このウィンドウでは、アンチクリプターの保護範囲の追加や設定ができます。

保護範囲設定

設定	説明
範囲名	保護範囲の名前を入力するフィールド。この名前は、［**スキャン範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品がこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、コンポーネントの動作中にこの保護範囲が処理されます。 このチェックボックスをオフにすると、コンポーネントの動作中にこの保護範囲は処理されません。このチェックボックスをオンにすることにより、後からこの範囲をコンポーネントの動作設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	これらの設定では、スキャン範囲を設定できます。 ファイルシステムのドロップダウンリストで、ファイルシステムの種別を選択できます： • **Local**：ローカルディレクトリ。 • **Shared**：Samba または NFS プロトコルでアクセス可能なサーバーファイルシステムリソースを表示します。 • **共有済みのすべての場所**（既定値）：Samba および NFS プロトコルでアクセス可能なすべてのサーバーファイルシステムリソースを表示します。
	ファイルシステムのドロップダウンリストで **Shared** を選択した場合は、右側のドロップダウンリストでリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。
	ファイルシステムのドロップダウンリストで **Local** を選択した場合は、保護範囲に追加するディレクトリのパスを入力フィールドに入力できます。パスの指定にマスクを使用できます。

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」

アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。

マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。

マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。

ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。

このフィールドを空白のままにすることはできません。

マスク

このリストには、アンチクリプターコンポーネントの動作中にスキャンするオブジェクト名のマスクが含まれます。

既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［保護の設定］ウィンドウ

保護設定

設定	説明
暗号化の検知	悪意のある暗号化を検知した際に、Kaspersky Endpoint Security が実行する処理です。

時の処理	• ユーザーに**通知**します。Kaspersky Endpoint Security は暗号化を実行するデバイスをブロックしません。悪意のある暗号化の検知に関するイベントをイベントログに記録するだけです。 • 暗号化を実行するデバイスを**ブロック**します（既定値）。
ブロックする時間（分）	このフィールドでは、信頼しないデバイスのブロック期間を分単位で指定します。指定された時間が経過すると、ブロックするデバイスのリストから信頼しないデバイスを削除します。ネットワークファイルリソースへのホストのアクセスは、信頼しないホストのリストから削除された後で自動的に復元されます。 侵入されたホストがブロックされ、この設定値を変更すると、このホストのブロック時間は変更されません。ブロックの時間は動的な値ではなく、ブロックの瞬間に計算されます。 使用できる値：1～4294967295 の整数。 既定値：30

［除外範囲］ウィンドウ

この表には、スキャンの除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	スキャンから除外されるディレクトリのパス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［<新しい除外範囲>］ウィンドウ

このウィンドウでは、スキャンの除外範囲の追加や設定ができます。

除外範囲の設定

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表

	示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品の実行時にこの範囲をスキャンから除外するかどうかを選択します。 チェックボックスをオンにすると、スキャン中にこの範囲が除外されます。 このチェックボックスをオフにすると、この範囲がスキャン範囲に含まれます。このチェックボックスをオンにすることにより、後からこの範囲を除外することができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	これらの設定では、除外範囲を設定できます。 ファイルシステムのドロップダウンリストで、スキャンから除外するディレクトリのファイルシステムの種別を選択できます： • **Local**：ローカルディレクトリ。 • **Mounted**：マウントされたディレクトリ。 • **リモートでマウント済みのすべての場所** - Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。
	ファイルシステムのドロップダウンリストで **Mounted** を選択した場合は、右側のドロップダウンリストでリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。
	ファイルシステムのドロップダウンリストで **Local** を選択した場合は、除外範囲に追加するディレクトリのパスを入力フィールドに入力できます。パスの指定にマスクおよびタグを使用できます。

特別なタグを使用してコンテナまたはイメージを指定できます：

- [container-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>]/<ローカルディレクトリへのパス>
- [image-id:<識別子>]/<ローカルディレクトリへのパス>
- [image-name:<名前>]/<ローカルディレクトリへのパス>

[container-id:<識別子>]、[container-name:<名前>]、[image-id:<識別子>]、および [image-name:<名前>]/<ローカルディレクトリ> タグの一意の組み合わせを使用することもできます。

1つのエリア内で1～4個の一意のタグを任意に組み合わせて使用できます。リストされている順序は重要ではありません。

例：

- [container-name:<名前>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-ID:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [image-name:<名前>][image-id:<識別子>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>
- [container-name:<名前>][image-id:<識別子>][container-id:<識別子>][image-name:<名前>]/<ローカルディレクトリへのパス>

名前と識別子にはマスク（? および * 記号）を使用できます。

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」

アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。

マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。

マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。

ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。

「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。

ファイルシステム名

除外範囲に追加するディレクトリがあるファイルシステムの名前を入力するためのフィールドです。

このフィールドは、ファイルシステムのドロップダウンリストで［**Mounted**］が選択され、右側のドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。

マスク

このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。マスクは、［パス］フィールドに指定されたディレクトリ内のオブジェクトにのみ適用されます。

既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、スキャンからのオブジェクトの除外を設定できます。指定したマスクが名前に含まれるファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、スキャンから除外されるファイル名のマスクのうち、選択したマスクが削除されます。

このボタンは、少なくとも1つのファイルマスクをリストから選択している場合に使用できます。

マスクをクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを編集できます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

コマンドラインでのアンチクリプターの設定

コマンドラインで、アンチクリプタータスク（*Anti_Cryptor*）を使用してアンチクリプターを管理できます。

既定では、アンチクリプターのタスクは実行されません。このタスクは、手動で開始および停止できます。

アンチクリプターの事前定義済みタスクの設定を編集することで、アンチクリプターの設定を構成できます。

設定	説明	値
ActionOnDetect	［信頼されていないホストのブロック］をオンにする。	`Block`（既定値）– 信頼されていないホストのブロックを有効にします。 `Notify`：信頼されていないホストのブロックを無効にします。
`BlockTime`	信頼できないデバイスがブロックされる時間（分単位）。 侵入されたホストがブロックされてから `BlockTime` の設定値を変更しても、このホストのブロック時間は変更されません。ブロックの時間は動的な値ではなく、ブロックの瞬間に計算されます。	1 - 4294967295 の整数。 既定値：30
`UseExcludeMasks`	`ExcludeMasks.item_#` 設定で指定されたオブジェクトの保護範囲からの除外を有効にします。 この設定は、`ExcludeMasks.item_#` 設定に値が指定されている場合にのみ適用されます。	`Yes` - `ExcludeMasks.item_#` 設定で指定されたオブジェクトを保護範囲から除外します。 `No`（既定値） - `ExcludeMasks.item_#` 設定で指定されたオブジェクトを保護範囲から除外しません。
`ExcludeMasks.item_#`	名前またはマスクによる指定で、オブジェクトを保護範囲から除外します。この設定を使用すると、指定したスキャン範囲から名前によって個別のファイルを除外したり、シェル形式でマスクを使用して複数のファイルを除外したりできます。 この設定の値を指定する前に、`UseExcludeMasks` 設定が有効になっていることを確認します。 複数のマスクを指定する場合は、新しいインデックスを使用して新しい行に各マスクを指定する必要があります。	既定値は定義されていません。
[ScanScope.item_#] セクションには、本製品が保護する範囲が含まれます。アンチクリプタータスクには、少なくとも 1 つの保護対象範囲を指定する必要があります。共有ディレクトリのみが指定可能です。 複数の [ScanScope.item_#] セクションを、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。 [ScanScope.item_#] セクションには、次の設定が含まれています：		
`AreaDesc`	保護範囲の説明。保護範囲に関する詳細情報を含みます。	既定値：`All shared directories`。
`UseScanArea`	指定した範囲の保護を有効にします。タスクを実行するには、少なくとも 1 つの範囲の保護を有効にします。	`Yes`（既定値） - 指定された範囲を保護します。 `No` - 指定された範囲を保護しません。
`AreaMask.item_#`	保護範囲の制限事項。保護範囲内で、シェル形式のマスクを使用して指定したオブジェクトのみを保護します。	既定値：`*`（すべてのオブジェクトを保護）

	複数の AreaMask.item_# 項目を、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。	
Path	保護するオブジェクトがあるディレクトリのパス。	< ローカルディレクトリのパス > - SMB/NFS 経由でアクセス可能なローカルディレクトリを保護します。パスの指定にマスクを使用できます。 アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 AllShared（既定値） - SMB / NFS を使用してアクセスされるすべてのリソースを保護します。 Shared:SMB - SMB を使用してアクセスされるリソースを保護します。 Shared:NFS - NFS を使用してアクセスされるリソースを保護します。

[ExcludedFromScanScope.item_#] セクションには、すべての [ScanScope.item_#] セクションから除外されるオブジェクトが含まれます。[ExcludedFromScanScope.item_#] セクションのルールに一致するオ

ブジェクトはスキャンされません。[ExcludedFromScanScope.item_#] セクションの形式は、[ScanScope.item_#] セクションの形式と似ています。複数の [ExcludedFromScanScope.item_#] セクションを、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。

[ExcludedFromScanScope.item_#] セクションには、次の設定が含まれています：

`AreaDesc`	保護の除外範囲の説明。除外範囲に関する詳細情報を含みます。	既定値：`All objects`
`UseScanArea`	指定した範囲を保護から除外します。	`Yes`（既定値） - 指定された範囲を保護から除外します。 `No` - 指定された範囲を保護から除外しません。
`AreaMask.item_#`	保護の除外範囲の制限事項。除外範囲で、シェル形式のマスクを使用して指定したオブジェクトのみを除外します。 複数の `AreaMask.item_#` 項目を、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。	既定値：`*`（すべてのオブジェクトを除外）。
`Path`	保護から除外されるオブジェクトがあるディレクトリのパス。	`<` ローカルディレクトリのパス `>` - 指定されたディレクトリのオブジェクトを保護から除外します。パスの指定にマスクを使用できます。

		アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を2文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 Mounted:NFS - NFSプロトコルを使用してクライアントデバイスにマウントされるすべてのリモートディレクトリを保護から除外します。 Mounted:SMB - Sambaプロトコルを使用してクライアントデバイスにマウントされるリモートディレクトリを保護から除外します。 AllRemoteMounted - Sambaプロトコルと NFSプロトコルを使用してクライアントデバイスにマウントされるすべてのリモートディレクトリを保護から除外します。

ブロックされるデバイスの管理

Kaspersky Endpoint Security は、ネットワークの脅威やリモートの悪意のある暗号化からデバイスを保護しながら、悪意のある動作を行うリモートデバイスをブロックできます：

- 悪意のある暗号化が検出された場合、アプリケーションは、保護対象デバイスの共有ネットワークディレクトリへのリモートデバイスのアクセスをブロックします。
- 保護対象デバイスに対するネットワーク攻撃の試みを検知すると、アプリケーションは攻撃デバイスからのネットワークトラフィックをブロックします。

ブロック期間は、ネットワーク脅威対策とリモートの悪意のある暗号化に対する保護の設定で変更できます。指定された時間が経過すると、アプリケーションはデバイスのブロックを解除します。

コマンドラインを使用してアプリケーションを管理している場合は、ブロックされるデバイスを管理するコマンドを使用して、デバイス上で実行されているアプリケーションの結果としてブロックされたデバイスのリストを表示し、ブロック時間が経過する前にこれらのデバイスのブロックを手動で解除できます。Kaspersky Security Center には、*ネットワーク攻撃の検知*と*暗号化の検知*イベントを除き、ブロックされたデバイスを監視および管理するためのツールはありません。

「-H」は、アンチクリプターおよびネットワーク脅威対策によってブロックされたデバイスを管理するためのコマンドのグループに属することを示す接頭辞です。

The kesl-control --get-blocked-hosts コマンド

このコマンドを使用すると、ブロックされるデバイスのリストをコンソールに出力できます。

コマンド構文

```
kesl-control [-H] --get-blocked-hosts
```

kesl-control --allow-hosts コマンド

このコマンドを使用すると、ブロックされるデバイスのブロックを解除できます。

コマンド構文

```
kesl-control [-H] --allow-hosts <アドレス>
```

引数とキー

< address > は、デバイスまたはサブネットの IP アドレス（IPv4 / IPv6、短縮形式のアドレスを含む）です。デバイスまたはサブネットの IP アドレスをスペースで区切って複数指定できます。

ブロックされたデバイスのリストを表示するには、次のコマンドを実行します：

```
kesl-control --get-blocked-hosts
```

コマンド実行の結果、アプリケーションはブロックされるデバイスのリストをコンソールに出力します。

デバイスをブロック解除するには、次のコマンドを実行します：

```
kesl-control --allow-hosts <アドレス>
```

<address> は、デバイスまたはサブネットの1つ以上のIPアドレス（IPv4 / IPv6、短縮形式のアドレスを含む）です。デバイスまたはサブネットのIPアドレスをスペースで区切って複数指定できます。

コマンド実行の結果、アプリケーションは指定されたデバイスのブロックを解除します。

例：
IPv4アドレス：
```
dec - 192.168.0.1
dec - 192.168.0.0/24
```
IPv6アドレス：
```
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210%1
hex - 2001:db8::ae21:ad12
hex - ::ffff:255.255.255.254
hex - ::
```

アプリケーションコントロール

アプリケーションコントロールコンポーネントにより、保護対象デバイス上のアプリケーションの起動を管理できます。アプリケーションコントロールは、アプリケーションへのユーザーアクセスを制限することで、デバイス感染のリスクを軽減します。

このコンポーネントを使用するには、対応する機能を含むライセンスが必要です。

この機能は、KESL コンテナではサポートされていません。

アプリケーションの起動は、*アプリ管理ルール*によって制限されます。

アプリケーションコントロールコンポーネントは、2 つのモードのいずかれかで動作できます：

- *拒否リスト*：このモードでは、Kaspersky Endpoint Security は、すべてのユーザーがアプリ管理ルールで指定されていないアプリケーションを起動できるようにします。アプリケーションコントロールコンポーネントは、既定ではこのモードで動作します。
- *許可リスト*：このモードでは、Kaspersky Endpoint Security は、すべてのユーザーがアプリ管理ルールで指定されていないアプリケーションは起動できないようにします。

アプリ管理ルールが最大限作成された場合、組織のローカルネットワークの管理者によって検証されていない、すべての新しいアプリケーションの起動が禁止されます。ただし、ユーザーが職務を遂行するために必要なオペレーティングシステムと検証済みアプリケーションのパフォーマンスは保証されます。

Kaspersky Security Center の管理者、またはアプリケーションの管理者ロールを割り当てられたローカルユーザーは、アプリ管理の使用により、root アカウントの下でプロセスの開始を許可、または拒否することができます。

既定で、アプリケーションコントロールは無効です。アプリケーションコントロールを有効または無効にしたり、コンポーネントの動作を設定できます：

- アプリケーションコントロールモード（*allowlist* または *denylist*）を選択します。
- モードごとにアプリケーションコントロールルールを作成します。
- ルールに一致するアプリケーションの起動試行を検知したときに Kaspersky Endpoint Security が実行する処理を選択します。*ルールを適用*するか、ルールに一致するアプリケーションの起動試行について*ルールをテストして通知*します。

インベントリタスクを使用して、保護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に関する情報を受け取ることができます。

アプリケーションコントロールタスクは、Kaspersky Endpoint Security でサポートされていないインタープリターからのスクリプトの起動や、コマンドラインを介してインタープリターに渡されないスクリプトの起動を制御しません。Kaspersky Endpoint Security は、python、perl、bash、ssh のインタープリターをサポートしています。

アプリケーションコントロールルールでインタープリターの起動を許可している場合、このインタープリターから起動されたスクリプトはブロックされません。インタープリターコマンドラインで指定した、少なくとも1つのスクリプトの起動をアプリケーションコントロールルールで禁止している場合、インタープリターコマンドラインで指定したすべてのスクリプトがブロックされます。除外：cat script.py | Python

アプリケーションコントロールルールの概要

*アプリケーションコントロールルール*とは、ルールをトリガーするための条件と、ルールがトリガーされたときのアプリケーションコントロールコンポーネントの処理（アプリケーションの起動時にユーザーを許可またはブロックする）を含む設定のセットです：

- アプリケーションカテゴリに属するアプリケーション。*アプリケーションカテゴリ*は、共通の特性を持つアプリケーションのグループです。たとえば、インストールされたアプリケーションの実行ファイルを含むカテゴリ、または組織で使用されるアプリケーションの標準セットを含む操作に必要なアプリケーションカテゴリなどです。各カテゴリは、1つのルールでのみ使用できます。

  Kaspersky Endpoint Security は、Kaspersky Security Center の KL カテゴリの使用をサポートしていません。

- アプリケーションを実行するための選択したユーザーまたはユーザーグループに対する許可または禁止。指定したカテゴリのアプリケーションの実行を許可または許可しないユーザーまたはユーザーグループを指定できます。

- ルールの適用条件：条件は、「条件種別 - 条件基準 - 条件値」の対応で表されます。ルールの適用条件に基づいて、ルールをアプリケーションに適用するかどうかが決定されます。ルールには対象条件と除外条件が使用されます：

  - *対象条件*：アプリケーションが少なくとも1つの対象条件を満たす場合、ルールがアプリケーションに適用されます。

  - *除外条件*：アプリケーションが少なくとも1つの除外条件を満たす場合、または対象条件のいずれも満たさない場合、ルールはアプリケーションに適用されません。

  ルールの適用条件は、以下の基準を使用して作成されます：

  - アプリケーションの実行ファイルの名前。

  - アプリケーションの実行ファイルがあるディレクトリの名前。

  - アプリケーションの実行ファイルのハッシュ。SHA256 のみが許可されます。

  条件で使用される基準ごとに、値を指定する必要があります。

  マスクを使用して、ファイル名とディレクトリ名を指定できます

* 文字（任意の 2 文字以上）または ? 文字（任意の 1 文字）をファイル名またはディレクトリ名のマスクとして使用できます。

/ 文字を含むファイル名またはディレクトリ名には、任意の文字数の文字列（0 文字の場合も含む）を表す * 文字を入れることができます。例：「`/dir/*/file*/`」または「`/dir/file*/`」。

ファイル名またはディレクトリ名には、? 文字で任意の文字（`/` を含む）を表示できます。

起動するアプリケーションの設定が、対象条件で指定された基準と一致する場合、ルールが適用されます。この場合、Kaspersky Endpoint Security はルールで指定された処理を実行します。アプリケーション設定が除外条件で指定された基準と一致する場合、Kaspersky Endpoint Security はアプリケーションの起動を制御しません。

アプリケーションコントロールルールは、次のいずれかの*動作ステータス*を伴います：

- *Enabled*：ルールが有効であり、Kaspersky Endpoint Security によってアプリケーションコントロールのこのルールが適用されます。
- *無効*：ルールは無効であり、アプリケーションコントロールには使用されません。
- *Test* - ルールの条件を満たすアプリケーションの起動が許可されます。ただし、これらのアプリケーションの起動に関する情報がレポートに記録されます。

ルールの動作ステータスの優先度は、ルールで指定された処理の優先度よりも高くなります。

Web コンソールでのアプリケーションコントロールの設定

Web コンソールでは、ポリシーのプロパティ内でアプリケーションコントロールの設定を行うことができます（**製品設定 → 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**）。

アプリケーションコントロールコンポーネントの設定

設定	説明
アプリケーションコントロールの有効化 / 無効化	この切り替えボタンでは、アプリケーションコントロールを有効にするかどうかを選択します。 既定では、切り替えボタンはオフになっています。
ルールによってブロックされたアプリケーションの起動に関する措置	設定済みルールと一致する、アプリケーションの起動の試行を検知した場合に Kaspersky Endpoint Security が実行する処理： • **ルールをテスト**：このオプションをオンにすると、Kaspersky Endpoint Security によってルールがテストされ、ルールに一致するアプリケーションの起動の試行に関するイベントが生成されます。 • **ルールを適用**（既定値）：このオプションをオンにすると、Kaspersky Endpoint Security はアプリ管理ルールを適用し、ルールで指定された処理を実行します。
アプリケーションコントロールのモード	アプリケーションコントロールタスクの操作モード： • **許可リスト**：このオプションをオンにすると、Kaspersky Endpoint Security は、すべてのユーザーがアプリ管理ルールで指定されているものを除いた、すべてのアプリケーションを起動できないようにします。

	• **拒否リスト**（既定値）：このオプションをオンにすると、Kaspersky Endpoint Security は、すべてのユーザーがアプリ管理ルールで指定されているものを除いた、すべてのアプリケーションを起動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	［**ルールを設定する**］をクリックすると、［**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。
ルールの適用	このドロップダウンリストでは、ルールを追加する方法を選択できます： • **ローカルルールをポリシーのルールで置き換え**。この項目を選択すると、ポリシーで指定されたルールのみを適用します。 • **ポリシーのルールをローカルルールに追加**（既定値）。この項目を選択すると、保護されたデバイスで設定されたローカルルールとともに、ポリシーで指定されたルールを適用します。

［アプリケーションコントロールルール］ウィンドウ

［**アプリケーションコントロールルール**］の表には、各動作モードのルール（［**拒否リスト（アクティブ）**］、［**許可リスト**］）を表示するタブがあります。アプリケーションコントロールルールの表の両方のタブは、既定では空です。

アプリケーションコントロールルールの設定

設定	説明
カテゴリ	ルールによって使用されるアプリケーションカテゴリの名前。
ステータス	アプリ管理ルールの操作ステータス： • *有効*– ルールが有効であり、アプリケーションコントロールは動作中にこのルールを適用します。 • *無効*– ルールは無効であり、アプリケーションコントロールの実行時にルールは使用されません。 • *テスト*– アプリケーションコントロールによりルールの条件を満たすアプリケーションの起動が許可されます。ただし、これらのアプリケーションの起動に関する情報がレポートに記録されます。

アプリケーションコントロールルールは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［アプリケーションコントロールルール］ウィンドウ

このウィンドウでは、アプリケーションコントロールルールを設定します。

アプリケーションコントロールルールを設定

設定	説明
ルールの説明	アプリケーションコントロールルールの説明。
ステータス	アプリケーションコントロールルールの動作ステータスを選択できます： • *有効* – ルールが有効であり、アプリケーションコントロールは動作中にこのルールを適用します。 • *無効* – ルールは無効であり、アプリケーションコントロールの実行時にルールは使用されません。 • *テスト* – アプリケーションコントロールによりルールの条件を満たすアプリケーションの起動が許可されます。ただし、これらのアプリケーションの起動に関する情報がレポートに記録されます。
カテゴリ	［**カテゴリを選択する**］をクリックすると、［**アプリケーションカテゴリ**］ウィンドウが表示されます。
ユーザーおよび権限	この表には、アプリ管理ルールが適用されるユーザーまたはユーザーグループのリストと、それらに割り当てられているアクセスの種別が表示されており、次の列で構成されています： • ［**ユーザーまたはグループ名**］ – アプリ管理ルールが適用されるユーザー名またはユーザーグループ名。 • **アクセス** – アクセスの種別（アプリケーションの起動の許可、ブロック）。この切り替えボタンでは、アクセスの種別を切り替えます（製品の起動を［**許可**］、製品の起動を［**ブロック**］）。 ユーザーまたはユーザーグループを追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

［アプリケーションカテゴリ］ウィンドウ

このウィンドウでは、新しいカテゴリの追加や、アプリケーションコントロールルールのカテゴリの設定ができます。

Kaspersky Endpoint Security は、Kaspersky Security Center の KL カテゴリの使用をサポートしていません。

アプリケーションコントロールのカテゴリ

設定	説明
カテゴリ名。	追加されたアプリケーションカテゴリの検索バー。
追加	ボタンをクリックすると、カテゴリ作成ウィザードが起動します。ウィザードの指示に従います。
編集	このボタンをクリックすると、カテゴリのプロパティウィンドウが表示され、カテゴリの設定を変更できます。
Remove	ボタンをクリックすると、選択したカテゴリが削除されます。［**ゴールデンイメージ（ローカル）**］カテゴリは削除できません。

［ユーザーまたはグループの選択］ウィンドウ

このウィンドウでは、ルールを設定するローカルまたはドメインのユーザーまたはユーザーグループを指定できます。

アプリケーションコントロールルールを設定

設定	説明
マニュアル	このオプションがオンの場合、下のフィールドに、アプリ管理ルールを適用するローカルまたはドメインユーザーの名前、あるいはユーザーグループの名前を入力します。
グループまたはユーザーのリスト	このオプションがオンの場合、検索フィールドに、アプリ管理ルールを適用するユーザー名またはグループ名の検索条件を入力するか、下のリストからユーザーグループ名を選択できます。

管理コンソールでのアプリケーションコントロールの設定

管理コンソールでは、ポリシーのプロパティ内でアプリケーションコントロールの設定を行うことができます（**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**）。

アプリケーションコントロールコンポーネントの設定

設定	説明
アプリケーションコントロールを有効にする	このチェックボックスは、アプリケーションコントロールを有効にします。 既定では、このチェックボックスはオフです。
アプリケーションの起動時の処理	設定済みルールと一致する、アプリケーションの起動の試行を検知した場合に Kaspersky Endpoint Security が実行する処理： • **ルールを適用**（既定値）：このオプションをオンにすると、Kaspersky Endpoint Security はアプリ管理ルールを適用し、ルールで指定された処理を実行します。 • **ルールをテスト**：このオプションをオンにすると、Kaspersky Endpoint Security によってルールがテストされ、ルールに一致するアプリケーションの起動の試行に関するイベントが生成されます。
アプリケーションコントロールのモード	アプリケーションコントロールタスクの操作モード： • **許可リスト**：このオプションをオンにすると、Kaspersky Endpoint Security は、すべてのユーザーがアプリ管理ルールで指定されているものを除いた、すべてのアプ

	リケーションを起動できないようにします。 • **拒否リスト**（既定値）：このオプションをオンにすると、Kaspersky Endpoint Security は、すべてのユーザーがアプリ管理ルールで指定されているものを除いた、すべてのアプリケーションを起動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	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**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。
ルールの適用	このドロップダウンリストでは、ルールを追加する方法を選択できます： • **ローカルルールをポリシーのルールで置き換え**。この項目を選択すると、ポリシーで指定されたルールのみを適用します。 • **ポリシーのルールをローカルルールに追加**（既定値）。この項目を選択すると、保護されたデバイスで設定されたローカルルールとともに、ポリシーで指定されたルールを適用します。

［アプリケーションコントロールルール］ウィンドウ

［**アプリケーションコントロールルール**］の表には、アプリケーションコントロールによって使用されるルールが表示されています。アプリケーションコントロールルールの表は、既定では空です。

アプリケーションコントロールルールの設定

設定	説明
カテゴリ名。	ルールによって使用されるアプリケーションカテゴリの名前。
ステータス	アプリ管理ルールの操作ステータス： • *有効* – ルールが有効であり、アプリケーションコントロールは動作中にこのルールを適用します。 • *無効* – ルールは無効であり、アプリケーションコントロールの実行時にルールは使用されません。 • *テスト* – アプリケーションコントロールによりルールの条件を満たすアプリケーションの起動が許可されます。ただし、これらのアプリケーションの起動に関する情報がレポートに記録されます。 ルールのステータスは、［**ルールの追加 / ルールの編集**］ウィンドウで変更できます。

アプリケーションコントロールルールは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

［ルールの追加］ウィンドウ

このウィンドウでは、アプリケーションコントロールルールを設定します。

アプリケーションコントロールルールの追加

設定	説明
説明	アプリケーションコントロールルールの説明。
ルールのステータス	ドロップダウンリストで、アプリケーションコントロールルールのステータスを選択できます： • *有効* – ルールが有効であり、アプリケーションコントロールは動作中にこのルールを適用します。 • *無効* – ルールは無効であり、アプリケーションコントロールの実行時にルールは使用されません。 • *テスト* – アプリケーションコントロールによりルールの条件を満たすアプリケーションの起動が許可されます。ただし、これらのアプリケーションの起動に関する情報がレポートに記録されます。
カテゴリ	設定のグループには、［**設定**］が含まれています。このボタンをクリックすると、［**アプリケーションカテゴリ**］ウィンドウが表示されます。
ユーザーおよび権限	この表には、アプリ管理ルールが適用されるユーザーまたはユーザーグループのリストと、それらに割り当てられているアクセスの種別が表示されており、次の列で構成されています： • ［**ユーザーまたはグループ名**］– アプリ管理ルールが適用されるユーザー名またはユーザーグループ名。 • ［**アクセス**］– アクセスの種別：アプリケーションの起動を［**許可**］、アプリケーションの起動を［**ブロック**］。 ユーザーまたはユーザーグループを追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

［アプリケーションカテゴリ］ウィンドウ

このウィンドウでは、新しいカテゴリの追加や、アプリケーションコントロールルールのカテゴリの設定ができます。

Kaspersky Endpoint Security は、Kaspersky Security Center の KL カテゴリの使用をサポートしていません。

アプリケーションコントロールのカテゴリ

設定	説明

カテゴリ名。	追加されたアプリケーションコントロールのカテゴリのリスト。
追加	ボタンをクリックすると、カテゴリ作成ウィザードが起動します。ウィザードの指示に従います。
編集	このボタンをクリックすると、カテゴリのプロパティウィンドウが表示され、カテゴリの設定を変更できます。

［ユーザーまたはグループ］ウィンドウ

このウィンドウでは、ルールを設定するローカルまたはドメインのユーザーまたはユーザーグループを指定できます。

アプリケーションコントロールルールの追加

設定	説明
種別	アプリ管理ルールが適用される［**ユーザー**］または［**グループ**］。
ユーザーまたはグループ名	アプリケーションコントロールルールが適用されるユーザーまたはユーザーグループの名前。
アクセス	アクセスの種別：アプリケーションの起動を［**許可**］、アプリケーションの起動を［**ブロック**］。

コマンドラインでのアプリ管理の設定

コマンドラインでは、アプリ管理の定義済みタスク（*Application_Control*）を使用することで、アプリ管理ができます。

既定では、アプリ管理のタスクは実行されません。タスクは、手動で開始および停止できます。

アプリケーションコントロール事前定義済みタスクの設定を編集することで、デバイス上のアプリケーションコントロールを設定できます。

許可リストを変更する場合や、すべてのアプリケーションの起動を禁止する場合、または Kaspersky Endpoint Security の動作に影響を与えるアプリケーションの起動を禁止する場合は、設定情報ファイルを使用するかコマンドラインキーを使用してタスクの設定を変更する時に、`--accept` フラグを指定して `kesl-control --set-settings` コマンドを実行します。

アプリケーションコントロールのコマンドを使用してアプリケーションコントロールを設定することもできます。

- カテゴリのリストを作成および編集します。
- 本製品で作成されたカテゴリのリストを表示します。
- アプリケーションコントロールルールのリストを設定します。

アプリケーションコントロールタスクの設定

この表では、アプリケーションコントロールタスクで指定できるすべての設定と、その設定で使用可能なすべての値と既定値を説明します。

アプリケーションコントロールタスクの設定

設定	説明	値
AppControlMode	アプリケーションコントロールタスクの操作モード。	AllowList - アプリ管理ルールで指定されていないアプリケーションをユーザーが起動できないようにします。 DenyList（既定値） - アプリ管理ルールで指定されていないアプリケーションをユーザーが起動できるようにします。
AppControlRulesAction	設定済みルールと一致する、アプリケーションの起動の試行を検知した場合に Kaspersky Endpoint Security が実行する処理：	ApplyRules（既定値） - アプリケーションコントロールルールが適用され、ルールで指定された処理が実行されます。 TestRules – ルールがテストされ、ルールを満たすアプリケーションの検出に関するイベントが生成されます。
[Categories.item_#] セクションには、次の設定が含まれています：		
Name	ルールが適用される、アプリケーションカテゴリの名前。	
UseIncludes	ルールを適用するための対象条件の使用。	Yes - アプリケーションが少なくとも1つの対象条件を満たしている場合は、ルールをアプリケーションに適用します。 No（既定値） - アプリケーションが対象条件を満たす場合でも、ルールをアプリケーションに適用しません。
IncludeFileNames.item_#	ルールを適用する実行ファイルの名前。	ファイル名の指定にマスクを使用できます。 * 文字（任意の 2 文字以上）または ? 文字（任意の 1 文字）をファイル名またはディレクトリ名のマスクとして使用できます。 / 文字を含むファイル名またはディレクトリ名には、任意の文字数の文字列（0 文字の場合も含む）を表す * 文字を入れることができます。例：「/dir/*/file*/」または「/dir/file*/」。 ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。
IncludeFolders.item_#	ルールを適用するアプリケーションの実行ファイルがあるディレクトリの名前。	ディレクトリ名の指定にマスクを使用できます。

		* 文字（任意の 2 文字以上）または ? 文字（任意の 1 文字）をファイル名またはディレクトリ名のマスクとして使用できます。 / 文字を含むファイル名またはディレクトリ名には、任意の文字数の文字列（0 文字の場合も含む）を表す * 文字を入れることができます。例：「`/dir/*/file*/`」または「`/dir/file*/`」。 ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。
`IncludeHashes.item_#`	ルールを適用する実行ファイルの SHA256 ハッシュ。	SHA256 のみが許可されます。
`UseExcludes`	ルールを適用するための除外条件の使用。	`Yes` - アプリケーションが少なくとも 1 つの除外条件を満たしている場合、または対象条件のいずれも満たしていない場合は、ルールをアプリケーションに適用しません。 `No`（既定値） - アプリケーションが少なくとも 1 つの除外条件を満たす場合でも、ルールをアプリケーションに適用します。
`ExcludeFileNames.item_#`	ルールを適用する実行ファイルの名前。	ファイル名の指定にマスクを使用できます。 * 文字（任意の 2 文字以上）または ? 文字（任意の 1 文字）をファイル名またはディレクトリ名のマスクとして使用できます。 / 文字を含むファイル名またはディレクトリ名には、任意の文字数の文字列（0 文字の場合も含む）を表す * 文字を入れることができます。例：「`/dir/*/file*/`」または「`/dir/file*/`」。 ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。
`ExcludeFolders.item_#`	ルールを適用するアプリケーションの実行ファイルがあるディレクトリの名前。	ディレクトリ名の指定にマスクを使用できます。

		* 文字（任意の 2 文字以上）または ? 文字（任意の 1 文字）をファイル名またはディレクトリ名のマスクとして使用できます。 / 文字を含むファイル名またはディレクトリ名には、任意の文字数の文字列（0 文字の場合も含む）を表す * 文字を入れることができます。例：「`/dir/*/file*/`」または「`/dir/file*/`」。 ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。
`ExcludeHashes.item_#`	ルールを適用する実行ファイルの SHA256 ハッシュ。	SHA256 のみが許可されます。
[AllowListRules.item _#] セクションには、*AllowList*操作モードのアプリ管理ルールのリストが含まれています。 [AllowListRules.item_#] の各セクションには、次の設定が含まれています：		
説明	アプリケーションコントロールルールの説明。	
`AppControlRuleStatus`	アプリ管理ルールの操作ステータス：	`On`（規定値）：ルールが有効であり、Kaspersky Endpoint Security によってアプリケーションコントロールのこのルールが適用されます。 `Off`：アプリケーションコントロールで使用されているルールではありません。 `Test` - ルールの対象となるアプリケーションの起動が許可されます。ただし、これらのアプリケーションの起動に関する情報がレポートに記録されます。
`Category`	ルールが適用される、作成されたアプリケーションカテゴリの名前。 「ゴールデンイメージ」カテゴリを指定できます。	
[AllowListRules.item_#.ACL.item_#] セクションには、アプリケーションの実行を許可または拒否されたユーザーのリストが含まれます。		
`Access`	ユーザーまたはユーザーグループに割り当てられるアクセスの種別。	`Allow`（既定値） - アプリケーションの実行を許可します。 `Block`–実行中のアプリケーションを拒否します。
`Principal`	アプリケーションコントロールルールが適用されるユーザーまたはユーザーグループ。	`\Everyone`（既定値）：すべてのユーザーにルールが適用されます。 < ユーザ名 >：ルールを適用するユーザーの名前。

		@<グループ名>：ルールを適用するユーザーのグループの名前。
[DenyListRules.item_#] セクションには、*DenyList*操作モードのアプリ管理ルールのリストが含まれています。 [DenyListRules.item_#] の各セクションには、次の設定が含まれています：		
説明	アプリケーションコントロールルールの説明。	
AppControlRuleStatus	アプリ管理ルールの操作ステータス：	On（規定値）：ルールが有効であり、Kaspersky Endpoint Security によってアプリケーションコントロールのこのルールが適用されます。 Off：アプリケーションコントロールで使用されているルールではありません。 Test - ルールの対象となるアプリケーションの起動が許可されます。ただし、これらのアプリケーションの起動に関する情報がレポートに記録されます。
Category	ルールが適用される、作成されたアプリケーションカテゴリの名前。 アプリケーションの「ゴールデンイメージ」リストをカテゴリとして指定できます。	
[DenyListRules.item_#.ACL.item_#] セクションには、アプリケーションの実行を許可または拒否されたユーザーのリストが含まれます。		
Access	ユーザーまたはユーザーグループに割り当てられるアクセスの種別。	Allow - アプリケーションの起動を許可します。 Block（既定値）- アプリケーションの起動を許可しません。
Principal	アプリケーションコントロールルールが適用されるユーザーまたはユーザーグループ。	\Everyone（既定値）：すべてのユーザーにルールが適用されます。 <ユーザ名>：ルールを適用するユーザーの名前。 @<グループ名>：ルールを適用するユーザーのグループの名前。

カテゴリのリストの作成と編集

新しいカテゴリは次の 2 つの方法で作成できます。

- 「kesl --set-settings」コマンドと製品制御タスクの設定情報ファイル (Application_Control) を使用します。
- 「kesl --set-categories」コマンドとカテゴリ設定情報ファイルを使用します。

製品カテゴリを作成するには、次のコマンドを実行します：

```
kesl-control --set-categories --file <設定情報ファイルへのパス>
```

説明：

--file <設定情報ファイルへのパス> – カテゴリ設定が含まれる設定情報ファイルへのパスです。

カテゴリ設定を含むファイルの構造は次のようになります：

```
[
  {
    "Exclude": ["(FilePath like <実行ファイルへの絶対パス>)", "(FileHash == <実行ファイルハッシュ>)"],
    "GUID" : "<一意のカテゴリ ID>",
    "Include" : [ "(FilePath like <実行ファイルへの絶対パス>)", "(FileHash == <実行ファイルハッシュ>)" ],
    "Name" : "<カテゴリ 1 の名前>"
  },
  {
    "Exclude": ["(FilePath like <実行ファイルへの絶対パス>)", "(FileHash == <実行ファイルハッシュ>)"],
    "GUID" : "<一意のカテゴリ ID>",
    "Include" : [ "(FilePath like <実行ファイルへの絶対パス>)", "(FileHash == <実行ファイルハッシュ>)" ],
    "Name" : "<カテゴリ 2 の名前>"
  }
]
```

［除外］フィールドと［含める］フィールドにファイル名を指定するには、マスクを使用できます。

*文字（任意の2文字以上）または?文字（任意の1文字）をファイル名またはディレクトリ名のマスクとして使用できます。

/文字を含むファイル名またはディレクトリ名には、任意の文字数の文字列（0文字の場合も含む）を表す*文字を入れることができます。例：「**/dir/*/file*/**」または「**/dir/file*/**」。

ファイル名またはディレクトリ名には、?文字で任意の文字（**/** を含む）を表示できます。

名前設定は必須です。カテゴリ名を指定しないと、カテゴリは作成されないか、削除されます。**GUID** 設定も必須です。指定しない場合はエラーメッセージが表示され、カテゴリは作成されません。**GUID** 設定はハイフンなしで指定する必要があります。

作成された製品カテゴリのリストを編集するには、次のコマンドを実行します：

```
kesl-control --set-categories [--names <カテゴリ 1 の名前> <カテゴリ 2 の名前> ... <カテゴリ N の名前>] --file <設定情報ファイルへのパス>
```

説明：

- **<カテゴリ 1 の名前> <カテゴリ 2 の名前> ... <カテゴリ N の名前>** – 情報を変更するカテゴリの名前複数のカテゴリに関する情報を変更する場合は、カテゴリ名をスペースで区切って指定します。カテゴリ名を指定しない場合は、既存のカテゴリが削除され、指定されたファイルから新しいカテゴリが作成されます。

- `--file <`設定情報ファイルへのパス`>` – カテゴリ設定が含まれる設定情報ファイルへのパスです。

作成したカテゴリのリストの表示

コマンドラインで、アプリケーションコントロール管理コマンドを使用して、作成されたアプリケーション カテゴリのリストを表示できます。

作成されたカテゴリのリストには次のカテゴリが含まれます：

- Kaspersky Security Center で作成されたカテゴリ。
- コマンドラインを使用して、アプリケーションコントロールタスクの設定で追加されたカテゴリ。
- インベントリタスク（Kaspersky Security Center か、コマンドラインを使用）を使用して作成された「ゴールデンイメージ」カテゴリ。

作成されたすべてのアプリケーションカテゴリのリストを表示するには、次のコマンドを実行します：

```
kesl-control --get-categories [--file <設定情報ファイルのパス> [--json]
```

説明：

- `--file <path to configuration file>` – 設定が出力される JSON 構成ファイルへの絶対パス。
- `--json` を指定すると、設定はJSON形式で出力されます。--json ライセンスを省略すると、設定は INI 形式で出力されます。

各アプリケーションカテゴリに関する次の情報が表示されます：

- カテゴリの一意な識別子（GUID）。
- カテゴリ名。
- ルールを適用するための対象条件のリスト。
- ルールを適用するための除外条件のリスト

作成されたアプリケーションカテゴリのリストを表示するには、次のコマンドを実行します：

```
kesl-control --get-categories [--names <カテゴリ 1 の名前> <カテゴリ 2 の名前> ... <カテゴリ N の名前>] --file <設定情報ファイルへのパス> [--json]
```

説明：

- `<`カテゴリ `1` の名前`>` `<`カテゴリ `2` の名前`>` `...` `<`カテゴリ `N` の名前`>` – 情報を変更するカテゴリの名前 複数のカテゴリに関する情報を表示する場合は、カテゴリ名をスペースで区切って指定します。
- `--file <path to configuration file>` – カテゴリリストがエクスポートされる JSON 設定情報ファイルへの絶対パス。

- `--json` を指定すると、設定はJSON形式で出力されます。`--json` ライセンスを省略すると、設定は INI 形式で出力されます。

アプリケーションコントロールタスクの設定で、`[Categories.item_#]` セクションに、ルールのトリガー条件を含めるかまたは除外するために、アプリケーションファイルや実行ファイルのあるディレクトリへのシンボリックリンクを指定すると、この条件のカテゴリーリストを表示するときに、シンボリックリンクが参照するソースパスが表示されます。

アプリケーションコントロールのルールリストの設定

製品のアプリケーションコントロールのリストを表示するには、次のコマンドを実行します：

```
kesl-control --get-settings 21 --file <設定情報ファイルのパス> [--jason]
```

説明：

`--file <設定情報ファイルのパス>` – 設定がエクスポートされる構成ファイルへの絶対パス。

`--json`：データを JSON 形式で出力します。

Kaspersky Endpoint Securityは、アプリケーションコントロールルールに関する次の情報を表示します：

- アプリケーションコントロールタスクの操作モード。
- 設定済みルールと一致する、本製品の起動の試行を検知した場合に アプリケーションコントロールが実行する処理：
- アプリケーションコントロールルールの説明（ある場合）。
- アプリ管理ルールの操作ステータス。
- ルールが適用されるアプリケーションカテゴリの名前。
- ユーザーまたはユーザーグループに割り当てられるアクセスの種別。
- アプリケーションコントロールルールが適用されるユーザーまたはユーザーグループ。

製品カテゴリとアプリケーションコントロールルールのリストを編集するには、次のコマンドを実行します：

```
kesl-control --set-settings 21 [--file <設定情報ファイルのパス>] [--json]
```

説明：

`--file <設定情報ファイルのパス>` – 設定がインポートされる設定情報ファイルへの絶対パス。

`--json` – JSON ファイルからデータをインポートします。

製品カテゴリとアプリケーションコントロールルールのリストを削除するには、次のコマンドを実行します：

```
kesl-control --set-settings 21 --set-to-default
```

インベントリ

インベントリスキャンタスクは、クライアントデバイスに保存されているすべてのアプリケーションの実行ファイルに関する情報を提供します。デバイスに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すると、アプリ管理ルールを作成する場合などに役立ちます。

この機能は、KESL コンテナではサポートされていません。

このタスクを使用するには、対応する機能を含むライセンスが必要です。

インベントリ設定を行うことができます：

- インベントリ中にアプリケーションがデバイス上で検知するオブジェクトのタイプ（ファイル、スクリプト）を選択します。
- インベントリタスクによってデバイス上で検知されたアプリケーションをゴールデンイメージカテゴリに追加することを有効または無効にします。
- インベントリ範囲（実行可能なアプリケーションファイルを検索するディレクトリへのパス）を設定します。
- インベントリからの除外を設定します。

Web コンソールでのインベントリ

Web コンソールでは、インベントリタスクを使用して、保護されたデバイスのアプリケーションのインベントリを実行できます。

インベントリのユーザータスクを作成し、実行できます。これらのタスクの設定を編集することで、インベントリ設定を構成できます。

Kaspersky Security Center のデータベースには、最大 150 000 個の処理されたファイルに関する情報を保存できます。このレコード数に達すると、新しいファイルは処理されません。インベントリタスクを再開するには、Kaspersky Endpoint Security がインストールされているデバイスから、以前のインベントリの結果として Kaspersky Security Center のデータベースに登録されているファイルを削除する必要があります。

インベントリタスクの設定

設定	説明
ゴールデンイメージカテゴリにファイルを追加	このチェックボックスは、インベントリタスクによってデバイス上で検知されたアプリケーションをゴールデンイメージカテゴリに追加することを有効または無効にします。このチェックボックスが選択されている場合、アプリ管理ルールの「ゴールデンイメージ」カテゴリを使用できます。 既定では、このチェックボックスはオフです。
実行ファイルをすべてスキャン	このチェックボックスでは、実行ファイルをスキャンするかどうかを選択します。 既定では、このチェックボックスはオンです。

バイナリをスキャン	このチェックボックスでは、バイナリファイル（拡張子 elf、java、pyc）をスキャンするかどうかを選択します。 既定では、このチェックボックスはオンです。
スクリプトをスキャン	このチェックボックスでは、スクリプトをスキャンするかどうかを選択します。 既定では、このチェックボックスはオンです。
インベントリ範囲	アプリケーションによってスキャンされたインベントリ範囲を示す表。表で指定されたパス内のファイルとディレクトリをすべてスキャンします。表には、既定で1つのインベントリ範囲（/usr/bin）が含まれています。 表内ではインベントリ範囲に対して次の操作ができます：追加、設定、削除、上に移動、下に移動。 ［**下へ**］をクリックすると、表内で選択した項目が下に移動します。 指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。 このボタンは、1つの範囲を表から選択している場合に使用できます。 ［**上へ**］をクリックすると、表内で選択した項目が上に移動します。 指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。 このボタンは、1つの範囲を表から選択している場合に使用できます。 ［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。 このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。 スキャン範囲名をクリックすると、［**<スキャン範囲>**］ウィンドウが表示されます。このウィンドウでは、選択したスキャン範囲の設定を編集できます。 ［**追加**］をクリックすると、［**<新しいスキャン範囲>**］ウィンドウが表示されます。このウィンドウでは、新しいスキャン範囲を指定できます。

［スキャン範囲の追加］ウィンドウ

このウィンドウでは、インベントリタスクのスキャン範囲の追加や設定ができます。

インベントリ範囲の設定

設定	説明
範囲名	インベントリ範囲の名前を入力するフィールド。この名前は、**スキャン設定**セクションの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、タスクの実行時にこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、タスクの実行中にこのインベントリ範囲が処理されます。 このチェックボックスをオフにすると、タスクの実行中にこのインベントリ範囲は処理されません。このチェックボックスをオンにすることにより、後からこの範囲をタスク設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	インベントリ範囲に含めるローカルディレクトリのパスを入力するフィールド。パスの指定にマスクを使用できます。 アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 このフィールドを空白のままにすることはできません。「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリをスキャンします。
マスク	このリストには、タスクの実行中にスキャンするオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。

	［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲］セクション

インベントリタスクの**除外範囲**セクションで、スキャンから除外する範囲を設定できます。

［除外範囲］ウィンドウ

この表には、スキャンの除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	スキャンから除外されるディレクトリのパス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲の追加］ウィンドウ

このウィンドウでは、インベントリタスクのスキャン除外範囲の追加や設定ができます。

除外範囲の設定

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、タスクの実行時にこの範囲を除外するかどうかを選択します。 チェックボックスをオンにすると、タスクの実行中にこの範囲が除外されます。

	チェックボックスをオフにすると、タスクの実行中にこの範囲が含まれます。このチェックボックスをオンにすることにより、後からこの範囲をスキャンから除外することができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	インベントリから除外するローカルディレクトリのパスを入力するフィールド。パスの指定にマスクを使用できます。 アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を2文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 このフィールドを空白のままにすることはできません。
マスク	このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

管理コンソールでのインベントリ

Kaspersky Security Center 管理コンソールでは、*インベントリタスク*を使用して、保護されたデバイスのアプリケーションのインベントリを実行できます。

インベントリのユーザータスクを作成し、実行できます。タスクの設定を編集してスキャン設定を管理できます。

Kaspersky Security Center のデータベースには、最大 150 000 個の処理されたファイルに関する情報を保存できます。このレコード数に達すると、新しいファイルは処理されません。インベントリタスクを再開するには、Kaspersky Endpoint Security がインストールされているデバイスから、以前のインベントリの結果として Kaspersky Security Center のデータベースに登録されているファイルを削除する必要があります。

インベントリタスクの設定

設定	説明
ゴールデンイメージカテゴリにファイルを追加	このチェックボックスは、インベントリタスクによってデバイス上で検知されたアプリケーションをゴールデンイメージカテゴリに追加することを有効または無効にします。このチェックボックスが選択されている場合、アプリ管理ルールの「ゴールデンイメージ」カテゴリを使用できます。 既定では、このチェックボックスはオフです。
実行ファイルをすべてスキャン	このチェックボックスでは、実行ファイルをスキャンするかどうかを選択します。 既定では、このチェックボックスはオンです。
バイナリをスキャン	このチェックボックスでは、バイナリファイル（拡張子 elf、java、pyc）をスキャンするかどうかを選択します。 既定では、このチェックボックスはオンです。
スクリプトをスキャン	このチェックボックスでは、スクリプトをスキャンするかどうかを選択します。 既定では、このチェックボックスはオンです。
インベントリ範囲	設定のグループには、［**設定**］が含まれています。このボタンをクリックすると、［**スキャン範囲**］ウィンドウが表示されます。

インベントリタスクの**除外範囲**セクションで、スキャンから除外する範囲を設定することもできます。

［スキャン範囲］ウィンドウ

この表にはスキャン範囲が含まれます。表で指定されたパス内のファイルとディレクトリをすべてスキャンします。表には、既定で 1 つのスキャン範囲（/usr/bin）が含まれています。

インベントリタスクのスキャン範囲の設定

設定	説明
範囲名	スキャン範囲名。
パス	スキャンするディレクトリのパス。
ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1 つの範囲を表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、範囲の表の並び順でスキャンされます。必要に応じて、サブディレクトリを親ディレクトリよりもリストの上に配置し、親ディレクトリとは異なるセキュリティ設定をサブディレクトリに設定します。

［<新しいスキャン範囲>］ウィンドウ

このウィンドウでは、インベントリタスクのスキャン範囲の追加や設定ができます。

インベントリ範囲の設定

設定	説明
スキャン範囲名	スキャン範囲の名前を入力するフィールド。この名前は、［**スキャン範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、タスクの実行時にこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、タスクの実行中にこのスキャン範囲が処理されます。 このチェックボックスをオフにすると、タスクの実行中にこのスキャン範囲は処理されません。このチェックボックスをオンにすることにより、後からこの範囲をタスク設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	スキャン範囲に含めるローカルディレクトリのパスを入力するフィールド。パスの指定にマスクを使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 このフィールドを空白のままにすることはできません。
マスク	このリストには、タスクの実行中にスキャンするオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

除外セクション

スキャンの除外の設定

設定のグループ	説明
除外範囲	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**除外範囲**］ウィンドウが表示されます。このウィンドウでは、監視から除外する範囲のリストを指定できます。

［除外範囲］ウィンドウ

この表には、スキャンの除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	スキャンから除外されるディレクトリのパス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［<新しい除外範囲>］ウィンドウ

このウィンドウでは、インベントリタスクのスキャン除外範囲の追加や設定ができます。

除外範囲の設定

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、タスクの実行時にこの範囲を除外するかどうかを選択します。 チェックボックスをオンにすると、タスクの実行中にこの範囲が除外されます。 チェックボックスをオフにすると、タスクの実行中にこの範囲が含まれます。このチェックボックスをオンにすることにより、後からこの範囲をスキャンから除外することができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	インベントリから除外するローカルディレクトリのパスを入力するフィールド。パスの指定にマスクを使用できます。このフィールドを空白のままにすることはできません。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。
マスク	このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。 例： 「*.txt」というマスクはすべてのテキストファイルを表します。 「*_my_file_??.html」というマスクは、任意の文字列から始まって、ファイル名の末尾が「_my_file_」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

コマンドラインのインベントリ

次のようにコマンドラインを使用して、保護されたデバイス上のアプリケーションのインベントリを作成できます：

- Inventory_Scan *事前定義済みタスク*を利用します。このタスクを手動で開始または停止し、タスクの実行スケジュールを設定できます。このタスクの設定を編集することで、スキャン設定を構成できます。

- ユーザーインベントリタスク（*InventoryScan* タイプのタスク）を利用します。ユーザータスクを手動で開始、停止、一時停止、再開し、タスクのスケジュールを設定できます。

アプリケーションコントロールの管理コマンドを使用すると、インベントリタスクの結果としてデバイス上で検知されたアプリケーションのリストを表示できます。

インベントリタスクの設定

この表では、インベントリタスクで指定できるすべての設定と、その設定で使用可能なすべての値と既定値を説明します。

インベントリタスクの設定

設定	説明	値
ScanScripts	スクリプトスキャンを指定します。	Yes（既定値） – スクリプトスキャンを行います。 No – スクリプトスキャンを行いません。
ScanBinaries	バイナリファイルのスキャン（elf、java、pyc）を指定します。	Yes（既定値） – バイナリをスキャンします。 No – バイナリをスキャンしません。
ScanAllExecutable	実行可能なファイルのスキャンを指定します。	Yes（既定値） – 実行可能なファイルをスキャンします。 No – 実行ファイルをスキャンしません。
CreateGoldenImage	インベントリタスクによってデバイス上で検知されたアプリケーションをゴールデンイメージカテゴリに追加します。CreateGoldenImage=Yes の場合、アプリ管理ルールで「ゴールデンイメージ」の製品カテゴリを使用できます。	Yes – 検出されたアプリケーションを「ゴールデンイメージ」アプリケーションカテゴリに追加します。 No（既定値） – 検出されたアプリケーションを「ゴールデンイメージ」アプリケーションカテゴリに追加しません。
[ScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	インベントリ範囲の説明。インベントリ範囲に関する詳細情報を含みます。この設定を使用して指定される文字列の最大長は 4096 文字です。	既定値：All objects
UseScanArea	指定されたインベントリ範囲のスキャンを指定します。タスクを実行するには、少なくとも 1 つのインベントリ範囲のスキャンを有効にします。	Yes（既定値） – 指定されたインベントリ範囲をスキャンします。 No – 指定されたインベントリ範囲をスキャンしません。
AreaMask.item_#	インベントリ範囲の制限。インベントリ範囲で、シェル形式のマスクを使用して指定したファイルのみをスキャンします。	既定値：*（すべてのオブジェクトをスキャン）

	この設定が指定されていない場合、インベントリ範囲のすべてのオブジェクトがスキャンされます。この設定には、複数の値を指定できます。	
Path	スキャンされるオブジェクトがあるディレクトリのパス。	< ローカルディレクトリのパス > - 指定されたディレクトリのオブジェクトをスキャンします。 既定値：/usr/bin
[ExcludedFromScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	インベントリの除外範囲の説明。インベントリ範囲に関する詳細情報を含みます。	既定値は定義されていません。
UseScanArea	指定された範囲のインベントリを除外します。	Yes（既定値） – 指定された範囲を除外します。 No – 指定された範囲を除外しません。
AreaMask.item_#	シェルマスクを使用してインベントリの除外範囲を制限します。 この設定が指定されていない場合、インベントリ範囲のすべてのオブジェクトが除外されます。この設定には、複数の値を指定できます。	既定値：*（すべてのオブジェクトを除外）。
Path	除外するオブジェクトを含むディレクトリのパス。	< ローカルディレクトリのパス > - 指定されたディレクトリのオブジェクトをスキャンから除外します。パスの指定にマスクを使用できます。

		アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。

検知されたアプリケーションのリストの表示

デバイスで検出されたアプリケーションのリストを表示するには、次のコマンドを実行します。

```
kesl-control --get-app-list [--json]
```

--json はJSON形式でのデータ出力を意味します。

検知されたアプリケーションに関する次の情報が表示されます：

- **インベントリの日時**。インベントリタスクが実行された日付と時刻
- **アプリケーションの数**。デバイスで検出されたアプリケーションの数
- 次の情報を含むアプリケーションのリスト：
  - **パス**：アプリケーションへのパス。
  - **ハッシュ**。アプリケーションのハッシュ値。

- **タイプ**。アプリケーションタイプ。例えば、`Script`、`Executable`。
- **カテゴリ**。アプリケーションが属するカテゴリ（以前に作成されている場合）。作成されたアプリケーションカテゴリのリストは、コマンド `kesl-control --get-categories` で表示することができます。

新しいカテゴリを追加しても、アプリケーションリストでその情報は自動的に更新されません。アプリケーションリストを更新するには、インベントリタスクを再起動する必要があります。

デバイスコントロール

*デバイスコントロール*コンポーネントは、クライアントデバイスに搭載または接続されたデバイス（例：ハードディスク、カメラ、Wi-Fi モジュールなど）へのユーザーアクセスを管理します。アクセス管理では、外部デバイスの接続時に感染からクライアントデバイスを保護したり、データの消失や漏洩を防止したりできます。

この機能は、KESL コンテナではサポートされていません。

デバイスコントロールコンポーネントは、Kaspersky Endpoint Security の起動時に既定で自動的に有効になります。

デバイスコントロールは、ユーザーアクセスを次のレベルで管理します：

- デバイスコントロールによって分類された**デバイス タイプ**（プリンタ、リムーバブルドライブ、CD / DVD ドライブなど）。次のアクセスモードのいずれかを各デバイスタイプに適用できます：
  - *許可*：この種別のデバイスに対するアクセスが許可されます。
  - *ブロック*：この種別のデバイスに対するアクセスをブロックします。
  - *バスに依存*：デバイスが接続されているバスに設定されたアクセスモードに応じて、デバイスへのアクセスを許可またはブロックします。
  - *ルール別*：デバイスへのアクセスを、アクセスルールに従って許可またはブロックします。*デバイスアクセスルール*は、クライアントデバイスにインストールまたは接続されているデバイスにアクセス可能なユーザーとその時間を決定する一連の設定項目です。

    禁止されたデバイスが接続されると、アプリケーションはルールで指定されたユーザーに対してデバイスへのアクセスを拒否し、通知を表示します。このデバイスで読み取りと書き込みを試行している間、アプリケーションは、ルールで指定されたユーザーの読み取りと書き込みをサイレントにブロックします。

    アクセスモードが［*ルール別*］に設定されているデバイスで操作を実行しようとした時にアクセス時にアクティブなルールが存在しない場合、操作はブロックされます。
- **接続バス**：*接続バス*は、デバイスをクライアントデバイスに接続するために使用するインターフェイスです（USB または FireWire など）。次のアクセスモードのいずれかを接続バスに適用できます：
  - *許可*：この接続バスを使用して接続されたデバイスへのアクセスを許可します。
  - *ブロック*：この接続バスを使用して接続されたデバイスへのアクセスを拒否します。

  たとえば、USB 経由で接続されているすべてのデバイスへのアクセスが拒否される場合があります。

既定では、すべてのデバイスの種別に対して「*接続バスアクセスモードに依存する*」が選択されています。接続バスに対してアクセス*許可*モードが選択されています。デバイスコントロールは、それに応じてユーザーにすべてのデバイスへの完全なアクセスを許可します。

システムデバイスドライバーを介してデバイスの種別または接続バスによってデバイスをブロックすることには、Linux カーネル 3.10、5.14、5.15、5.17、6.1 では対応していません。これらのカーネルと*ルールによる*アクセスモードでは、ファイルのオープンとディレクトリの読み取り（つまり、ファイルとディレクトリの名前の取得）のみがブロックされます。fanotify をサポートしていないシステムでは、ディレクトリの読み取りのブロックにも対応していません。

デバイスコントロールを初めて有効にすると、既知のデバイスまたはバスタイプの検知されたすべてのデバイスに対して *DeviceAllowed* イベントが生成されます。これらのデバイスの管理設定が変更されない限り、後続のコンポーネントの実行時に繰り返しイベントが生成されることはありません。

デバイスコントロールが無効になっている場合、アプリケーションはブロックされているデバイスへのアクセスのブロックを解除します。

デバイスコントロールを有効、無効、および設定できます：

- デバイスコントロール設定によってアクセスが禁止されているデバイスにアクセスしようとした場合の動作モードを選択します。デバイスへのアクセスの試行をブロックするか、通知のみするかを選択します。
- タイプに応じてデバイスアクセスモードを選択します。
- デバイスが接続するバスのアクセスモードを選択します。
- 個々のデバイスを信頼するデバイスのリストに追加することで、デバイスコントロールの範囲から削除します。*信頼するデバイス*は、ユーザーによるフルアクセスが可能なデバイスです。信頼するデバイスのリストに、識別子または識別子マスクでデバイスを追加できます。たとえば、指定した USB デバイスへのアクセスを制限するか、USB ドライブのみに制限できます。他の USB デバイスへのアクセスはできません。

  コマンドライン経由でアプリケーションを管理している場合は、クライアントデバイスで `kesl-control --get-device-list` を実行することで、接続されているデバイスの ID を表示できます。

  Kaspersky Security Center 経由でアプリケーションを管理している場合、クライアントデバイスにインストールまたは接続されているデバイスに関する情報を管理サーバーに送信できます。情報共有は既定で有効になっています。

  > デバイスに関する情報は、クライアントデバイスが現在のポリシーの制御下にあり、ネットワークエージェントと同期されている場合に転送されます（ネットワークエージェントのポリシーのプロパティで指定された頻度で実行され、既定では 15 分ごとに実行されます）。

- デバイスのアクセススケジュールを定義します：ハードドライブ、リムーバブルドライブ、フロッピーディスク、および CD / DVD ドライブのみ。

  > アプリケーションの全般設定で、スキャン中のファイルへのアクセスのブロックが無効になっている場合、デバイスアクセススケジュールを使用してデバイスへのアクセスをブロックすることはできません。

- デバイスのタイプに応じて、デバイスのアクセスルールを定義できます。指定した時間に指定したユーザーのアクセスを許可またはブロックします。

> デバイスコントロールはマウントポイントの除外を無視します。除外ポイントにマウントされたデバイスへのアクセスは、デバイスコントロール設定で制限できます。

Web コンソールでのデバイスコントロールの設定

Web コンソールでは、ポリシーのプロパティ内でデバイスコントロールの設定を行うことができます（**製品設定 → セキュリティコントロール → デバイスコントロール**）。

デバイスコントロールの設定

設定	説明
デバイスコントロールの有効化 / 無効化	この切り替えボタンでは、デバイスコントロールを有効にするかどうかを選択します。 この切り替えボタンは既定でオンになっています。
信頼するデバイスの設定	このリンクをクリックすると、［**信頼するデバイス**］ウィンドウが表示されます。このウィンドウでは、信頼するデバイスのリストにデバイスを追加します。追加するデバイスは、デバイス ID によって指定するか、またはクライアントデバイスで検知されたデバイスのリストから選択します。
デバイスコントロール操作モード	デバイスコントロールルールに従って制限されているデバイスへのアクセス試行への応答処理： • **通知する**。このオプションを選択すると、Kaspersky Endpoint Security は選択したアクセスモードをテストし、デバイスへのアクセス試行の検出に関するイベントを生成します。 • **ブロック**（既定値）：このオプションを選択すると、Kaspersky Endpoint Security はデバイスまたはバスに定義されたアクセスモードを適用します。
デバイス種別のアクセス設定を設定	このリンクをクリックすると、［**デバイス種別**］ウィンドウが表示されます。このウィンドウでは、タイプ別にデバイスへのアクセスを設定できます。
接続バスのアクセス設定	このリンクをクリックすると、［**接続バス**］ウィンドウが表示されます。このウィンドウでは、接続バスのアクセスを設定できます。

［信頼するデバイス］ウィンドウ

この表には、信頼するデバイスのリストが表示されます。既定では、表は空です。

信頼するデバイスの設定

設定	説明
デバイス ID	信頼するデバイスの ID。
デバイス名	信頼するデバイスの名前。
デバイス種別	信頼するデバイスの種別（例：ハードディスクやスマートカードリーダーなど）。
ホスト名	信頼するデバイスに接続済みのホスト名。
コメント	信頼するデバイスに関するコメント。

信頼するデバイスのリストにデバイスを追加できます。追加するデバイスはデバイス ID で指定するか、またはユーザーデバイスで検出されたデバイスのリストから必要なデバイスを選択します。

表内の信頼するデバイスを編集および削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

また、［**インポート**］をクリックしてファイルからデバイスリストをインポートすることも、［**エクスポート**］をクリックして追加したデバイスリストをファイルにエクスポートすることもできます。インポート時に、信頼できるデバイスのリストを置き換えるか、既存のリストにデバイスを追加するかを尋ねるメッセージが表示されます。

［信頼するデバイス］（デバイス ID）ウィンドウ

このウィンドウでは、識別子によってデバイスを信頼するデバイスのリストに追加できます。

ID によるデバイスの追加

設定	説明
デバイス ID	デバイス ID またはデバイス ID のマスクの入力フィールド。デバイス ID を手動で指定するか、［**ホストで検出されたデバイス**］リストから必要なデバイス ID をコピーできます。 識別子を指定するには、次のワイルドカードを使用できます：*（任意の 2 文字以上）または ?（任意の 1 文字）。たとえば、USBSTOR* マスクを指定して、すべての USB ドライブへのアクセスを許可することができます。
コメント	コメントの入力フィールド（任意）。このフィールドは、デバイス ID を入力して［**次へ**］をクリックした後に使用可能になります。

［信頼するデバイス］ウィンドウ（検知されたデバイスのリスト）

このウィンドウでは、既存の管理対象デバイスのリストから選択することで、信頼するデバイスのリストにデバイスを追加できます。

既存のデバイスに関する情報は、現在のポリシーがあり、ネットワークエージェントと同期されている場合にのみ使用できます（ネットワークエージェントのポリシーのプロパティで指定された頻度で、既定では 15 分以内に実行されます）。新しいポリシーを作成し、他に現在のポリシーがない場合、リストは空になります。

リストからデバイスを追加

設定	説明
デバイス種別	このドロップダウンリストでは、［**ホスト上で検出されたデバイス**］表に表示されるデバイスの種別を選択できます。
デバイス ID マスク	デバイス ID のマスクの入力フィールド。
コメント	コメントの入力フィールド（任意）。このフィールドは、デバイスを選択して［**次へ**］をクリックした後に使用可能になります。

［**フィルター**］をクリックすると表示されるウィンドウで、デバイスに関して表示される情報のフィルタリングを設定できます。

［デバイス種別］ウィンドウ

このウィンドウでは、様々な種別のデバイスのアクセスルールを設定できます。

デバイス種別のアクセスルール

設定	説明

ストレージデバイスのデータへのアクセス設定	表には次の列があります：
	• **種別**：デバイス種別（例：ハードディスクやプリンターなど）を表します。
	• **アクセスモード**は、このタイプのデバイスのアクセスモードを表します。次のいずれかのアクセスモードを選択できます：
	  • **許可**：この種別のデバイスに対するアクセスが許可されます。
	  • **ブロック**：この種別のデバイスに対するアクセスをブロックします。
	  • **バスに依存**（既定値）：デバイスを接続する時に使用するバスを対象としたアクセスモードに従って、デバイスへのアクセスが許可またはブロックされます。
	  • ［**ルール別**］：デバイスへのアクセスを、アクセスルールとスケジュールに従って許可またはブロックします。アクセスルールとそのスケジュールを、必要なデバイス種別をクリックして設定できます。

その他のデバイスへのアクセス設定	表には次の列があります：
	• **種別** - デバイスの種別（入力デバイス、サウンドアダプターなど）。
	• **アクセスモード**は、このタイプのデバイスのアクセスモードを表します。次のいずれかのアクセスモードを選択できます：
	  • **許可**：この種別のデバイスに対するアクセスが許可されます。
	  • **ブロック**：この種別のデバイスに対するアクセスをブロックします。［**ブロック**］アクセスモードは、ネットワークアダプターに対しては選択できません。
	  • **バスに依存**（既定値）：デバイスを接続する時に使用するバスを対象としたアクセスモードに従って、デバイスへのアクセスが許可またはブロックされます。

［デバイスアクセス設定］ウィンドウ

このウィンドウでは、指定した種別のデバイスのアクセスモードとアクセスルールを設定できます。

デバイスアクセスの設定

設定	説明
デバイスアクセスモード	選択した種別のデバイスに対するアクセスモード： • **許可**：選択した種別のデバイスに対するアクセスが許可されます。 • **ブロック**：選択した種別のデバイスに対するアクセスがブロックされます。 • **バスに依存**（既定値）：デバイスを接続する時に使用する「バスを対象としたアクセスルール」に従って、デバイスへのアクセスが許可またはブロックされます。 • ［**ルール別**］：デバイスへのアクセスを、アクセスルールとスケジュールに従って許可またはブロックします。

デバイスアクセスルール	表はアクセスルールのリストを含み、次の列で構成されています：
	• **アクセススケジュール** – 既存のアクセススケジュールの名前。
	• **ユーザーおよび / またはグループ** – アクセスルールを適用するユーザーまたはユーザーグループの名前。
	• ［**アクセス**］–スケジュールのアクセスモード：
	  • ［**許可**］（選択した種別のデバイスに対するアクセスが許可されます）。
	  • ［**ブロック**］（選択した種別のデバイスに対するアクセスがブロックされます）。
	• ［**ステータス**］- アクセスルールのステータス：
	  • ［**有効**］- ルールが有効であり、アプリ管理の実行時にこのルールを適用します。
	  • ［**無効**］- ルールは無効であり、アプリ管理の実行時にルールは使用されません。
	既定では、この表には**既定のスケジュール**が含まれています。接続バスによるアクセスがこのデバイス種別で許可されている場合、既定のアクセススケジュールはいつでもすべてのユーザーにデバイスへのフルアクセスを提供します（**\Everyone** オプションは［ユーザーとグループ］のリストで選択されます）。
	アクセスルールは、追加、編集、削除できます。
	［**削除**］をクリックすると、選択した項目が表から削除されます。
	このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

［デバイスアクセスルール］ウィンドウ

このウィンドウでは、デバイスのアクセスルールを設定できます。

デバイスアクセスルール

設定	説明
デバイスアクセスルールの設定	選択した種別のデバイスに対するアクセスモード： • **許可**（既定値）：選択した種別のデバイスに対するアクセスが許可されます。 • **ブロック**：選択した種別のデバイスに対するアクセスがブロックされます。
ユーザーとユーザーグループ	ルールが適用されるユーザーまたはユーザーグループの名前。 規定値は **\All**（すべてのユーザー）です。 ユーザーまたはユーザーグループを追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

ステータス	アクセスルールのステータス： • **有効** - ルールが有効であり、アプリ管理は動作中にこのルールを適用します。 • **無効** - ルールは無効であり、アプリ管理の実行時にルールは使用されません。
デバイスへのアクセススケジュール	デバイスへの特定のユーザーのアクセス用のスケジュール。既定値は**既定のスケジュール**です。異なるスケジュールを設定できます。

［ユーザーまたはグループの選択］ウィンドウ

このウィンドウでは、アクセスルールを設定するローカルまたはドメインのユーザーまたはユーザーグループを指定できます。

アクセスルールの設定

設定	説明
マニュアル	このオプションがオンの場合、下のフィールドに、デバイスアクセスルールを適用するローカルまたはドメインユーザーの名前、あるいはユーザーグループの名前を入力します。
グループまたはユーザーのリスト	このオプションがオンの場合、検索フィールドに、デバイスアクセスコントロールルールを適用するユーザー名またはグループ名の検索条件を入力するか、下のリストからユーザーグループ名を選択できます。

［スケジュール］ウィンドウ

このウィンドウでは、選択したデバイスアクセスルールのスケジュールを指定できます。

アクセススケジュールは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

既定のスケジュールを削除することはできません。

スケジュールウィンドウにアクセス

このウィンドウでは、デバイスのアクセススケジュールを設定できます。スケジュールは、ハードディスク、リムーバブルドライブ、フロッピーディスク、および CD/DVD ドライブに対してのみ設定できます。

［**全般設定**］→［**製品設定**］セクションで、［**スキャン中のファイルアクセスをブロックする**］がオフになっている場合、アクセススケジュールを使用してデバイスへのアクセスをブロックすることはできません。

デバイスへのアクセススケジュール

設定	説明
名前	アクセススケジュールの名前を入力するフィールド。スケジュール名は一意である必要があります。
スケジュールの間隔	この表では、スケジュールの時間間隔（日、時間）を選択できます。 緑でハイライトされた間隔はスケジュールに含まれます。 スケジュールから間隔を除外するには、除外する時間のセルをクリックします。スケジュールから除外された間隔は灰色で強調表示されます。 既定では、すべての時間間隔（1週間 24 時間）がスケジュールに含まれています。

［接続バス］ウィンドウ

このウィンドウでは、接続バスのアクセスモードを設定できます。

バス接続のアクセスモード

設定	説明
接続バス	クライアントデバイスに接続するためにデバイスが使用する接続バス： • **FireWire** • **USB**
アクセスモード	この切り替えボタンは、このバスを使用するデバイスのアクセスモードを設定します： • **許可**（既定）：このバスを使用して接続されたデバイスへのアクセスを許可します。 • **ブロック**：この接続バスを使用して接続されたデバイスへのアクセスを拒否します。

管理コンソールでのデバイスコントロールの設定

管理コンソールでは、ポリシーのプロパティ内でデバイスコントロールの設定を行うことができます（**セキュリティコントロール → デバイスコントロール**）。

デバイスコントロールの設定

設定	説明
デバイスコントロールを有	このチェックボックスでは、デバイスコントロールを有効にするかどうかを選択します。 既定では、このチェックボックスはオンです。

効にする	
信頼するデバイス	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**信頼するデバイス**］ウィンドウが表示されます。このウィンドウでは、信頼するデバイスのリストにデバイスを追加します。追加するデバイスは、デバイス ID によって指定するか、またはクライアントデバイスで検出されたデバイスのリストから選択します。
デバイスコントロール操作モード	デバイスコントロールルールに従って制限されているデバイスへのアクセス試行への応答処理： • **通知する**。このオプションを選択すると、Kaspersky Endpoint Security は選択したアクセスモードをテストし、デバイスへのアクセス試行の検出に関するイベントを生成します。 • **ブロック**（既定値）：このオプションを選択すると、Kaspersky Endpoint Security はデバイスまたはバスに定義されたアクセスモードを適用します。
デバイスコントロールの設定	この設定グループにはウィンドウを開くボタンがあり、タイプ別および接続バス別にデバイスのアクセスモードを設定できます。

［信頼するデバイス］ウィンドウ

この表には、信頼するデバイスのリストが表示されます。既定では、表は空です。

信頼するデバイスの設定

設定	説明
デバイス ID	信頼するデバイスの ID。
デバイス名	信頼するデバイスの名前。
デバイス種別	信頼するデバイスの種別（例：ハードディスクやスマートカードリーダーなど）。
ホスト名	信頼するデバイスに接続済みのホスト名。
コメント	信頼するデバイスに関するコメント。

信頼するデバイスのリストにデバイスを追加できます。追加するデバイスは ID、マスクで指定するか、またはユーザーデバイスで検出されたデバイスのリストから必要なデバイスを選択します。

表内の信頼するデバイスを編集および削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

また、［**詳細設定**］->［**インポート**］をクリックしてファイルからデバイスのリストをインポートしたり、［**詳細設定**］->［**選択項目をエクスポート**］または［**詳細設定**］->［**すべてエクスポート**］をクリックして追加したデバイスのリストをファイルにエクスポートすることもできます。インポート時に、信頼できるデバイスのリストを置き換えるか、既存のリストにデバイスを追加するかを尋ねるメッセージが表示されます。

［信頼するデバイス］ウィンドウ

このウィンドウでは、識別子によってデバイスを信頼するデバイスのリストに追加できます。

ID によるデバイスの追加

設定	説明
デバイス ID	信頼するデバイスのリストに追加するデバイスの識別子または識別子のマスクを入力するフィールド。 識別子を指定するには、次のワイルドカードを使用できます：*（任意の 2 文字以上）または ?（任意の 1 文字）。たとえば、USBSTOR* マスクを指定して、すべての USB ドライブへのアクセスを許可することができます。
ホスト上を検索	ボタンをクリックすると、指定した ID またはマスクを使用して接続されているクライアントデバイスで検出されたデバイスが表示されます。このボタンは［**デバイス ID**］フィールドが空でない場合に使用できます。
検出されたデバイス	表には次の列があります： • **デバイス種別**：信頼するデバイスの種別（例：ハードディスクやスマートカードリーダーなど）が表示されます。 • **デバイス ID** – 検出されたデバイスの ID。 • **デバイス名** – 検出されたデバイスの名前。 • **ホスト名** – 検出されたデバイスに接続済みのクライアントデバイスの名前。
コメント	信頼するデバイスのリストに追加するデバイスに対するコメントを入力するフィールド（オプション）。

クライアントデバイスのデバイスウィンドウ

このウィンドウでは、クライアントデバイスで検知した既存のデバイスのリストから選択することで、信頼するデバイスのリストにデバイスを追加できます。

既存のデバイスに関する情報は、現在のポリシーがあり、ネットワークエージェントと同期されている場合にのみ使用できます（ネットワークエージェントのポリシーで指定された制限内、既定では 15 分以内に実行されます）。新しいポリシーを作成し、他に現在のポリシーがない場合、リストは空になります。

リストからデバイスを追加

設定	説明
ホスト名	接続されているデバイスを検索する管理対象デバイスの名前または名前マスクを入力するフィールド。既定のマスクは * – すべての管理対象デバイスです。
デバイス種別	このドロップダウンリストでは、検索する接続デバイスの種別を選択できます（ハードディスク、スマートカードリーダーなど）。既定では［**All devices**］が選択されています。
デバイス ID	検索するデバイスの識別子または識別子のマスクを入力するフィールド。既定のマスクは * – すべてのデバイスです。

ホスト上を検索	このボタンをクリックすると、指定した設定のデバイスを検索します。検索結果を下の表に示します。

［デバイス種別］ウィンドウ

このウィンドウでは、様々な種別のデバイスのアクセスモードを設定できます。

デバイス種別のアクセスモード

設定	説明
デバイス種別	デバイス種別（ハードディスク、プリンターなど）。
アクセスモード	デバイスアクセスモード。マウスを右クリックして表示されるコンテキストメニューから、次のいずれかのオプションを選択します： • **許可**：選択した種別のデバイスに対するアクセスが許可されます。 • **ブロック**：選択した種別のデバイスに対するアクセスがブロックされます。 • **バスに依存**（既定値）：接続バスのアクセスモードに応じて、デバイスへのアクセスを許可またはブロックします。 • ［**ルール別**］– デバイスへのアクセスを、アクセスルールとスケジュールに従って許可またはブロックします。

アクセスルールとスケジュールは、デバイスタイプをダブルクリックすると開く［**デバイスアクセスルールの設定**］ウィンドウで設定できます。

［デバイスアクセスルールの設定］ウィンドウを設定

このウィンドウでは、選択したデバイス種別に対するアクセスルールとスケジュールを設定します。

このウィンドウは、［**デバイス種別**］ウィンドウでデバイス種別をダブルクリックすると表示されます。

デバイスアクセスルールとスケジュール

設定	説明
ユーザーとユーザーグループ	このリストには、アクセススケジュールを設定するユーザーとグループが含まれます。 既定では、**\Everyone**（すべてのユーザー）が含まれています。 ユーザーまたはユーザーグループを追加、編集、削除できます。
選択したグループのスケジュールに基づくアク	この表には、ユーザーとユーザーグループのアクセススケジュールが表示されます。次の列で構成されています： • **アクセススケジュール** – 既存のアクセススケジュールの名前。スケジュールの隣にあるチェックボックスは、このスケジュールがコンポーネントによって使用されているかを示します。 • **アクセス** – スケジュールのアクセス種別：**許可**（選択した種別のデバイスへのアクセスを許可）または**ブロック**（選択した種別のデバイスへのアクセスを拒否）。

セスルール	スケジュールは、ハードディスク、リムーバブルドライブ、フロッピーディスク、およびCD/DVDドライブに対してのみ設定できます。既定では、この表には**既定**のアクセススケジュールが含まれています。**接続バス**を介したアクセスがこのデバイス種別で許可されている場合、既定のアクセススケジュールはいつでもすべてのユーザーにデバイスへのフルアクセスを提供します（**\Everyone** は［ユーザーおよびユーザーグループ］のリストで選択されます）。 選択したユーザーのアクセススケジュールを追加、編集、削除できます。**既定の**スケジュールは、編集や削除はできません。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

［ユーザーまたはグループ］ウィンドウ

このウィンドウでは、デバイスアクセスルールを適用するユーザーまたはユーザーグループを指定できます。

デバイスアクセスルールの設定

設定	説明
種別	アプリ管理ルールが適用される［**ユーザー**］または［**グループ**］。
ユーザーまたはグループ名	ルールが適用されるユーザーまたはユーザーグループの名前。

スケジュールウィンドウにアクセス

このウィンドウでは、デバイスのアクセススケジュールを設定できます。

デバイスへのアクセススケジュール

設定	説明
名前	アクセススケジュールの名前を入力するフィールド。
スケジュールの間隔	この表では、スケジュールの時間間隔（日、時間）を選択できます。 緑でハイライトされた間隔はスケジュールに含まれます。 スケジュールから間隔を除外するには、除外する時間のセルをクリックします。スケジュールから除外された間隔は灰色で強調表示されます。 既定では、すべての時間間隔（1週間 24 時間）がスケジュールに含まれています。

［接続バス］ウィンドウ

このウィンドウでは、接続バスのアクセスモードを設定できます。

バス接続のアクセスモード

設定	説明
接続バス	クライアントデバイスに接続するためにデバイスが使用する接続バス：

	• **FireWire** • **USB**
アクセスモード	接続バスのアクセスモード。マウスを右クリックして表示されるコンテキストメニューから、次のいずれかのオプションを選択します： • **許可**（既定）：このバスを使用して接続されたデバイスへのアクセスを許可します。 • **ブロック**：この接続バスを使用して接続されたデバイスへのアクセスを拒否します。

コマンドラインでの Web コントロールの設定

デバイスコントロールの事前定義済みタスク（*Device_Control*）を使用すれば、コマンドラインでデバイスコントロールを管理できます。

デバイスコントロールは既定では実行しません。タスクは、手動で開始および停止できます。

デバイスコントロールの事前定義済みタスクの設定を編集することで、デバイスコントロールを設定できます。

デバイスコントロールコマンドを使用して、接続されているデバイスのリストを表示することもできます。

デバイスコントロールタスクの設定

この表では、デバイスコントロールタスクで指定できるすべての設定と、その設定で使用可能なすべての値と既定値を説明します。

デバイスコントロールタスクの設定

設定	説明	値
OperationMode	デバイスコントロールルールに従って制限されているデバイスへのアクセス試行への応答処理です。	`Block`（既定値）– アプリスまたはバスに定義された用します。 `Notify` – 選択されたアクされ、デバイスへのアクセするイベントを生成します
［**DeviceClass**］セクションには、デバイスの種別に応じたアクセスモードが含まれます。		
HardDrive	クライアントデバイスに接続されたハードドライブに対するアクセスルール。	`Allow` – ハードディスクへーに許可します。 `DependsOnBus`（既定）：アクセスは、接続されているアクセスモードに依存 `Block` – すべてのハードドをユーザーに対してブロックシステムハードディスクにールでブロックされないの

		ByRule – ハードディスク は、アクセスルールに応じ
RemovableDrive	クライアントデバイスに接続されたリムーバブルドライブに対するアクセスルール。	**Allow** – リムーバブルドラ ユーザーに対して許可しま **DependsOnBus**（既定）： ブへのアクセスは、接続さ されているアクセスモード **Block** – リムーバブルドラ ユーザーに対してブロック **ByRule** – リムーバブルド 可否は、アクセスルールに
FloppyDrive	クライアントデバイスに接続されたフロッピーディスクに対するアクセスモード。 本製品は、ISA バスを使用してクライアントデバイスに接続されたフロッピーディスクをブロックしません。	**Allow** – フロッピーディス ーザーに許可します。 **DependsOnBus**（既定）： へのアクセスは、接続され れているアクセスモードに **Block** – フロッピーディス ーザーに対してブロックし **ByRule** – フロッピーディ 否は、アクセスルールに応
OpticalDrive	クライアントデバイスに接続された CD/DVD に対するアクセスモード。	**Allow** – CD/DVD ドライブ ザーに許可します。 **DependsOnBus**（既定）： スは、接続されているバス クセスモードに依存します **Block** – CD/DVD ドライブ ザーに対してブロックしま **ByRule** – CD/DVD ドライ は、アクセスルールに応じ
SerialPortDevice	クライアントデバイスにシリアルポートで接続されているデバイスに対するアクセスモード。 本製品は、ISA バスを使用してシリアルポート経由でクライアントデバイスに接続されたデバイスをブロックしません。	**Allow** – シリアルポートで へのアクセスをユーザーに **DependsOnBus**（既定）： で接続されたデバイスへの クセスモードに依存します **Block** – シリアルポートで へのアクセスをユーザーに す。
ParallelPortDevice	クライアントデバイスにパラレルポートで接続されているデバイスに対するアクセスモード。	**Allow** – パラレルポートで へのアクセスをユーザーに **DependsOnBus**（既定）： で接続されたデバイスへの クセスモードに依存します **Block** – パラレルポートで へのアクセスをユーザーに す。
Printer	クライアントデバイ	**Allow** – プリンターへのア

	スに接続されたプリンターに対するアクセスモード。	許可します。 DependsOnBus（既定）：セスは、接続されているアクセスモードに依存しま Block – プリンターへの対してブロックします。
Modem	クライアントデバイスに接続されたモデムに対するアクセスモード。	Allow – モデムへのアクセします。 DependsOnBus（既定）：は、接続されているバスにセスモードに依存します。 Block – モデムへのアクセてブロックします。
TapeDrive	クライアントデバイスに接続されたテープデバイスに対するアクセスモード。	Allow – テープデバイスーに許可します。 DependsOnBus（既定）：アクセスは、接続されているアクセスモードに依存 Block – テープデバイスーに対してブロックします
MultifuncDevice	クライアントデバイスに接続された多機能デバイスに対するアクセスモード。	Allow – 多機能デバイスーに許可します。 DependsOnBus（既定）：アクセスは、接続されているアクセスモードに依存 Block – 多機能デバイスーに対してブロックします
SmartCardReader	クライアントデバイスに接続されたスマートカードリーダーに対するアクセスモード。	Allow – スマートカードをユーザーに対して許可 DependsOnBus（既定）：ダーへのアクセスは、接続義されているアクセスモー Block – スマートカードをユーザーに対してブロッ
WiFiAdapter	クライアントデバイスに接続された Wi-Fi アダプターに対するアクセスモード。	Allow – Wi-Fi アダプターザーに許可します。 DependOnBus（既定）：Wアクセスは、接続バスのします。 Block – Wi-Fi アダプターザーに対してブロックしま
NetworkAdapter	クライアントデバイスに接続された外部ネットワークアダプターに対するアクセスモード。	Allow – 外部ネットワークセスをユーザーに許可しま DependsOnBus（既定）：ダプターへのアクセスは、に定義されているアクセスす。

		デバイスコントロールて デバイスをネットワーク を避けるため、外部ネッ ーへのアクセスを拒否す ん。
PortableDevice	クライアントデバイスに接続されたポータブルデバイスに対するアクセスモード。	`Allow` – ポータブルデバイ ーザーに許可します。 `DependsOnBus`（既定）： へのアクセスは、接続され れているアクセスモードに `Block` – ポータブルデバイ ーザーに対してブロックし
BluetoothDevice	クライアントデバイスに接続された Bluetooth デバイスに対するアクセスモード。	`Allow` – Bluetooth デバイ ーザーに許可します。 `DependsOnBus`（既定）： のアクセスは、接続されて ているアクセスモードに依 `Block` – Bluetooth デバイ ーザーに対してブロックし
ImagingDevice	クライアントデバイスに接続されたイメージングデバイスに対するアクセスモード。	`Allow` – すべてのイメージ クセスをユーザーに対して `DependsOnBus`（既定）： スへのアクセスは、接続さ されているアクセスモード `Block` – すべてのイメージ クセスをユーザーに対して
SoundAdapter	クライアントデバイスに接続されたサウンドアダプターに対するアクセスモード。	`Allow` – すべてのサウンド セスをユーザーに対して許 `DependsOnBus`（既定）： へのアクセスは、接続され れているアクセスモードに `Block` – すべてのサウンド セスをユーザーに対してブ
InputDevice	クライアントデバイスに接続された入力デバイス（キーボード、マウス、タッチパッド、その他）へのアクセスモード。	`Allow` – 入力デバイスへの に許可します。 `DependsOnBus`（既定）： クセスは、接続されている るアクセスモードに依存し `Block` – 入力デバイスへの に対してブロックします。
[DeviceBus] セクションには、接続バスのアクセスモードが含まれています。		
USB	USB 経由でクライアントデバイスに接続されたデバイスのアクセスモード。	`Allow`（既定値） – USB デ をユーザーに許可します。 `Block` – USB デバイスへの に対してブロックします。
FireWire	FireWire 経由でクライアントデバイスに接	`Allow`（既定値） – FireW で接続されたデバイスへの

	続されたデバイスのアクセスモード。	に許可します。 Block – FireWire インターたデバイスへのアクセスをロックします。
[TrustedDevices.item_#] セクションには、信頼するデバイスが含まれています。		
DeviceId	信頼するデバイスの ID または ID マスクを指定します。	「*」（任意の 2 文字以上）の 1 文字）のマスクを、テクとして使用できます。 例： *指定した USB デバイス* *デバイスへのアクセスを* *の設定を指定します：* ［DeviceBus］セクションを指定します ［TrustedDevices.it で、DeviceId=<device *すべての USB デバイス* *し、すべての USB ドラ* *許可するには、次の設定* ［DeviceBus］セクションを指定します ［TrustedDevices.it で、DeviceId=USBSTOR
Comment	指定された信頼するデバイスへコメントします。	-
[Schedules.item _#] セクションには、デバイスアクセスのスケジュールが含まれています。スケジュールはリムーバブルドライブ、フロッピーディスク、および CD/DVD ドライブに対してのみ設定できます。		
ScheduleName	スケジュールの名前を指定します。 スケジュール名は一意である必要があります。	既定値：Default Default のスケジュールス種別へのアクセスが接続る場合、ユーザーはいつでクセスできます。 Default のスケジュールません。
DaysHours	スケジュールの時間を指定します。	All（既定値） – 24 時間ールです（時間制限なし） < week_day > – 曜日で指定名または省略形のいずれとえば、月曜日の場合は、で指定できます）。平日にの日を指定できます。週にす。 < hour > –時間 [0:24] で指る間隔の単位は時間のみで

		例： Schedule_1 は、日曜日か 時から午前 11 時、午後 1 および午後 4 時から午前 す： [Schedules.item_000 ScheduleName=schedu DaysHours=Su-Sa:0.. Schedule_2 は、木曜日の 後 2 時、金曜日の午前 2 および午後 4 時から午前 す： [Schedules.item_000 ScheduleName=schedu DaysHours=Th:12..14 Schedule_3 は 週 7 日 24 [Schedules.item_000 ScheduleName=schedu DaysHours=All
[HardDrivePrincipals.item_#] セクションには、ハードディスクのアクセスルールが含まれています。 ハードディスクの場合、少なくとも 1 つのスケジュールを常時有効にしておく必要があります。複数のアクセ ィスクに割り当てられます。また、ユーザーまたはユーザーのグループに対して複数のスケジュールを指定 たはグループに対してアクセスルールの競合が発生した場合、最小限のアクセス権が付与されます。		
Principal	アクセスルールが適用されるユーザーまたはユーザーグループを指定します。	`\Everyone`（既定値） – す クセスルールが適用されま `<user name>` – アクセス ーザーの名前を指定します `@<group name>` – アクセ ユーザーのグループの名前
[HardDrivePrincipals.item_#.AccessRules.item_#]	アクセスルールを設定します。	-
UseRule	ルールを有効にするか無効にするかを指定します。	`Yes`（既定値） – アクセス `No` – アクセスルールは無効
ScheduleName	［Schedules.item_#］セクションで指定されたスケジュールです。	既定値：`Default`
Access	アクセスの種別を指定します。	`Allow`（既定値） – ハード スを許可します。 `Block` – ハードディスクへ クします。
[RemovableDrivePrincipals.item_#] セクションには、リムーバブルドライブのアクセスルールが含まれます。 リムーバブルドライブの場合、少なくとも 1 つのスケジュールを常時有効にしておく必要があります。複数の ムーバブルドライブに割り当てられます。また、ユーザーまたはユーザーのグループに対して複数のスケジ す。ユーザーまたはグループに対してアクセスルールの競合が発生した場合、最小限のアクセス権が付与され		
Principal	アクセスルールが適用されるユーザーまたはユーザーグループを指定します。	`\Everyone`（既定値） – す クセスルールが適用されま

		<user name> – アクセス ーザーの名前を指定します @<group name> - アクセ ユーザーのグループの名前
[RemovableDrivePrincipals.item_#.AccessRules.item_#]	アクセスルールを設定します。	-
UseRule	ルールを有効にするか無効にするかを指定します。	Yes（既定値） – アクセス No – アクセスルールは無効
ScheduleName	［Schedules.item_#］セクションで指定されたスケジュールです。	既定値：Default
Access	アクセスの種別を指定します。	Allow（既定値） – リムー アクセスを許可します。 Block – リムーバブルドラ ブロックします。
[FloppyDrivePrincipals.item_#] セクションには、フロッピーディスクのアクセスルールが含まれます。 フロッピードライブの場合、少なくとも1つのスケジュールを常時有効にしておく必要があります。複数のフ ッピーディスクに割り当てられます。また、ユーザーまたはユーザーのグループに対して複数のスケジュール ーザーまたはグループに対してアクセスルールの競合が発生した場合、最小限のアクセス権が付与されます。		
Principal	アクセスルールが適用されるユーザーまたはユーザーグループを指定します。	\Everyone（既定値） – す クセスルールが適用されま <user name> – アクセス ーザーの名前を指定します @<group name> - アクセ ユーザーのグループの名前
[FloppyDrivePrincipals.item_#.AccessRules.item_#]	アクセスルールを設定します。	-
UseRule	ルールを有効にするか無効にするかを指定します。	Yes（既定値） – アクセス No – アクセスルールは無効
ScheduleName	［Schedules.item_#］セクションで指定されたスケジュールです。	既定値：Default
Access	アクセスの種別を指定します。	Allow（既定値） – フロッ クセスを許可します。 Block – フロッピーディス ロックします。
[OpticalDrivePrincipals.item_#] セクションには、CD/DVD ドライブのアクセスルールが含まれます。 CD/DVD ドライブの場合、少なくとも1つのスケジュールを常時有効にしておく必要があります。複数のアク CD/DVD ドライブに割り当てられます。また、ユーザーまたはユーザーのグループに対して複数のスケジュー ユーザーまたはグループに対してアクセスルールの競合が発生した場合、最小限のアクセス権が付与されます		
Principal	アクセスルールが適用されるユーザーまたはユーザーグループを指定します。	\Everyone（既定値） – す クセスルールが適用されま <user name> – アクセス ーザーの名前を指定します

		@< group name > - アクセ ユーザーのグループの名前
[OpticalDrivePrincipals.item_#.AccessRules.item_#]	アクセスルールを設定します。	-
UseRule	ルールを有効にするか無効にするかを指定します。	Yes（既定値） – アクセス No – アクセスルールは無効
ScheduleName	［Schedules.item_#］セクションで指定されたスケジュールです。	既定値：Default
Access	アクセスの種別を指定します。	Allow（既定値） – CD/DV セスを許可します。 Block – CD/DVD ドライブ ックします。

コマンドラインでの接続デバイスリストの表示

管理者 または 監査 のロールがあるユーザーのみが、接続されたデバイスのリストを表示できます。

接続されたデバイスのリストを表示するには、次のコマンドを実行します：

```
kesl-control [-D] --get-device-list
```

接続されたデバイスに関する次の情報が表示されます：

- **デバイス種別**：接続されたデバイスの種別。例：OpticalDrive または HardDrive。
- **識別子**：接続されたデバイスの ID。
- **名前**：接続されたデバイスの名前。
- **パス**：sysfs 仮想オペレーティングシステム内のデバイスへのパス。
- **システムドライブ**：接続されたデバイスがシステムドライブであるかどうかを示します（はいまたはいいえ）。
- **バス**：接続バス。設定可能な値：UnknownBus、USB、FireWire。
- **ドライバー**：sysfs 仮想オペレーティングシステムに読み込まれるドライバーの名前。

ウェブコントロール

ウェブコントロールは、Web リソースへのユーザーアクセスを制御します。これにより、トラフィックの消費を削減し、作業時間の不適切な使用を減らすことができます。ユーザーが Web コントロールによってアクセスが制限されている Web サイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックするか、その Web サイトが望ましくないことをユーザーに伝える警告メッセージを表示します。

Kaspersky Endpoint Security は、HTTP および HTTPS トラフィックのみを監視します。

ウェブコントロールを使用すると、次の方法で Web サイトへのアクセスを設定できます。

- コンテンツカテゴリ。Web サイトの分類は、Kaspersky Security Network、ヒューリスティック分析、既知の Web サイトのデータベース（定義データベースに含まれる）に基づいて分類されます。たとえば、「ソーシャルネットワーク」コンテンツのカテゴリやその他のカテゴリへのユーザーアクセスを制限できます。

- データ種別カテゴリ。たとえば、Web サイト上のデータへのユーザーアクセスを制限したり、グラフィックを非表示にしたりできます。アプリケーションは、拡張子ではなくファイル形式によってデータタイプを決定します。

  > アプリケーションはアーカイブ内のファイルをスキャンしません。たとえば、画像ファイルがアーカイブされている場合、アプリケーションはデータタイプを画像ファイルではなくアーカイブとして検知します。

- ウェブアドレス。Web アドレスまたは Web アドレスマスクを指定できます。

複数の方法を使用して、同時に Web サイトへのアクセスを制御できます。たとえば、「Web メール」のカテゴリの Web サイトに対してのみ、「Office アプリケーションファイル」のデータタイプへのアクセスを制限できます。

既定では、すべての Web リソースに対して選択される *既定のルール*は「**許可**」です。このルールに従って、他の*Web リソースアクセスルール*が定義されていない場合、ウェブコントロールではユーザーが Web リソースにアクセスできるようになります。

他のルールの対象でない Web リソースへのアクセスを本製品がどのように制御するかを制御するウェブコントロールの既定ルールを変更し、**既定のルール**を［*ブロック*］に設定できます。このルールに従って、他の*Web リソースアクセスルール*が定義されていない場合、ウェブコントロールはユーザーが Web リソースにアクセスできないようにします。

Web リソースアクセスルールについて

*Web リソースアクセスルール*は、ルールスケジュールで指定された時間に、ルールに記述された Web リソースにユーザーがアクセスしたときに本製品が実行するフィルターと処理のセットです。フィルターを使用すると、ウェブコントロールコンポーネントによってアクセスが監視される Web リソースを指定できます。

次のフィルターを使用できます：

- **コンテンツカテゴリで絞り込む**。ウェブコントロールはコンテンツに基づいて Web リソースを分類できます。これらのカテゴリで定義されたコンテンツを持つ　Web リソースへのユーザーアクセスを制御できます。ユーザーが選択したコンテンツカテゴリに属する Web リソースにアクセスすると、本製品はルールで指定された処理を実行します。

- **データ種別カテゴリで絞り込む**。ウェブコントロールはデータの種別に基づいて Web リソースを分類できます。特定の種別のデータに関連する Web リソースにあるデータへのユーザーアクセスを制御できます。ユーザーが選択したデータ種別カテゴリに関連する Web リソースにアクセスすると、本製品はルールで指定された処理を実行します。

- **Web リソースアドレスで絞り込む**。Web リソースのすべてのアドレス、Web リソースの個々のアドレス、または Web リソースのアドレスのグループへのユーザーアクセスを制御できます。

  コンテンツカテゴリおよびデータ種別カテゴリによるフィルターと Web リソースアドレスによるフィルターの両方を定義し、指定した Web リソースのアドレスおよび Web リソースアドレスのグループが選択したコンテンツカテゴリまたはデータ種別カテゴリに属する場合、本製品は選択したコンテンツカテゴリおよびデータ種別カテゴリのすべての Web リソースへのアクセスを制御するのではなく、指定した Web リソースのアドレスおよび Web リソースのアドレスのグループへのアクセスのみを制御します。

- **ユーザー名とユーザーグループ名で絞り込む**。ルールに従って Web リソースへのアクセスを制御するユーザーやユーザーグループを定義できます。たとえば、IT 部門を除く組織のすべてのユーザーに対して、インターネットへのブラウザアクセスを制限できます。

- **ルールスケジュール**。スケジュールを設定できます。ルールスケジュールは、ルールで指定された Web リソースへのアクセスを本製品が制御する時間を決定します。たとえば、ブラウザ経由のインターネットアクセスを勤務時間のみに制限できます。

各ルールごとに、ユーザーがルール設定に一致する Web リソースにアクセスしたときに ウェブコントロールが実行する処理を指定できます。

- *許可*。ウェブコントロールを使用すると、ユーザーは Web リソースにアクセスできます。

- *ブロック*。ウェブコントロールは、ユーザーの Web リソースへのアクセスをブロックし、アクセスがブロックされていることを示すメッセージを表示します。ブロックメッセージ内のリンクをクリックすると、ユーザーは誤ったブロックについて企業の LAN 管理者に問い合わせのメッセージを送信し、要求された Web リソースにアクセスできます。

- *通知*。ウェブコントロールには、Web リソースが望ましくないことを示す警告が表示されます。警告メッセージ内のリンクをクリックすると、ユーザーは誤った警告について企業の LAN 管理者に問い合わせのメッセージを送信できます。この場合、ユーザーの Web リソースへのアクセスはブロックされません。

各ルールには優先順位があります。リスト内のルールが上位にあるほど、優先度が高くなります。Web サイトが複数のルールに追加されている場合、ウェブコントロールは最も優先度の高いルールに従って Web サイトへのアクセスを管理します。たとえば、アプリケーションは企業ポータルをソーシャルネットワークとして識別する場合があります。企業の Web ポータルへのアクセスを許可しながらソーシャルネットワークへのアクセスを制限するには、「ソーシャルネットワーク」カテゴリのブロックルールと企業の Web ポータルの許可ルールの 2 つのルールを作成します。企業の Web ポータルのアクセスルールは、ソーシャルネットワークのアクセスルールよりも優先度を高くする必要があります。

ブロックルールが作成されていない場合、HTTPS トラフィックは復号化されません。

Web コンソールでの ウェブコントロールの設定

Web コンソールでは、ポリシーのプロパティ内でウェブコントロールの設定を行うことができます（**製品設定** → **セキュリティコントロール** → **ウェブコントロール**）。

ウェブコントロールコンポーネントの設定

設定	説明

ウェブコントロールが有効/無効	この切り替えボタンでは、ウェブコントロールを有効にするかどうかを選択します。 この切り替えボタンは既定でオフになっています。

ルールリスト	表には、Web リソースアクセスルールのリストが含まれています。ウェブコントロールは、表にリストされている順序でルールを適用します。
	表には次の列があります：
	• **ルール名**。Web リソースアクセスルール名。
	• **ステータス**：Web リソースアクセスルールのステータス：
	  • *有効* – ルールが有効であり、ウェブコントロールは動作中にこのルールを適用します。
	  • *無効* – ルールは無効であり、ウェブコントロールの実行時にルールは使用されません。
	  表内のトグルスイッチを有効または無効にし、［ウェブコントロールルール］ウィンドウで［**このルールを使用する**］チェックボックスをオンまたはオフにできます。
	• **処理**：ルールに一致する Web リソースへのアクセス試行を検出したときに本製品が実行する処理。
	表内の項目に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。
	［**下へ**］をクリックすると、表内で選択した項目が下に移動します。
	このボタンは、1つの項目のみを表から選択している場合に使用できます。
	［**上へ**］をクリックすると、表内で選択した項目が上に移動します。
	このボタンは、1つの項目のみを表から選択している場合に使用できます。
	［**削除**］をクリックすると、選択した項目が表から削除されます。
	このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。
	また、［**インポート**］をクリックしてファイルからルールリストをインポートすることも、［**エクスポート**］をクリックして追加したルールリストをファイルにエクスポートすることもできます。インポート時に、ルールのリストを置き換えるか、既存のリストにルールのリストを追加するかを尋ねるメッセージが表示されます。

デフォルトのルール	他のルールの対象でない Web リソースへのアクセスを本製品がどのように制御するかを制御する既定のルールを選択できます。 • **ルールリストに指定されていないすべてのものを許可して**（既定）、Web リソースへのアクセスを許可します。 • **ルールのリストに指定されていないものをすべてブロックして**、Web リソースへのアクセスをブロックします。
テンプレ	**警告**。入力フィールドには、望ましくない Web リソースへのアクセス試行について警告するルールがトリガーされたときに表示されるメッセージのテンプレートが含まれています。

ート	**ブロックメッセージ**。入力フィールドには、Web リソースへのアクセスをブロックするルールがトリガーされたときに表示されるメッセージのテンプレートが含まれています。 **管理者へのメッセージ**。入力フィールドには、ブロックされた Web リソースをブロックすべきではないとユーザーが考える場合に、企業 LAN の管理者に送信される問い合わせのテンプレートが含まれています。ユーザーがアクセスを要求すると、Kaspersky Endpoint Security は、*Web ページへのアクセスが拒否されたというイベントに関するメッセージを* Kaspersky Security Center の管理者に送信します。イベントの説明には、変数がその値に置き換えられた管理者へのメッセージが含まれます。組織内に Kaspersky Security Center ソリューションが導入されていない場合、または管理サーバーに接続されていない場合、本製品は管理者の指定されたメールアドレスにメッセージを送信します。

［ウェブコントロールルール］ウィンドウ

このウィンドウでは、Web リソースアクセスルールの設定を行うことができます。

Web リソースアクセスルールの追加

設定	説明
ルール名	Web リソースアクセスルールの名前を入力するフィールド。
ステータス	Web リソースアクセスルールのステータスを選択できます。 • *有効* – ルールが有効であり、ウェブコントロールは動作中にこのルールを適用します。 • *無効* – ルールは無効であり、ウェブコントロールの実行時にルールは使用されません。
処理	ルールに一致する Web リソースへのアクセス試行を検出したときにウェブコントロールが実行する処理を選択できます。 • **許可**（既定値）– Web リソースへのアクセスを許可します。 • **ブロック** – Web リソースへのアクセスをブロックし、アクセスがブロックされたことを示すメッセージを表示します。 • **通知** – Web リソースが望ましくないことを示す警告を表示します。警告メッセージ内のリンクをクリックすると、ユーザーは要求された Web リソースにアクセスできます。
コンテンツカテゴリで絞り込む	このチェックボックスでは、コンテンツカテゴリフィルターを有効または無効にします。チェックボックスをオンにすると、**コンテンツカテゴリ**リンクが使用可能になります。このリンクをクリックするとウィンドウが開き、関連するコンテンツカテゴリを選択できます。 既定では、このチェックボックスはオフです。
データ種別カテゴリで絞り込む	このチェックボックスでは、コンテンツカテゴリフィルターを有効または無効にします。チェックボックスをオンにすると、**データ種別カテゴリ**リンクが使用可能になります。このリンクをクリックするとウィンドウが開き、関連するデータ種別カテゴリを選択できます。 既定では、このチェックボックスはオフです。
アドレス	Web リソースアドレスフィルターの使用方法を選択できます。

	• **すべてのアドレスに適用**（既定）。このオプションを選択すると、Web リソースのアドレスフィルターは使用されず、ウェブコントロールルールがすべての Web リソースのアドレスに適用されます。 • **指定したアドレスおよび / またはグループに適用**。このオプションを選択すると、ルールの対象となる Web リソースアドレスの表が使用可能になります。また、クリックすると Web リソースの必要なアドレスを追加できるウィンドウが開く［**アドレスの追加**］ボタンと、Web リソースアドレスのグループを追加できる［**アドレスグループ**］ウィンドウが開く［**グループの追加**］ボタンも使用可能になります。
ユーザー	Web リソースアクセスルールの対象となるユーザーに対してユーザーフィルターを適用する方法を選択できます。 • **すべてのユーザーに適用**（既定）。このオプションを選択すると、ユーザーフィルターは使用されず、ウェブコントロールルールがすべてのユーザーに適用されます。 • **指定したユーザーおよび / またはグループに適用**。このオプションを選択すると、ルールの対象となるユーザーとユーザーグループの表と、［**追加**］ボタンが使用可能になり、［**ユーザーまたはグループの選択**］ウィンドウが開き、ユーザーやユーザーグループを追加できるようになります。
ルールスケジュール	［ウェブコントロールルール］ウィンドウ既定では、スケジュールとして［**常時**］が指定されます。［**常時**］リンクをクリックすると、［**スケジュール**］ウィンドウが開き、ルールの別のスケジュールを設定できます。

［アドレスグループ］ウィンドウ

表には、ウェブコントロールコンポーネントによってユーザーアクセスが制御される Web リソースのアドレスグループが含まれています。既定では、表は空です。

Web リソースアクセスルールの設定

設定	説明
グループ名	ルールが適用される Web リソースアドレスのグループの名前。
グループ内のアドレス数	アドレスグループ内のアドレス数

表内の項目は、追加、編集、削除できます。

このウィンドウのグループリストに新しいアドレスグループを追加する場合は、表の上にある［**追加**］ボタンをクリックして［**グループ**］ウィンドウを開きます。

［**ウェブコントロールルール**］ウィンドウのグループリストにアドレスグループを追加する場合は、表内のグループ名の横にあるチェックボックスをオンにし、表の下の［**ルールにグループを追加**］ボタンをクリックします。

［グループ］ウィンドウ

このウィンドウでは、Web リソースアドレスのグループを追加できます。

Web リソースアクセスルールの設定

設定	説明
グループ名	新しい Web リソースアドレスグループの名前。
アドレス	Web リソースアドレスグループに含まれるアドレスの表。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［ユーザーまたはグループの選択］ウィンドウ

このウィンドウでは、アクセスルールを設定するローカルまたはドメインのユーザーまたはユーザーグループを指定できます。

Web リソースアクセスルールの設定

設定	説明
マニュアル	このオプションがオンの場合、次のフィールドに、Web リソースアクセスルールを適用させるローカルまたはドメインユーザーの名前、あるいはユーザーグループの名前を入力します。
グループまたはユーザーのリスト	このオプションがオンの場合、検索フィールドに、Web リソースアクセスコントロールルールを適用させるユーザー名またはグループ名の検索条件を入力するか、次のリストからユーザーグループ名を選択できます。

［スケジュール］ウィンドウ

このウィンドウでは、選択したデバイスアクセスルールのスケジュールを指定できます。

アクセススケジュールは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

［**常時**］の既定スケジュールは削除または編集できません。

スケジュールウィンドウにアクセス

このウィンドウでは、Web リソースアクセススケジュールを設定できます。

Web リソースアクセススケジュール

設定	説明
名前	アクセススケジュールの名前を入力するフィールド。スケジュール名は一意である必要があります。
スケジュールの間隔	この表では、スケジュールの時間間隔（日、時間）を選択できます。 緑でハイライトされた間隔はスケジュールに含まれます。 スケジュールから間隔を除外するには、除外する時間のセルをクリックします。スケジュールから除外された間隔は灰色で強調表示されます。 既定では、すべての時間間隔（1週間 24 時間）がスケジュールに含まれています。

管理コンソールでの ウェブコントロールの設定

Web コンソールでは、ポリシーのプロパティ内でアプリケーションコントロールの設定を行うことができます（**セキュリティコントロール → ウェブコントロール**）。

ウェブコントロールコンポーネントの設定

設定	説明
ウェブコントロールを有効にする	このチェックボックスは、ウェブコントロールを有効にします。 既定では、このチェックボックスはオフです。

ウェブコントロールの設定	表には、Web リソースアクセスルールのリストが含まれています。ウェブコントロールは、表にリストされている順序でルールを適用します。
	表には次の列があります：
	• **ステータス**：Web リソースアクセスルールのステータス：
	  • *有効*– ルールが有効であり、ウェブコントロールは動作中にこのルールを適用します。
	  • *無効*– ルールは無効であり、ウェブコントロールの実行時にルールは使用されません。
	表内のチェックボックスをオンまたはオフにすることができ、［**ウェブコントロールルール**］ウィンドウで［**このルールを使用する**］チェックボックスをオンまたはオフにすることもできます。
	• **処理**：ルールに一致する Web リソースへのアクセス試行を検出したときに本製品が実行する処理。
	• **Name**。Web リソースアクセスルール名。
	表内の項目に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。
	［**下へ**］をクリックすると、表内で選択した項目が下に移動します。
	このボタンは、1つの項目のみを表から選択している場合に使用できます。

	［**上へ**］をクリックすると、表内で選択した項目が上に移動します。 このボタンは、1つの項目のみを表から選択している場合に使用できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。 また、［**詳細設定**］->［**インポート**］の順にクリックしてファイルからルールのリストをインポートしたり、［**追加**］->［**選択項目をエクスポート**］または［**追加**］->［**すべてエクスポート**］の順にクリックして追加したルールのリストをファイルにエクスポートすることもできます。インポート時に、ルールのリストを置き換えるか、既存のリストにルールのリストを追加するかを尋ねるメッセージが表示されます。
デフォルトのルール	ドロップダウンリストで、他のルールの対象でない Web リソースへのアクセスを本製品がどのように制御するかを制御する既定のルールを選択できます。 • **許可**（既定値）– Web リソースへのアクセスを許可します。 • **ブロック** – Web リソースへのアクセスをブロックします。
メッセージテンプレート	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**メッセージテンプレート**］ウィンドウが表示されます。

［ウェブコントロールルール］ウィンドウ

このウィンドウでは、Web リソースアクセスルールの設定を行うことができます。

ウェブコントロールルールの追加

設定	説明
ルール名	Web リソースアクセスルールの名前を入力するフィールド。
このルールを使用する	このチェックボックスでは、製品の実行時にこのルールを使用するかどうかを選択します。 チェックボックスをオンにすると、ルールが有効になり、ウェブコントロールは実行時にこのルールを適用します。 チェックボックスをオフにすると、ルールは無効になり、ウェブコントロールの実行時には使用されません。チェックボックスをオンにすることで、後でこのウェブコントロールルールの使用を有効にすることができます。 既定では、このチェックボックスはオンです。
コンテンツのフィルタリング	ドロップダウンリストで、Web リソースのコンテンツフィルターを選択できます。 • **フィルタリングしない**（既定値）。この項目を選択すると、Web リソースのコンテンツフィルターは使用されません。 • **コンテンツカテゴリ**。この項目を選択すると、［**選択**］ボタンが使用可能になります。このボタンをクリックすると、［**コンテンツカテゴリ**］ウィンドウが表示されます。

	• **データタイプカテゴリ**。この項目を選択すると、［**選択**］ボタンが使用可能になります。このボタンをクリックすると、［**データ種別**］ウィンドウが表示されます。 • **コンテンツカテゴリとデータ種別カテゴリ**。この項目を選択すると、［**選択**］ボタンが使用可能になります。これらのボタンをクリックするとウィンドウが開き、必要なカテゴリを選択できます。
アドレスのフィルタリング	ドロップダウンリストでは、Web リソースのアドレスのフィルターを選択できます： • **すべてのアドレス**（既定値）。この項目を選択すると、Web リソースのアドレスフィルターは使用されず、ウェブコントロールルールがすべての Web リソースのアドレスに適用されます。 • **指定のアドレス**。この項目を選択すると、［**アドレスの選択**］ボタンが使用可能になります。このボタンをクリックすると、［**アドレスの選択**］ウィンドウが開き、必要な Web リソースアドレスを選択できます。
適用するユーザー	ドロップダウンリストで、Web リソースアクセスルールを適用するユーザーを選択できます。 • **すべてのユーザー**（既定値）。この項目を選択すると、ユーザーフィルターは使用されず、ウェブコントロールルールがすべてのユーザーに適用されます。 • **選択したユーザー**。この項目を選択すると、［**ユーザーの選択**］ボタンが使用可能になります。このボタンをクリックすると、［**ユーザーの選択**］ウィンドウが表示されます。
ルールスケジュール	ドロップダウンリストで、Web リソースアクセスルールのスケジュールを設定できます： • **常時**（既定値）。この項目を選択すると、Web リソースのアクセスルールが時間制限なしで、常に適用されます。 • **<スケジュール名>**。この項目を選択すると、［**削除**］ボタンと［**編集**］ボタンが使用可能になり、クリックしてスケジュールを削除または構成できます。 • **新規スケジュールを追加**。この項目を選択すると、［**アクススケジュール**］ウィンドウが開き、Web リソースアクセスルールのスケジュールを設定できます。
ルールアクション	ドロップダウンリストでは、ルールに一致する Web リソースへのアクセス試行を検出したときにウェブコントロールが実行する処理を選択できます。 • **許可**（既定値）– Web リソースへのアクセスを許可します。 • **ブロック** – Web リソースへのアクセスをブロックし、アクセスがブロックされたことを示すメッセージを表示します。 • **通知** – Web リソースが望ましくないことを示す警告を表示します。警告メッセージ内のリンクをクリックすると、ユーザーは要求された Web リソースにアクセスできます。

［コンテンツカテゴリの選択］ウィンドウ

このウィンドウでは、アクセスを制御するコンテンツカテゴリを選択できます。

これを行うには、関連するカテゴリの横にあるチェックボックスをオンにします。

既定では、すべてのチェックボックスがオフになっています。

ネストされたコンテンツカテゴリの横にあるチェックボックスを選択しても、ネストされたカテゴリを含む主なコンテンツカテゴリの横にあるチェックボックスは自動的に選択されません。

［データ種別カテゴリの選択］ウィンドウ

このウィンドウでは、アクセスを制御する種別カテゴリを選択できます。

これを行うには、関連するカテゴリの横にあるチェックボックスをオンにします。

既定では、すべてのチェックボックスがオフになっています。

［アドレスの選択］ウィンドウ

このウィンドウでは、ユーザーアクセスを制御する Web リソースのアドレスを指定できます。複数のアドレスを指定できます。コピーしやすいように、各アドレスを新しい行に入力します。アドレスの指定にマスクを使用できます。

アドレスのグループを指定する場合は、［**アドレス グループの追加**］ボタンをクリックして［**アドレスグループの選択**］ウィンドウを開きます。

［アドレスグループの選択］ウィンドウ

表には、ウェブコントロールコンポーネントによってユーザーアクセスが制御される Web リソースのアドレスグループが含まれています。

［**アドレスの選択**］ウィンドウのグループリストにアドレスグループを追加する場合は、表内のグループ名の横にあるチェックボックスをオンにし、表の下の［**追加**］ボタンをクリックします。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

このウィンドウのグループリストに新しいアドレスグループを追加する場合は、表の上にある［**追加**］**ボタンをクリックして**［アドレスグループの追加］ウィンドウを開きます。

既定では、表は空です。

［アドレスグループの追加］ウィンドウ

このウィンドウでは、ユーザーアクセスを制御するWebリソースのアドレスグループを指定できます。アドレスグループには、複数のアドレスを指定できます。コピーしやすいように、各アドレスを新しい行に入力します。アドレスの指定にマスクを使用できます。

［ユーザーの選択］ウィンドウ

表には、ルールに従ってWebリソースへのアクセスが制御されるユーザーとユーザーグループの名前が含まれます。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

このウィンドウのユーザーリストに新しいユーザーやユーザーグループを追加する場合は、表の上にある［**追加**］ボタンをクリックして、［**ユーザーまたはグループ**］ウィンドウを開きます。

既定では、表は空です。

［ユーザーまたはグループ］ウィンドウ

このウィンドウでは、Webリソースアクセスルールを適用するユーザーまたはユーザーグループを指定できます。

Webリソースアクセスルールの設定

設定	説明
種別	アプリ管理ルールが適用される［**ユーザー**］または［**グループ**］。
ユーザーまたはグループ名	ルールが適用されるユーザーまたはユーザーグループの名前。

スケジュールウィンドウにアクセス

このウィンドウでは、Webリソースアクセススケジュールを設定できます。

Webリソースアクセススケジュール

設定	説明
名前	アクセススケジュールの名前を入力するフィールド。
スケジュールの間隔	この表では、スケジュールの時間間隔（日、時間）を選択できます。 緑でハイライトされた間隔はスケジュールに含まれます。 スケジュールから間隔を除外するには、除外する時間のセルをクリックします。スケジュールから除外された間隔は灰色で強調表示されます。 既定では、すべての時間間隔（1週間 24 時間）がスケジュールに含まれています。

ウェブコントロールメッセージテンプレートの設定

ウェブコントロールルールのプロパティで指定された処理に応じて、ユーザーが Web リソースにアクセスしようとすると、本製品は次のいずれかの種類のメッセージを表示します（HTTP サーバー応答をメッセージを含む HTML ページに置き換えます）。

- 警告。この種別のメッセージは、Web リソースへのアクセスが望ましくないこと、および企業のセキュリティポリシーに違反していることをユーザーに警告します。この Web リソースに一致するルールの設定で**通知**処理が選択されている場合、本製品は警告メッセージを表示します。

  ユーザーが警告が間違いだと思った場合、警告内のリンクを使用して、自動生成された問い合わせメッセージを会社の LAN 管理者に送信できます。

- ブロックされた Web リソースメッセージ この Web リソースに一致するルールの設定で**ブロック**処理が選択されている場合、本製品は Web リソースがブロックされたことを示すメッセージを表示します（下の図を参照）。

  ユーザーが Web リソースをブロックすべきではないと考える場合は、ブロックされた Web リソースメッセージ内のリンクを使用して、自動的に生成された問い合わせを会社の LAN 管理者に送信できます。

警告メッセージ、ブロックされた Web リソースメッセージ、会社の LAN 管理者への問い合わせメッセージ用のテンプレートが提供されます。内容は編集できます。

Web コンソールでメッセージテンプレートを変更します：

1. Web コンソールのメインウィンドウで、**アセット（デバイス）→ ポリシーとポリシープロファイル**タブを順に選択します。

   ポリシーのリストが表示されます。

2. ポリシーを適用するデバイスを含む管理グループを選択します。そのためには、ウィンドウ上部の**現在のパス**フィールドのリンクをクリックし、開いたウィンドウで管理グループを選択します。

   リストには、選択した管理グループに設定されているポリシーが表示されます。

3. リスト内の必要な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が表示されます。

4. ポリシープロパティウィンドウで、**製品設定 → セキュリティコントロール → ウェブコントロール**の順に選択します。

5. ［**テンプレート**］セクションの次のタブでウェブコントロールのメッセージテンプレートを設定します：

   - **警告**。入力フィールドには、望ましくない Web リソースへのアクセス試行について警告するルールがトリガーされたときに表示されるメッセージのテンプレートが含まれています。

   - **ブロックメッセージ**。入力フィールドには、Web リソースへのアクセスをブロックするルールがトリガーされたときに表示されるメッセージのテンプレートが含まれています。

   - **管理者へのメッセージ**。入力フィールドには、ブロックされた Web リソースをブロックすべきではないとユーザーが考える場合に、企業 LAN の管理者に送信される問い合わせのテンプレートが含まれています。ユーザーがアクセスを要求すると、Kaspersky Endpoint Security は、*Web ページへのアクセスが拒否されたというイベントに関するメッセージを* Kaspersky Security Center の管理者に送信します。イベントの説明には、変数がその値に置き換えられた管理者へのメッセージが含まれます。組織内に Kaspersky Security Center ソリューションが導入されていない場合、または管理サーバーに接続されていない場合、本製品は管理者の指定されたメールアドレスにメッセージを送信します。

［**警告**］タブと［**ブロックメッセージ**］タブでは、［**変数の追加**］ボタンと［**リンクの追加**］ボタンを使用して、ユーザーへのメッセージに変数とリンクを追加できます。［**既定**］ボタンをクリックすると、メッセージテンプレートのテキストを復元できます。

6. ［**OK**］をクリックします。

7. **保存**をクリックして、変更内容を保存します。

管理コンソールでメッセージテンプレートを変更します：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、関連するデバイスが属する管理グループの名前が付いているフォルダーを選択します。

2. 作業領域で、［**ポリシー**］タブを選択します。

3. ポリシーのリストで必要なポリシーを選択し、ダブルクリックして**プロパティの <ポリシー名>** ウィンドウが開きます。

   ポリシーのコンテキストメニューの**プロパティ**項目を使用するか、ポリシー設定のセクションでポリシーのリストの右側にある**ポリシー設定の構成**リンクをクリックして、ポリシーのプロパティウィンドウを開くこともできます。

4. ポリシーウィンドウで、［**セキュリティコントロール**］→［**ウェブコントロール**］の順に選択します。

5. ［**メッセージテンプレート**］セクションで、［**設定**］ボタンをクリックします。

6. これにより、［**メッセージテンプレート**］ウィンドウが開きます。そのウィンドウ上の次のタブで ウェブコントロールメッセージテンプレートを設定します：

   - **警告**。入力フィールドには、望ましくない Web リソースへのアクセス試行について警告するルールがトリガーされたときに表示されるメッセージのテンプレートが含まれています。

   - **ブロックメッセージ**。入力フィールドには、Web リソースへのアクセスをブロックするルールがトリガーされたときに表示されるメッセージのテンプレートが含まれています。

   - **管理者への問い合わせ**。入力フィールドには、ブロックされた Web リソースをブロックすべきではないとユーザーが考える場合に、企業 LAN の管理者に送信される問い合わせのテンプレートが含まれています。ユーザーがアクセスを要求すると、Kaspersky Endpoint Security は、*Web ページへのアクセスが拒否されたというイベントに関するメッセージを* Kaspersky Security Center の管理者に送信します。イベントの説明には、変数がその値に置き換えられた管理者へのメッセージが含まれます。これらのイベントは、Kaspersky Security Center コンソールの［**ユーザのリクエスト**］の選択を使用して表示できます。組織内に Kaspersky Security Center ソリューションが導入されていない場合、または管理サーバーに接続されていない場合、本製品は管理者の指定されたメールアドレスにメッセージを送信します。

   ［**警告**］タブと［**ブロックメッセージ**］タブでは、［**変数**］ボタンと［**リンクの挿入**］ボタンを使用して、ユーザーへのメッセージに変数とリンクを追加できます。［**既定**］ボタンをクリックすると、メッセージテンプレートのテキストを復元できます。

7. ［**OK**］をクリックします。

8. ［**適用**］をクリックします。

コマンドラインでのウェブコントロールの設定

コマンドラインでは、ウェブコントロールの事前定義済みタスク（*Web_Control*）を使用してウェブコントロールを管理できます。

ウェブコントロールタスクは既定で停止されます。タスクは、手動で開始および停止できます。

ウェブコントロールの事前定義済みタスクの設定を変更することで、ウェブコントロールの設定を編集できます。

ウェブコントロール管理コマンドを使用して、 ウェブコントロール設定を表示および編集することもできます。

ウェブコントロールタスクの設定

次の表では、ウェブコントロールタスクで指定できるすべての設定と、その設定で使用可能なすべての値と既定値を説明します。

ウェブコントロールタスクの設定

設定	説明	値
`WebControlDefaultAction`	既定のルール、つまり、他のルールの対象でない Web リソースへのアクセス試行を検出したときにウェブコントロールが実行する処理です。	許可（既定値）– Web リソースへのアクセスを許可します。 ブロック – Web リソースへのアクセスをブロックします。
`ComplaintRecipient`	Web リソースの誤ったブロックに関するメッセージが送信される管理者のメールアドレス。	
［Rules.item_#］セクションには、次の設定が含まれています：		
名前	Web リソースアクセスルール名。	
`WebControlAction`	ルールに一致する Web リソースへのアクセス試行を検出したときにウェブコントロールが実行するルールの処理。	許可（既定値）– Web リソースへのアクセスを許可します。 ブロック – Web リソースへのアクセスをブロックします。 通知 – Web リソースが望ましいことを示す警告を表示します。告メッセージ内のリンクをクすると、ユーザーは要求されWeb リソースにアクセスできます。
`Enabled`	Web リソースアクセスルールのステータス。	`Yes` – ルールが有効であり、コントロールは動作中にこのを適用します。 `No`（既定値）– ルールは無効り、ウェブコントロールの実ルールは使用されません。
`ScheduleId`	`[Schedules.item_#]`セクションで使用されるス	

	ケジュール ID。	
UseUrls	ルール内での Web リソースアドレスフィルターの使用。	Yes – ルールで Web リソースアドレスフィルターを使用します No（既定値）– Web リソースアドレスフィルターを使用せず、すべての Web リソースアドレスに適用します。
Urls.item_#	ルールがアクセスを制御する Web リソースのアドレス。	Web リソースアドレスの指定スクを使用できます。
UseCategories	ルール内のコンテンツカテゴリとデータ種別カテゴリによるフィルターの使用。	なし（既定）– Web リソースコンテンツフィルターを使用しま ContentOnly – ルールでコンテンツカテゴリフィルターを使用します。 FormatOnly – ルールでデータ種別カテゴリフィルターを使用し ContentAndFormat – ルールでコンテンツカテゴリフィルターとデータ種別カテゴリフィルターを使用します。
[Rules.item_#.ContentCategories.item_#]	コンテンツカテゴリを指定するセクション。	–
ContentCategory	コンテンツカテゴリ。	AdultContent, AlcoholTobaccoNarcotics Violence, Profanity, We ChatForum, WebMail, OnlineShops, SocialNets, Recruitment HttpQueryRedirection, CreditCards, PoliceDecision, SoftwareAudioVideo, TechnologyElectronics, GamblingLotteriesSweeps InternetCommunicationMe CryptocurAndMining, LegislationBE, ECommerce, ComputerGame Religions, News, Torrents, FileSha AudioAndVideo, BankSite Blogs, DatingSites, Legislatio LegislationGlobal, SexuallyExplicit, Sexuality, GenerativeAI

[Rules.item_#.FormatCategories.item_#]	データ種別カテゴリを指定するセクション。	–
FormatCategories.item_#.FormatCategory	データ種別カテゴリ。	Video – ビデオ Audio – オーディオデータ OfficeDocument – Office アーションファイル Executable – 実行ファイル Archives – アーカイブ Images – 画像ファイル Scripts – スクリプト
UsePrincipals	Web リソースアクセスルールの対象となるユーザーのフィルターの使用。	Yes – ルールでユーザーフィを使用します。 No（既定値）– ユーザーフィを使用せず、すべてのユーザールを適用します。
[Rules.item_#.Principals.item_#]	Web リソースアクセスルールの対象となるユーザーを指定するセクション。	
名前	Web リソースアクセスルールの対象となるユーザーまたはユーザーグループ。	< ユーザ名 > ：ルールを適用ーザーの名前。 @< グループ名 > ：ルールを適るユーザーのグループの名前 既定値：Web リソースアクールはすべてのユーザーに適ます。
［UrlCategories.item_#］セクションには、次の設定が含まれています：		
名前	ルールがアクセスを制御する Web リソースアドレスのグループの名前。	
Urls.item_#	グループに属する Web リソースのアドレス。	Web リソースアドレスの指定スクを使用できます。
［Schedules.item _#］セクションには、ルールのスケジュールが含まれています。		
Id	［Rules.item_#］セクションで使用されるスケジュール ID。	1 から 999999 0 が既定のスケジュールの I り、ルールは時間制限なして機能します。
名前	スケジュールの名前を指定します。	
DaysHours	スケジュールの時間を指定します。	< week_day > – 曜日で指定し完全な曜日名または省略形のかを使用できます（たとえに日の場合は、Mo、Mon、Mor指定できます）。平日には、たは特定の日を指定できます日曜日から始まります。

		< hour > ―時間 [0:24] で指定す。指定できる間隔の単位はみです。

ウェブコントロール設定の表示と編集

ウェブコントロール設定を表示するには、次のコマンドを実行します：

```
kesl-control --get-settings 26 --file <設定情報ファイルのパス> [--jason]
```

説明：

`--file <設定情報ファイルのパス>` – 設定がエクスポートされる構成ファイルへの絶対パス。

`--json`：データを JSON 形式で出力します。

ウェブコントロール設定を編集するには、次のコマンドを実行します：

```
kesl-control --set-settings 26 [--file <設定情報ファイルのパス>] [--json]
```

説明：

`--file <設定情報ファイルのパス>` – 設定がインポートされる設定情報ファイルへの絶対パス。

`--json` – JSON ファイルからデータをインポートします。

構成された設定を削除し、ウェブコントロール設定を既定のルールにリセットするには、次のコマンドを実行します：

```
kesl-control --set-settings 26 --set-to-default
```

Web リソースアドレスマスクを作成するためのルール

Web リソースアドレスマスク（「アドレスマスク」）は、Web リソースアクセスルールを作成するときに、Web リソースの類似したアドレスを多数入力する必要がある場合に便利です。巧みに形成されたアドレスマスク 1 つで、Web リソースの多数のアドレスを置き換えることができます。

アドレスマスクを作成するときは、次のルールを適用します：

1. `*` 文字は、0 個以上の文字のシーケンスを置き換えます。

   たとえば、アドレスマスク `*abc*` を入力すると、Web リソースアクセスルールはシーケンス `abc` を含むすべてのアドレスに適用されます。例：`http://www.example.com/page_0-9abcdef.html`。

2. 文字列 `*.` を使用すると、アドレスのすべてのドメインを選択できます。これが *ドメインマスク*を表します。ドメインマスク `*.` は、任意のドメイン名、サブドメイン名、または空の文字列として解釈されます。

   例：次のアドレスは `*.example.com` マスクと一致します。

   - `http://pictures.example.com` – ドメインマスク `*.` は `pictures.` と一致します。

- `http://user.pictures.example.com` – ドメインマスク `*.` は `pictures.` および `user.` と一致します。

- `http://example.com` – ドメインマスク `*.` は空の文字列として解釈されます。

3. アドレスマスクの先頭にある文字シーケンス `www.` は、シーケンス `*.` として解釈されます。

   例：アドレスマスク `www.example.com` は `*.example.com` として解釈されます。マスクは、アドレス `www2.example.com` および `www.pictures.example.com` と一致します。

4. アドレスマスクが `*` 文字で始まっていない場合、アドレスマスクは `*` で始まっている場合と同じ内容に一致します。

5. アドレスマスクが `/` または `*` 以外の文字で終わる場合、アドレスマスクは `/*` で終わる場合と同じ内容に一致します。

   例: アドレス マスク `http://www.example.com` は、 `http://www.example.com/abc` 形式のアドレスと一致します。ここで、 `a`、 `b`、 `c` は任意の文字です。

6. アドレスマスクが `/` の文字で終わる場合、アドレスマスクは `/*` で終わる場合と同じ内容に一致します。

7. アドレスマスクの末尾の文字シーケンス `/*` は、 `/*` または空の文字列として解釈されます。

8. Web リソースアドレスをアドレスマスクと比較する場合、プロトコル（http: または https:）が考慮されます。

   - アドレスマスクにネットワークプロトコルがない場合、アドレスマスクは任意のネットワークプロトコルのアドレスと一致します。

     例：アドレスマスク `example.com` は、アドレス `http://` `example.com` および `https://` `example.com` と一致します。

   - アドレスマスクにネットワークプロトコルが存在する場合、同じネットワークプロトコルのアドレスのみがアドレスマスクと一致します。

     例：アドレスマスク `http://*.example.com` はアドレス `http://www.example.com` と一致しますが、アドレス `https://www.example.com` とは一致しません。

9. 二重引用符で囲まれたアドレスマスクは、アドレスマスクに最初から含まれていた `*` 文字を除き、それ以上の置換なしで解釈されます。二重引用符で囲まれたアドレスマスクの場合、ルール 5 と 7 は適用されません（下の表の例 14 〜 18 を参照）。

10. Web リソースアドレスマスクの評価では、ユーザー名とパスワード、接続ポート、大文字と小文字は考慮されません。

アドレスマスクを構築するためのルールの適用例

No.	アドレスマスク	Web リソースアドレス	アドレスはアドレスマスクと一致していますか?	コメント
1	*.example.com	http://www.123example.com	No	ルール 1 を参照してください。
2	*.example.com	http://www.123.example.com	はい	ルール 2 を参照してください。
3	*example.com	http://www.123example.com	はい	ルール 1 を参照して

				ください。
4	*example.com	http://www.123.example.com	はい	ルール 1 を参照してください。
5	http://www.*.example.com	http://www.123example.com	No	ルール 1 を参照してください。
6	www.example.com	http://www.example.com	はい	ルール 3、2、1 を参照してください。
7	www.example.com	https://www.example.com	はい	ルール 3、2、1 を参照してください。
8	http://www.*.example.com	http://123.example.com	はい	ルール 3、4、1 を参照してください。
9	www.example.com	http://www.example.com/abc	はい	ルール 3、5、1 を参照してください。
10	example.com	http://www.example.com	はい	ルール 3 と 1 を参照してください。
11	http://example.com/	http://example.com/abc	はい	ルール 6 を参照してください。
12	http://example.com/*	http://example.com	はい	ルール 7 を参照してください。
13	http://example.com	https://example.com	No	ルール 8 を参照してください。
14	"example.com"	http://www.example.com	No	ルール 9 を参照してください。
15	"http://www.example.com"	http://www.example.com/abc	No	ルール 9 を参照してください。
16	"*.example.com"	http://www.example.com	はい	ルール 1 と 9 を参照してください。
17	"http://www.example.com/*"	http://www.example.com/abc	はい	ルール 1 と 9 を参照してください。
18	"www.example.com"	http://www.example.com; https://www.example.com	はい	ルール 9 と 8 を参照してください。
19	www.example.com/abc/123	http://www.example.com/abc	No	アドレスマスクには、Web リソースアドレスよりも多くの情報が含まれます。

システム変更監視

Kaspersky Endpoint Security は、保護対象デバイス上のオペレーティングシステムの整合性をリアルタイムまたはオンデマンドで監視します。

- *システム変更監視*は、コンポーネント設定の監視範囲に追加したファイルとディレクトリの変更をリアルタイムで追跡します。保護対象デバイス上のセキュリティ侵害を示す可能性のあるファイルの変更を追跡できます。
- *システム整合性チェック*のタスクを使用すると、監視対象オブジェクトの現在の状態を以前に記録された状態と比較することにより、監視範囲に追加したファイルおよびディレクトリの変更をチェックできます。

システム変更監視を使用するには、この機能を含むライセンスが必要です。

この機能は、KESL コンテナではサポートされていません。

監視範囲内のファイルまたはディレクトリへの変更を検知すると、Kaspersky Endpoint Security はオブジェクトのアクセスコントロールリストの変更に関するイベントを生成します。システム変更監視は、行われた正確な変更に関するデータを共有しません。*システム整合性チェック*のタスクは、変更された属性、および移動されたファイルとディレクトリに関するデータを送信します。

リアルタイムのシステム整合性監視

システム変更監視は、ファイル操作をリアルタイムで傍受することにより、監視範囲内のオブジェクトへの各変更を検出します。

システム変更監視が実行されると、アプリケーションは次のファイル設定の変更を監視します：

- コンテンツ（write ()、truncate () など）
- メタデータ（所有者権限（chmod / chown））
- タイムスタンプ（utimensat）
- 拡張属性（setxattr）など

チェックサムのファイルは計算されていません。

Linuxオペレーティングシステムの技術的制限により、アプリケーションはファイルに変更を加えたユーザーやプロセスを特定することができません。

既定では、システム変更監視は無効になっています。システム変更監視を有効、無効、および設定できます：

- システム変更監視の監視範囲を定義するアプリケーションは、システム変更監視の設定で定義された監視範囲内のファイルに対する操作を監視します。コンポーネントが動作するためには、少なくとも1つの監視範囲を指定する必要があります。既定では、*カスペルスキー内部オブジェクト*（/opt/kaspersky/kesl/）の監視範囲が定義されています。

  複数の監視範囲を指定できます。リアルタイムモードで監視範囲を変更できます。

アプリケーションタスクは、監視範囲外にあるハードリンクを持つファイルの変更（属性と内容）を監視しません。

- 名前のマスクを使用して、監視対象からオブジェクトを除外することができます。
- システム変更監視の除外範囲を設定します。除外は各個別の範囲に対して定義され、示された範囲に対してのみ機能します。複数の監視除外を指定できます。

  除外は監視範囲よりも優先順位が高く、除外されたオブジェクトは監視範囲内であってもスキップされます。監視範囲が除外されたディレクトリよりも低いレベルで定義されている場合、アプリケーションはシステム変更監視中にこの監視範囲をスキップします。

ディレクトリが監視または除外範囲に追加されると、アプリケーションはそのディレクトリが存在するかどうかをチェックしません。

Web コンソールでのシステム変更監視の設定

Web コンソールでは、ポリシーのプロパティ（**製品設定 → セキュリティコントロール →システム変更監視**）でシステム変更監視設定を構成できます。

システム変更監視の設定

設定	説明
システム変更監視の有効化 / 無効化	この切り替えボタンでは、システム変更監視コンポーネントを有効にするかどうかを選択します。 この切り替えボタンは既定でオフになっています。
監視範囲	［**監視範囲を設定する**］をクリックすると、［**監視範囲**］ウィンドウが表示されます。
除外範囲	［**監視からの除外範囲を設定する**］をクリックすると、［**除外範囲**］ウィンドウが表示されます。
マスクによる除外	［**除外をマスクで設定する**］をクリックすると、［**マスクによる除外**］ウィンドウが表示されます。

［監視範囲］ウィンドウ

この表には、システム変更監視コンポーネントの監視範囲が表示されます。表で指定されたパスのファイルとディレクトリが監視されます。表には既定で、**Kaspersky の内部オブジェクト**の監視範囲（/opt/kaspersky/kesl/）が表示されています。

システム変更監視の監視範囲の設定

設定	説明
範囲名	監視範囲名。
パス	保護されるディレクトリのパス。
ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、範囲の表の並び順でスキャンされます。必要に応じて、サブディレクトリを親ディレクトリよりもリストの上に配置し、親ディレクトリとは異なるセキュリティ設定をサブディレクトリに設定します。

［監視範囲の追加］ウィンドウ

このウィンドウでは、システム変更監視コンポーネントの監視範囲の追加や設定ができます。

監視範囲の設定

設定	説明
範囲名	監視範囲の名前を入力するフィールド。この名前は、［**監視範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品がこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、動作中にアプリケーションがこの監視範囲を制御します。 このチェックボックスをオフにすると、動作中にアプリケーションがこの監視範囲を制御しません。このチェックボックスをオンにすることにより、後からこの範囲をコンポーネント設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	監視範囲に含めるローカルディレクトリのパスを入力するフィールド。パスの指定にマスクを使用できます。このフィールドを空白のままにすることはできません。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリをスキャンします。
マスク	このリストには、動作中に製品がスキャンするオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲］ウィンドウ

この表には、システム変更監視コンポーネントの監視除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

監視除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	監視から除外されるディレクトリのパス。

ステータス	コンポーネントの動作中にアプリケーションはこの範囲が監視から除外されるかどうかを示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲の追加］ウィンドウ

このウィンドウでは、システム変更監視コンポーネントの監視除外範囲の追加や設定ができます。

監視除外範囲の設定

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、アプリケーションの実行時にこの範囲を監視から除外するかどうかを選択します。 このチェックボックスをオンにすると、コンポーネントの動作時に、アプリケーションはこの範囲を監視から除外します。 このチェックボックスをオフにすると、アプリケーションはコンポーネントの動作時にこの範囲を監視します。このチェックボックスをオンにすることにより、この範囲を監視から後で除外することができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	除外範囲に追加するローカルディレクトリのパスの入力フィールドです。パスの指定にマスクを使用できます。このフィールドを空白のままにすることはできません。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。 マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。 ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。
マスク	このリストには、監視から除外するオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、監視からのオブジェクトの除外を設定できます。指定されたマスクを含む名前のファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

管理コンソールでのシステム変更監視の設定

管理コンソールでは、ポリシーのプロパティ（**セキュリティコントロール → システム変更監視**）でシステム変更監視設定を構成できます。

システム変更監視の設定

設定	説明
システム変更監視を有効にする	このチェックボックスでは、システム変更監視を有効にするかどうかを選択します。 既定では、このチェックボックスはオフです。
監視範囲	設定のグループには、［**設定**］が含まれています。このボタンをクリックすると、［**スキャン範囲**］ウィンドウが表示されます。
監視からの除外	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**除外範囲**］ウィンドウが表示されます。
マスクによる除外	この設定グループには［**設定**］が含まれています。クリックすると、［**マスクによる除外**］ウィンドウが表示されます。

［スキャン範囲］ウィンドウ

この表には、システム変更監視コンポーネントの監視範囲が表示されます。表で指定されたパスのファイルとディレクトリが監視されます。表には既定で、1つの監視範囲［**Kaspersky の内部オブジェクト**］（/opt/kaspersky/kesl/）が表示されています。

監視範囲の設定

設定	説明
範囲名	監視範囲名。
パス	保護されるディレクトリのパス。

ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、範囲の表の並び順でスキャンされます。必要に応じて、サブディレクトリを親ディレクトリよりもリストの上に配置し、親ディレクトリとは異なるセキュリティ設定をサブディレクトリに設定します。

［<新しいスキャン範囲>］ウィンドウ

このウィンドウでは、システム変更監視コンポーネントの監視範囲の追加や設定ができます。

監視範囲の設定

設定	説明
スキャン範囲名	監視範囲の名前を入力するフィールド。この名前は、［**スキャン範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品がこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、動作中にアプリケーションがこの監視範囲を制御します。 このチェックボックスをオフにすると、動作中にアプリケーションがこの監視範囲を制御しません。このチェックボックスをオンにすることにより、後からこの範囲をコンポーネント設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	監視範囲に含めるローカルディレクトリのパスを入力するフィールド。 このフィールドを空白のままにすることはできません。既定のパスは、/opt/kaspersky/kesl です。
マスク	このリストには、動作中に製品がスキャンするオブジェクト名のマスクが含まれま

す。
既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。
マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲］ウィンドウ

この表には、システム変更監視コンポーネントの監視除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

監視除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	監視から除外されるディレクトリのパス。
ステータス	コンポーネントの動作中にアプリケーションはこの範囲が監視から除外されるかどうかを示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［<除外範囲名>］ウィンドウ

このウィンドウでは、システム変更監視コンポーネントの監視除外範囲の追加や設定ができます。

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、アプリケーションの実行時にこの範囲を監視から除外するかどうかを選択します。 このチェックボックスをオンにすると、コンポーネントの動作時に、アプリケーションはこの範囲を監視から除外します。 このチェックボックスをオフにすると、アプリケーションはコンポーネントの動作時にこの範囲を監視します。このチェックボックスをオンにすることにより、この範囲を監視から後で除外することができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	除外範囲に追加するローカルディレクトリのパスの入力フィールドです。このフィールドを空白のままにすることはできません。 「**/**」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。
マスク	このリストには、監視から除外するオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*****」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。 例： 「`*.txt`」というマスクはすべてのテキストファイルを表します。 「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の2文字で終わるHTMLファイルを表します（例：2020_my_file_09.html）。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、監視からのオブジェクトの除外を設定できます。指定されたマスクを含む名前のファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

コマンドラインからのシステム変更監視の設定

システム変更監視の事前定義済みタスク（*System_Integrity_Monitoring*）を使用してコマンドラインからリアルタイムでシステム変更監視を管理できます。タスクの種別：*OAFIM*

既定では、システム変更監視は実行されません。タスクは、手動で開始および停止できます。

システム変更監視の事前定義済みタスクの設定を編集することでシステム変更監視をデバイスから設定できます。

オンアクセスファイル変更監視タスクの設定

設定	説明	値
`UseExcludeMasks`	`ExcludeThreats.item_#` 設定で指定されたオブジェクトの監視範囲からの除外を有効にします。 この設定は、`ExcludeMasks.item_#` 設定に値が指定されている場合にのみ適用されます。	`Yes` – `ExcludeMasks.item_#` 設定で指定されたオブジェクトを監視範囲から除外します。 `No`（既定値） – `ExcludeMasks.item_#` 設定で指定されたオブジェクトを監視範囲から除外しません。
`ExcludeMasks.item_#`	名前またはマスクにより、オブジェクトを監視から除外します。この設定を使用すると、指定されたスキャン範囲から名前によって個別のファイルを除外したり、シェル形式でマスクを使用して複数のファイルを除外したりできます。 この設定の値を指定する前に、`UseExcludeMasks` 設定が有効になっていることを確認します。 複数のマスクを指定できます。各マスクは、新しいインデックスで新しい行に指定する必要があります。	既定値は定義されていません。

[ScanScope.item _#] セクションには、システム変更監視タスクの監視範囲が含まれます。タスクに対して少なくとも1つの監視範囲を指定する必要があります。複数の [ScanScope.item_#] セクションを、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。

[ScanScope.item_#] セクションには、次の設定が含まれています：

`AreaDesc`	インベントリ範囲の説明。インベントリ範囲に関する詳細情報を含みます。	既定値は定義されていません。
`UseScanArea`	指定した範囲の監視を有効にします。	`Yes`（既定値） – 指定された範囲を監視します。 `No` – 指定された範囲を監視しません。
`Path`	監視対象のディレクトリのパス。	パスの指定にマスクを使用できます。 アスタリスク記号「`*`」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「`/`」記号の前にある任意の文字数の文字列（0文字の場合を含む）を表す「`*`」記号を1つ指定することができます。例：「`/dir/*/file`」または「`/dir/*/*/file`」 2つの連続する「`*`」記号は、ファイル名またはディレクトリ名における「`/`」記号を含む任意の文字数の文字列（0文字の場合も含む）を示します。例：「`/dir/**/file*/`」または「`/dir/file**/`」 アスタリスク記号を2文字連続させた「`**`」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「`/dir/**/**/file`」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、`?` 文字を使用して任意の文字を表示できます。 既定値：/opt/kaspersky/kesl/
`AreaMask.item_#`	監視範囲の制限。監視範囲内で、シェル形式のマスクを使用して指定したファイルのみをスキャンします。	既定値：`*`（すべてのオブジェクトが監視されます）

	複数の AreaMask.item_# 項目を、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。	
[ExcludedFromScanScope.item_#] には、すべての [ScanScope.item_#] セクションから除外されるオブジェクトが含まれます。複数の [ExcludedFromScanScope.item_#] セクションを、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。 [ExcludedFromScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	監視から除外される範囲の説明。除外範囲に関する詳細情報が含まれます。	既定値は定義されていません。
UseScanArea	指定された範囲の監視の除外を指定します。	Yes（既定値） – 指定した範囲を監視から除外します。 No – 指定した範囲を監視から除外しません。
Path	監視から除外されるオブジェクトがあるディレクトリのパス。	パスの指定にマスクを使用できます。 アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 既定値は定義されていません。
AreaMask.item_#	監視の除外範囲の制限。監視の除外範囲で、シェル形式のマスクを使用して指定	既定値：*（すべてのオブジェクトを監視から除外）

	したオブジェクトのみを除外します。 複数の `AreaMask.item_#` 項目を、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。	

システム整合性チェック

*システム整合性チェック*のタスクが実行されている間、監視対象オブジェクトの現在の状態と元の状態を比較することにより、各オブジェクトの変更が検出されます。次の比較基準を用いることができます：

- ファイルハッシュ
- ファイル変更時間
- ファイルサイズ

監視対象オブジェクトの初期状態は、*ベースライン*として記録されます。ベースラインには、監視対象オブジェクトとそのメタデータへのパスが含まれます。

ベースラインには個人データが含まれる場合もあります。

システムのベースラインは、システム整合性チェックのタスクがデバイス上で初めて実行されたときに作成されます。複数のシステム整合性チェックのタスクを作成すると、それぞれに個別のベースラインが作成されます。タスクは、ベースラインがタスクに定義された監視範囲に属するオブジェクトに関する情報を含んでいる場合にのみ実行されます。ベースラインが監視範囲に一致しない場合、Kaspersky Endpoint Security はシステム変更違反のイベントを生成します。

タスクの設定が変更された時（新しい監視範囲が追加された時など）に、ベースラインを再構築します。

アプリケーションは、保護されたデバイス上にベースライン保管領域を作成します。既定では、ベースラインの保管領域は /var/opt/kaspersky/kesl/private/fim.db にあります。ベースラインを含むデータベースにアクセスするには、root 権限が必要です。

ベースラインを削除するには、該当するシステム整合性チェックのタスクを削除します。

オンデマンドでシステムの整合性チェックを実行し、スキャン設定を構成できます：

- システム整合性チェックのタスクが終了するたびに、ベースラインの再構築を有効または無効にします。
- 監視対象ファイルの現在の状態と元の状態を比較する基準として、ファイルハッシュと変更時間を使用するか、ファイルサイズのみを使用するかを選択します。
- システムの整合性をチェックするための監視範囲を設定します。
- システム変更チェックからの除外範囲を設定します。除外するファイルやディレクトリへのパスを指定したり、ネームマスクによって個々のオブジェクトを除外することができます。

Web コンソールでのシステム整合性チェックの設定

*システム整合性チェック*のタスクを使用してWeb Console でシステムの整合性チェックを実行できます。

ユーザーシステム整合性チェックのタスクを作成して実行できます。タスクの設定を編集してスキャン設定を管理できます。

システム整合性チェックのタスク設定

設定	説明
タスクを開始するたびにベースラインを再構築する	このチェックボックスは、*システム整合性チェック*タスクを開始するたびに、システムのベースラインを再確立するかどうかを選択します。 既定では、このチェックボックスはオフです。
SHA256 hash を確認する	このチェックボックスは、ファイルの現在の状態と元の状態を比較する際の基準として、ファイルハッシュを使用するかどうかを設定します。 このチェックをオフにした場合、製品はファイルサイズのみを比較します（ファイサイズが変更されていない場合、変更時間は重要なパラメータとは判断されません）。 既定では、このチェックボックスはオフです。
監視範囲にあるディレクトリを監視する	このチェックボックスは、システム整合性チェックの実行中にディレクトリ監視を使用するかどうかを設定します。 既定では、このチェックボックスはオフです。
ファイルの最終アクセス日時を監視する	このチェックボックスでは、システム変更監視の実行中にファイルアクセス時間を追跡するかどうかを設定します。 既定では、このチェックボックスはオフです。
監視範囲	タスクによってスキャンされた監視範囲を示す表。 表には既定で、**Kaspersky の内部オブジェクト**の監視範囲（/opt/kaspersky/kesl/）が表示されています。 表内では監視範囲に対して次の操作ができます：追加、設定、削除、上に移動、下に移動。 ［**下へ**］をクリックすると、表内で選択した項目が下に移動します。 指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。 このボタンは、1つの範囲を表から選択している場合に使用できます。 ［**上へ**］をクリックすると、表内で選択した項目が上に移動します。 指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。 このボタンは、1つの範囲を表から選択している場合に使用できます。 ［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。 このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

スキャン範囲名をクリックすると、［**<スキャン範囲>**］ウィンドウが表示されます。このウィンドウでは、選択したスキャン範囲の設定を編集できます。

［**追加**］をクリックすると、［**<新しいスキャン範囲>**］ウィンドウが表示されます。このウィンドウでは、新しいスキャン範囲を指定できます。

［スキャン範囲の追加］ウィンドウ

このウィンドウでは、システム整合性チェックタスクの監視範囲の追加や設定ができます。

監視範囲の設定

設定	説明
範囲名	監視範囲の名前を入力するフィールド。この名前は、**スキャン設定**セクションの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品がこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、動作中にアプリケーションがこの監視範囲を制御します。 このチェックボックスをオフにすると、動作中にアプリケーションがこの監視範囲を制御しません。このチェックボックスをオンにすることにより、後からこの範囲をコンポーネント設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	監視範囲に含めるローカルディレクトリのパスを入力するフィールド。パスの指定にマスクを使用できます。 アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 このフィールドを空白のままにすることはできません。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリをスキャンします。

マスク	このリストには、動作中に製品がスキャンするオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲］セクション

除外範囲セクションでは、システム整合性チェックタスクの除外範囲やマスクによる除外を設定することもできます。

［除外範囲］ウィンドウ

この表には、システム整合性チェックの監視除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

監視除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	監視から除外されるディレクトリのパス。
ステータス	タスクの動作中にアプリケーションはこの範囲が監視から除外されるかどうかを示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲の追加］ウィンドウ

このウィンドウでは、システム整合性チェックタスクの監視除外範囲の追加や設定ができます。

監視除外範囲の設定

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、アプリケーションの実行時にこの範囲を監視から除外するかどうかを選択します。 このチェックボックスをオンにすると、タスクの動作時に、アプリケーションはこの範囲を監視から除外します。 このチェックボックスをオフにすると、アプリケーションはタスクの動作時にこの範囲を監視します。このチェックボックスをオンにすることにより、この範囲を監視から後で除外することができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	除外範囲に追加するローカルディレクトリのパスの入力フィールドです。パスの指定にマスクを使用できます。 アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 このフィールドを空白のままにすることはできません。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。
マスク	このリストには、監視から除外するオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、監視からのオブジェクトの除外を設定できます。指定されたマスクを含む名前のファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

管理コンソールでのシステム整合性チェックの設定

*システム整合性チェック*のタスクを使用して管理コンソールでシステムの整合性チェックを実行できます。

ユーザーシステム整合性チェックのタスクを作成して実行できます。タスクの設定を編集してスキャン設定を管理できます。

［システム変更チェック］タスクのプロパティの［**設定**］セクションでは、次の表に示す設定を編集できます。

システム整合性チェックのタスク設定

設定	説明
タスクを開始するたびにベースラインを再構築する	このチェックボックスは、システム整合性チェックタスクを開始するたびに、システムのベースラインを再確立するかどうかを選択します。 既定では、このチェックボックスはオフです。
SHA256 hash を確認する	このチェックボックスは、ファイルの現在の状態と元の状態を比較する際の基準として、ファイルハッシュを使用するかどうかを設定します。 このチェックをオフにした場合、製品はファイルサイズのみを比較します（ファイサイズが変更されていない場合、変更時間は重要なパラメータとは判断されません）。 既定では、このチェックボックスはオフです。
監視範囲にあるディレクトリを監視する	このチェックボックスは、システムの整合性チェック中に指定した監視範囲内のディレクトリのスキャンを有効または無効にします。 既定では、このチェックボックスはオフです。
ファイルの最終アクセス日時を監視する	このチェックボックスでは、システム変更監視の実行中にファイルアクセス時間を追跡するかどうかを設定します。 既定では、このチェックボックスはオフです。
監視範囲	設定のグループには、［**設定**］が含まれています。このボタンをクリックすると、［**スキャン範囲**］ウィンドウが表示されます。

システム整合性チェックのプロパティの**除外範囲**で、監視除外とマスクによる除外を定義できます。

［スキャン範囲］ウィンドウ

この表には、システム整合性チェックタスクの監視範囲が表示されます。表で指定されたパスのファイルとディレクトリが監視されます。表には既定で、1つの監視範囲［**Kaspersky の内部オブジェクト**］（/opt/kaspersky/kesl/）が表示されています。

監視範囲の設定

設定	説明
範囲名	監視範囲名。
パス	保護されるディレクトリのパス。
ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：追加、編集、削除、上に移動、下に移動。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

このボタンは、1つの項目のみを表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、範囲の表の並び順でスキャンされます。必要に応じて、サブディレクトリを親ディレクトリよりもリストの上に配置し、親ディレクトリとは異なるセキュリティ設定をサブディレクトリに設定します。

［<新しいスキャン範囲>］ウィンドウ

このウィンドウでは、システム整合性チェックタスクの監視範囲の追加や設定ができます。

監視範囲の設定

設定	説明
スキャン範囲名	監視範囲の名前を入力するフィールド。この名前は、［**スキャン範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品がこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、動作中にアプリケーションがこの監視範囲を制御します。 このチェックボックスをオフにすると、動作中にアプリケーションがこの監視範囲を制御しません。このチェックボックスをオンにすることにより、後からこの範囲をコンポーネント設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	監視範囲に含めるローカルディレクトリのパスを入力するフィールド。パスの指定にマスクを使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 このフィールドを空白のままにすることはできません。 既定のパスは、/opt/kaspersky/kesl です。
マスク	このリストには、動作中に製品がスキャンするオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［除外範囲］セクション

スキャンの除外の設定

設定のグループ	説明
監視からの除外	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**除外範囲**］ウィンドウが表示されます。このウィンドウでは、監視から除外する範囲のリストを指定できます。

マスクによる除外	この設定グループには［**設定**］が含まれています。クリックすると、［**マスクによる除外**］ウィンドウが表示されます。このウィンドウでは、名前のマスクにより、監視からのオブジェクトの除外を設定できます。

［除外範囲］ウィンドウ

この表には、システム整合性チェックの監視除外範囲が表示されます。表で指定されたパスのファイルとディレクトリはスキャンされません。既定では、この表は空です。

システム整合性チェックタスクの監視除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	スキャンから除外されるディレクトリのパス。
ステータス	コンポーネントの動作中にアプリケーションはこの範囲が監視から除外されるかどうかを示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

［<新しい除外範囲>］ウィンドウ

このウィンドウでは、システム整合性チェックタスクの監視除外範囲の追加や設定ができます。

監視除外範囲の設定

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、アプリケーションの実行時にこの範囲を監視から除外するかどうかを選択します。 このチェックボックスをオンにすると、タスクの動作時に、アプリケーションはこの範囲を監視から除外します。 このチェックボックスをオフにすると、アプリケーションはタスクの動作時にこの範囲を監視します。このチェックボックスをオンにすることにより、この範囲を監視から後で除外することができます。

	既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	除外範囲に追加するローカルディレクトリのパスの入力フィールドです。パスの指定にマスクを使用できます。 アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 このフィールドを空白のままにすることはできません。 「/」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。
マスク	このリストには、監視から除外するオブジェクト名のマスクが含まれます。 既定では、すべてのオブジェクトを示すマスク「*」がリストに含まれています。 マスクは、追加、編集、削除できます。 ［**削除**］をクリックすると、選択した項目が表から削除されます。 このボタンは、少なくとも 1 つの項目を表から選択している場合に使用できます。 選択した要素の設定が、別のウィンドウで変更されます。 ［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。 例： 「*.txt」というマスクはすべてのテキストファイルを表します。 「*_my_file_??.html」というマスクは、任意の文字列から始まって、ファイル名の末尾が「_my_file_」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

［マスクによる除外］ウィンドウ

名前のマスクに基づいて、監視からのオブジェクトの除外を設定できます。指定されたマスクを含む名前のファイルはスキャンされません。既定では、マスクのリストは空です。

マスクは、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、［**オブジェクトマスク**］ウィンドウが表示されます。このウィンドウの［**オブジェクトマスクを設定する**］フィールドで、スキャンから除外されるファイル名のテンプレートを指定できます。

例：
「`*.txt`」というマスクはすべてのテキストファイルを表します。
「`*_my_file_??.html`」というマスクは、任意の文字列から始まって、ファイル名の末尾が「`_my_file_`」と任意の 2 文字で終わる HTML ファイルを表します（例：2020_my_file_09.html）。

コマンドラインでのシステム整合性チェックの設定

ユーザー *システム整合性チェック*のタスク（*ODFIM* タスク）を使用して、コマンドラインでデバイスのシステム整合性チェックを実行できます。

ユーザータスクを手動で開始、停止、一時停止、再開し、タスクのスケジュールを設定できます。これらのタスクの設定を編集することで、システム整合性チェックを設定できます。

システム整合性チェックのタスク設定

設定	説明	値
`RebuildBaseline`	*システム整合性チェック*タスクの終了後にベースラインを再構築できるようにします。	`Yes`：*システム整合性チェック*タスクが終了するたびにベースラインを再構築します。 `No`（既定）：*システム整合性チェック*タスクが終了するたびにベースラインを再構築しません。
`CheckFileHash`	監視対象ファイルの現在の状態と元の状態を比較する際の基準として、ファイルハッシュ（SHA256）を使用します。	`Yes`：ハッシュをチェックします。

		No（既定値）– ハッシュチェックを無効にします。このチェックを無効にした場合、アプリケーションはファイルサイズのみを比較します（ファイルサイズが変更されていない場合、変更時間は重要なパラメータとは判断されません）。
TrackDirectoryChanges	ディレクトリの監視を有効にします。	Yes：システムの整合性をチェックしている間にディレクトリを監視します。 No（既定値）– ディレクトリを監視しません。
TrackLastAccessTime	ファイルの最終アクセス日時の追跡を有効にします。Linux オペレーティングシステムでは、 noatime 設定です。	Yes – 最後にファイルへアクセスした日時を追跡します。 No（既定値）– 最後にファイルへアクセスした日時を追跡しません。
UseExcludeMasks	ExcludeMasks.item_# 設定で指定されたオブジェクトの監視範囲からの除外を有効にします。 この設定は、ExcludeMasks.item_# 設定に値が指定されている場合にのみ適用されます。	Yes – ExcludeMasks.item_# 設定で指定されたオブジェクトを監視範囲から除外します。 No（既定値）– ExcludeMasks.item_# 設定で指定されたオブジェクトを監視範囲から除外しません。
ExcludeMasks.item_#	名前またはマスクにより、オブジェクトを監視から除外します。この設定を使用すると、指定されたスキャン範囲から名前によって個別のファイルを除外したり、シェル形式でマスクを使用して複数のファイルを除外したりできます。 この設定の値を指定する前に、UseExcludeMasks 設定が有効になっていることを確認します。 複数のマスクを指定できます。各マスクは、新しいインデックスで新しい行に指定する必要があります。	既定値は定義されていません。
[ScanScope.item _#] セクションには、 *システム整合性チェック*の監視範囲が含まれます。タスクに対して少なくとも 1 つの監視範囲を指定する必要があります。複数の [ScanScope.item_#] セクションを、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。 [ScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	インベントリ範囲の説明。インベントリ範囲に関する詳細情報を含みます。	既定値は定義されていません。
UseScanArea	指定した範囲の監視を有効にします。	Yes（既定値）– 指定された範囲を監視します。 No – 指定された範囲を監視しません。
Path	監視対象のディレクトリのパス。	パスの指定にマスクを使用できます。

		アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 既定値：/opt/kaspersky/kesl/
AreaMask.item_#	監視範囲の制限。監視範囲内で、シェル形式のマスクを使用して指定したファイルのみをスキャンします。 複数の AreaMask.item_# 項目を、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。	既定値：*（すべてのオブジェクトが監視されます）
[ExcludedFromScanScope.item_#] セクションには、すべての [ScanScope.item_#] セクションから除外されるオブジェクトが含まれます。複数の [ExcludedFromScanScope.item_#] セクションを、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。 [ExcludedFromScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	監視から除外される範囲の説明。除外範囲に関する詳細情報が含まれます。	既定値は定義されていません。
UseScanArea	指定された範囲の監視の除外を指定します。	Yes（既定値） – 指定した範囲を監視から除外します。 No – 指定した範囲を監視から除外しません。
Path	監視から除外されるオブジェクトがあるディレクトリのパス。	パスの指定にマスクを使用できます。

		アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 既定値は定義されていません。
AreaMask.item_#	監視の除外範囲の制限。監視の除外範囲で、シェル形式のマスクを使用して指定したオブジェクトのみを除外します。 複数の AreaMask.item_# 項目を、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。	既定値：*（すべてのオブジェクトを監視から除外）

ふるまい検知

ふるまい検知 コンポーネントは、オペレーティングシステム内のアプリケーションからの悪意のあるアクティビティを監視できます。悪意のある動作を検知した時、Kaspersky Endpoint Security はその動作を実行しているアプリケーションのプロセスを終了させることができます。

この機能は、KESL コンテナではサポートされていません。

ふるまい検知コンポーネントは、Kaspersky Endpoint Security の起動時に既定で自動的に有効になります。

ふるまい検知を有効、無効、および設定できます：

- オペレーティングシステムで悪意のあるアクティビティを検知したときに Kaspersky Endpoint Security によって実行される処理を選択します。ユーザーに通知するか、悪意のあるアクティビティを実行するアプリケーションをブロックします。
- プロセスアクティビティをスキャンから除外します。

Kaspersky Endpoint Security と Kaspersky Managed Detection and Response の連携が有効になっている場合、オペレーティングシステムでアプリケーションの動作を検知するときに、プロセスによる除外がスキップされます。

既定では、SintezM-Client オペレーティングシステムでは、auditd サービスの設定は変更から保護されており、`enabled 2` モードになっています。Kaspersky Endpoint Security は、Kaspersky Managed Detection and Response および Kaspersky Anti Targeted Attack Platform ソリューションと連携されてい場合に、ふるまい検知コンポーネントを正しく動作させるためには、設定情報ファイルの auditd モードを `enabled 1`（設定ブロックなし）に変更し、オペレーティングシステムを再起動します。

Web コンソールでのふるまい検知の設定

Web コンソールでは、ポリシーのプロパティ（**製品設定 → 先進の脅威対策 → ふるまい検知**）でふるまい検知設定を構成できます。

ふるまい検知の設定

設定	説明
ふるまい検知の有効化 / 無効化	この切り替えボタンでは、ふるまい検知を有効にするかどうかを選択します。 この切り替えボタンは既定でオンになっています。
マルウェアの動作検出時の処理	オペレーティングシステムにおける悪意のある動作を検知した際に、Kaspersky Endpoint Security が実行するアクションです。 • ユーザーに**通知**します。Kaspersky Endpoint Security は、悪意のある動作を実行しているプロセスを終了させません。悪意のある動作を検知したことを、イベントログへ記録することのみ行います。 • 悪意のある動作（既定値）を実行するアプリケーションを**ブロック**する。Kaspersky Endpoint Security は、悪意のある動作を実行するプロセスを終了させ、検知された悪意のある動作に関する情報をログに記録します。

プロセスによる除外	［**除外をプロセスで設定する**］をクリックすると、［**プロセスによる除外**］ウィンドウが表示されます。このウィンドウで、プロセスの動作を除外できます。

［プロセスによる除外］ウィンドウ

表には、プロセスによる除外の範囲が含まれています。プロセスによる除外の範囲では、指定されたプロセスの動作と、指定されたプロセスによって変更されたファイルを除外できます。既定では、この表は空です。

Kaspersky Endpoint Security と Kaspersky Managed Detection and Response の統合が有効になっている場合、プロセスによる除外は適用されません。

プロセスによる除外範囲の設定

設定	説明
信頼できるプロセスをスキャンから除外する / 除外しない	このスイッチは、ふるまい検知の動作で、設定したプロセスによる除外を有効または無効にします。 この切り替えボタンは既定でオフになっています。
除外範囲名	除外範囲名。
パス	除外されるプロセスの絶対パス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

また、［**インポート**］をクリックしてファイルから除外リストをインポートすることも、［**エクスポート**］をクリックして追加した除外リストをファイルにエクスポートすることもできます。インポート時に、除外リストを置き換えるか、既存のリストに除外リストを追加するかを尋ねるメッセージが表示されます。

［プロセスの除外範囲の追加］ウィンドウ

このウィンドウでは、プロセスによる除外範囲の追加や設定ができます。

除外範囲の設定

設定	説明
プロセスベースの除外範囲名	プロセスベースの除外範囲名を入力するフィールド。この名前は、［**プロセスによる除外**］ウィンドウの表に表示されます。 この入力フィールドを空白のままにすることはできません。
この除外を使用する	このチェックボックスでは、製品の実行時にこのスキャン範囲除外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。
除外する	スキャンから除外するプロセスへの絶対パスです。パスの指定にマスクを使用できます。

プロセスのパス	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 この入力フィールドを空白のままにすることはできません。
子プロセスへ適用する	［**除外するプロセスのパス**］設定で指定した、除外されるプロセスの子プロセスを除外します。 既定では、このチェックボックスはオフです。

管理コンソールでのふるまい検知の設定

管理コンソールでは、ポリシーのプロパティ（**先進の脅威対策 → ふるまい検知**）でふるまい検知設定を構成できます。

ふるまい検知の設定

設定	説明
ふるまい検知を有効にする	このチェックボックスでは、ふるまい検知を有効にするかどうかを選択します。 既定では、このチェックボックスはオンです。
マルウェア活動検知のアクション	オペレーティングシステムにおける悪意のある動作を検知した際に、Kaspersky Endpoint Security が実行するアクションです。 • 悪意のある動作（既定値）を実行するアプリケーションを**ブロック**する。Kaspersky Endpoint Security は、悪意のある動作を実行するプロセスを終了させ、検知された悪意のある動作に関する情報をログに記録します。 • ユーザーに**通知**します。Kaspersky Endpoint Security は、悪意のある動作を実行しているプロセスを終了させません。悪意のある動作を検知したことを、イベントログへ記録することのみ行います。
プロセスによる除外を使用する	このチェックボックスは、ふるまい検知の操作で、プロセスによる除外を有効または無効にします。 既定では、このチェックボックスはオフです。 ［**設定**］をクリックすると、［**プロセスによる除外**］ウィンドウが表示されます。このウィンドウで、プロセスの動作を除外できます。

［プロセスによる除外］ウィンドウ

表には、プロセスによる除外の範囲が含まれています。プロセスによる除外の範囲では、指定されたプロセスの動作を除外できます。既定では、この表は空です。

Kaspersky Endpoint Security と Kaspersky Managed Detection and Response の統合が有効になっている場合、プロセスによる除外は適用されません。

プロセスによる除外範囲の設定

設定	説明
除外範囲名	除外範囲名。
パス	除外されるプロセスの絶対パス。
ステータス	この除外が使用されるかどうかをステータスに示します。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

また、［**詳細設定**］->［**インポート**］をクリックしてファイルから除外リストをインポートしたり、［**詳細設定**］->［**選択項目をエクスポート**］または［**詳細設定**］->［**すべてエクスポート**］をクリックして追加した除外リストをファイルにエクスポートすることもできます。インポート時に、除外リストを置き換えるか、既存のリストに除外リストを追加するかを尋ねるメッセージが表示されます。

［信頼するプロセス］ウィンドウ

このウィンドウでは、プロセスによる除外範囲の追加や設定ができます。

プロセスによる除外範囲の設定

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**プロセスによる除外**］ウィンドウの表に表示されます。
除外するプロセスのパス	スキャンから除外するプロセスへの絶対パスです。パスの指定にマスクを使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。 この入力フィールドを空白のままにすることはできません。
子プロセスへ適用する	［**除外するプロセスのパス**］設定で指定した、除外されるプロセスの子プロセスを除外します。 既定では、このチェックボックスはオフです。
この範囲を使用する	このチェックボックスでは、この除外範囲をオンまたはオフにします。 このチェックボックスをオンにすると、この範囲が除外されます。 このチェックボックスをオフにすると、この範囲が含まれます。このチェックボックスをオンにすることにより、後からこの範囲を除外することができます。 既定では、このチェックボックスはオンです。

コマンドラインでのふるまい検知の設定

Behavior_Detection の事前定義済みタスクを使用することで、コマンドライン経由でオペレーティングシステムのアプリケーション Behavior Detection を管理できます。

ふるまい検知は既定で実行します。タスクは、手動で開始および停止できます。

ふるまい検知の事前定義済みタスクの設定を編集することで、ふるまい検知を設定できます。

ふるまい検知タスクの設定

設定	説明	値
TaskMode	悪意のある活動がオペレーティングシステムで検知された時に実行される処理。	Block（既定値） – 悪意のある活動を実行中のアプリケーションのプロセスを終了します。 Notify – 悪意のある活動を実行するプロセスを終了しません。悪意のある活動の検知の、イベントログへの記録のみ実行します。
UseTrustedPrograms	プロセスをスキャンから除外します。	Yes – 指定されたプロセスの動作をスキャンしません。 No（既定値） – すべての Web サイトをスキャンします。

[TrustedPrograms.item_#] セクションには、スキャンから除外されたプロセスが含まれます。Kaspersky Endpoint Security は、指定したプロセスの活動を監視しません。

`ProgramPath`	除外するプロセスのパス。	< プロセスへの絶対パス > - 指定されたローカルディレクトリ内のプロセスはスキャンされません。パスの指定にマスクを使用できます。 アスタリスク記号「`*`」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「`/`」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「`*`」記号を 1つ指定することができます。例：「`/dir/*/file`」または「`/dir/*/*/file`」 2 つの連続する「`*`」記号は、ファイル名またはディレクトリ名における「`/`」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「`/dir/**/file*/`」または「`/dir/file**/`」 アスタリスク記号を 2 文字連続させた「`**`」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「`/dir/**/**/file`」は不適切なマスク表現となります。 ファイル名またはディレクトリ名には、`?` 文字を使用して任意の文字を表示できます。
`ApplyToDescendants`	`ProgramPath` 設定で指定された除外対象プロセスの子プロセスをスキャンから除外します。	`Yes` – 指定したプロセスとそのすべての子プロセスをスキャンから除外します。 `No`（既定値） - 指定したプロセスのみをスキャンから除外し、子プロセスはスキャンから除外しません。
`ProgramDesc`	除外されるプロセスの説明。	
`UseTrustedProgram`	指定されたプロセスをスキャンから除外できるようにします。	`Yes`（既定値）– 指定されたプロセスをスキャンから除外します。 `No` – 指定したプロセスをスキャンから除外しません。

Kaspersky Security Network を使用する

米国領土では、貿易制限に従い、2024 年 9 月 10 日東部夏時間（EDT）午前 12 時以降、KSN 機能がアプリケーションで利用できなくなります。

Kaspersky Endpoint Security は、デバイスとユーザーデータの保護を強化するために、Kasperskyのクラウド型ナレッジベース Kaspersky Security Network（KSN）を使用して、ファイル、インターネットリソース、ソフトウェアのレピュテーションをチェックできます。Kaspersky Security Network のデータを使用することで、様々な脅威への迅速な対応、保護コンポーネントの高い性能、誤検知の減少を実現しています。

Kaspersky Security Network の使用は任意です。KSN の使用はいつでも開始または停止ができます。

KSN 機能は、KESL コンテナではサポートされていません。

Kaspersky Security Network インフラストラクチャソリューション

Kaspersky Endpoint Security は、Kasperskyのレピュテーションデータベースと連携するために、次のインフラストラクチャーソリューションをサポートしています：

- *Kaspersky Security Network (KSN)* - Kasperskyから情報を受け取り、ユーザーデバイスで検知されたオブジェクトのデータを、Kasperskyのアナリストによる追加検証を受けるために Kasperskyに送信したり、レピュテーションデータベースや統計情報データベースに追加したりするソリューションです。

- *Kaspersky Private Security Network (KPSN)* - Kaspersky Endpoint Security 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にデータを送信することなく、Kasperskyのレピュテーションデータベースや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。KPSN は、次のような理由で Kaspersky Security Network を利用できない法人のお客様向けに設計されています：

  - 現地の職場がインターネットに接続されていない

  - 国外または組織のローカルネットワーク外にデータを送信することが法律上禁止されている、または企業のセキュリティ上制限されています

新しいアプリケーションライセンスを有効化した後に KPSN を使用するには、サービスプロバイダーに新しいライセンスを通知します。そうしない場合は、認証エラーにより KPSN とのデータ交換ができなくなります。

Kaspersky Security Network の使用オプション：

KSN を利用するには、2 つの選択肢があります：

- **拡張 KSN モード** - Kasperskyのナレッジベースから情報を受け取ることができ、Kaspersky Endpoint Security は動作中に取得した統計情報を自動的に Kaspersky Security Network に送信します。また、本製品は、侵入者がデバイスやデータに損害を与えるために使用する可能性がある特定のファイル（またはファイルの一部）を詳細にスキャンするためにカスペルスキーへ送信することもできます。

- **標準 KSN モード** - Kasperskyナレッジベースからの情報を受信できますが、Kaspersky Endpoint Security から脅威の種別や発生源に関する統計や情報を匿名で送信されません。

別の Kaspersky Security Network の使用オプションをいつでも選択できます。

個人情報の収集、処理、保存は行われません。KSN への参加中に生成された統計情報の保存や破棄、さらにカスペルスキーへの送信に関する詳細情報は、Kaspersky Security Network に関する声明およびカスペルスキーの Web サイトで確認できます。Kaspersky Security Network に関する声明が記載されているファイルは、製品の配布キットに含まれています。

Kaspersky Endpoint Security のクラウドモード

*クラウドモード*は、マルウェアデータベースの軽量バージョンを使用する Kaspersky Endpoint Security の操作モードです。これにより、デバイスのメモリ負荷を軽減できます。

Kaspersky Security Network により、アプリケーションによる軽量のマルウェアデータベースの使用が容易になります。

Kaspersky Endpoint Security が標準モードで実行されており、KSN を使用している場合は、クラウド モードを有効にすることができます。

Kaspersky Endpoint Security が仮想環境を保護するために Light Agent モードで実行されている場合、軽量のマルウェア対策データベースはサポートされません。アプリケーションは、Light Agent の動作に必要な特別なデータベースを保護サーバーから受け取ります。

Kaspersky Endpoint Security は、クラウドモードを有効にし、アプリケーションデータベースとモジュールの最新のアップデートを実行した後、マルウェアデータベースの軽量バージョンの使用に切り替えます。クラウドモードが無効になっている場合、Kaspersky Endpoint Security は、定義データベースとモジュールの次回のアップデート時に、カスペルスキーのサーバーから定義データベースとモジュールのフルバージョンをダウンロードします。

KSN を使用していない場合、またはクラウドモードが無効になっている場合、Kaspersky Endpoint Security は定義データベースのフルバージョンを使用します。

KSN の使用が無効になっている場合、クラウドモードは自動的に無効になります。

KSN プロキシサービスの使用

管理サーバーによって管理されるユーザーデバイスは、KSN と直接通信することも、KSN プロキシサービスを介して通信することもできます。

Kaspersky Endpoint Security を仮想環境保護用に Light Agent モードで使用する場合、KSN プロキシサービスは KSN インフラストラクチャとの通信に対応しています。KSN との直接通信には対応していません。KSN プロキシが使用できない場合、アプリケーションは KSN を使用しません。

KSN プロキシサーバーは、次の機能を提供します：

- ユーザーのデバイスがインターネットに直接アクセスしていない場合でも、KSN に照会したり情報を KSN に送信したりできます。
- KSN プロキシサーバーは処理されたデータをキャッシュするため、外部ネットワークへの接続の負荷を軽減し、ユーザーのデバイスから要求される情報の取得を高速化します。

KSN プロキシサーバー設定は、管理サーバーのプロパティで設定できます。KSN プロキシサーバーの詳細は、『Kaspersky Security Center のヘルプ』を参照してください。

Web コンソールでの Kaspersky Security Network の使用を設定します。

Web コンソールでは、ポリシーのプロパティ（**製品設定 → 先進の脅威対策 → Kaspersky Security Network**）でKaspersky Endpoint Security の Kaspersky Security Network の使用を設定できます。

「**Kaspersky Security Network に関する声明**」の本文は、［**Kaspersky Security Network に関する声明**］をクリックして表示される［Kaspersky Security Network に関する声明］ウィンドウで読むことができます。

Kaspersky Security Center は、［*アセット（デバイス）*］タブの管理対象デバイスのリストにあるクライアントデバイスのステータス（**OK、緊急、警告**）により KSN の可用性に関する情報を表示します。

Kaspersky Security Network の設定

設定	説明
KSN を使用しない	このオプションをオンにすることにより、Kaspersky Security Network の使用を拒否します。
拡張 KSN モード	このオプションをオンにすることにより、Kaspersky Security Network の利用規約に同意したことになります。Kasperskyのナレッジベースから、ファイル、Web リソース、ソフトウェアの評価情報を取得できるようになります。また、匿名化された統計情報と様々な脅威の種別と発生源に関する情報がカスペルスキーに送信され、Kaspersky Security Network の改善に役立てられます。
基本 KSN モード	このオプションをオンにすることにより、Kaspersky Security Network の利用規約に同意したことになります。Kasperskyのナレッジベースから、ファイル、Web リソース、ソフトウェアの評価情報を取得できるようになります。
クラウドモードを有効にする	このチェックボックスは、Kaspersky Endpoint Security が軽量バージョンのマルウェアデータベースを使用する操作モードを有効または無効にします。 KSN の使用が有効な場合、チェックボックスが使用可能になります。 ポリシーの作成時に Kaspersky Security Network に関する声明の条項に同意し、拡張 KSN モードで使用している場合は、このチェックボックスがオンになります。 このモードは、次回の定義データベースのアップデート後に有効または無効になります。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。
KSN プロキシが使用できない場合、KSN サーバーを使用する	このチェックボックスは、KSN プロキシサービスが使用できない場合に KSN サーバーと直接通信する機能を有効または無効にします。 既定では、このチェックボックスはオンです。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。
Kaspersky Security Network に関する声明	このリンクをクリックすると、［**Kaspersky Security Network に関する声明**］ウィンドウが開き、Kaspersky Security Network に関する声明の本文を読むことができます。

Kaspersky Security Network に関する声明

このウィンドウでは、Kaspersky Security Network に関する声明の本文を読み、条項に同意します。

Kaspersky Security Network の設定

設定	説明
Kaspersky Security Network に関する声明をすべて確認し、理解した上で条項に同意する	このオプションをオンにすることにより、Kaspersky Security Network を使用することを確認し、表示される Kaspersky Security Network に関する声明をすべて確認し、理解した上で条項に同意します。
Kaspersky Security Network に関する声明の条項に同意しない	このオプションをオンにすることにより、Kaspersky Security Network を使用しないことを確定します。

Kaspersky Private Security Network に関する声明

このウィンドウでは、Kaspersky Security Network に関する声明の本文を読み、条項に同意します。

Kaspersky Security Network の設定

設定	説明
Kaspersky Security Network に関する声明をすべて確認し、理解した上で条項に同意する	このオプションをオンにすることにより、Kaspersky Security Network に参加することを確認し、表示される Kaspersky Private Security Network に関する声明をすべて確認し、理解した上で条項に同意します。
Kaspersky Security Network に関する声明の条項に同意しない	このオプションをオンにすることにより、Kaspersky Security Network を使用しないことを確定します。

管理コンソールでの Kaspersky Security Network の使用を設定します。

管理コンソールでは、ポリシーのプロパティ（**先進の脅威対策 → Kaspersky Security Network**）でKaspersky Endpoint Security の Kaspersky Security Network の使用を設定できます。

「**Kaspersky Security Network に関する声明**」の本文は、［**Kaspersky Security Network に関する声明**］をクリックして表示される［Kaspersky Security Network に関する声明］ウィンドウで読むことができます。

Kaspersky Security Center は、［**デバイス**］タブの管理対象デバイスのリストにあるクライアントデバイスのステータス（*OK*、*緊急*、*警告*）により KSN の可用性に関する情報を表示します。

Kaspersky Security Network の設定

設定	説明
Kaspersky Security Network に関する声明	クリックすると、［**Kaspersky Security Network に関する声明**］ウィンドウが表示されます。このウィンドウでは、Kaspersky Security Network に関する声明を読むことができます。
Kaspersky Security Network（KSN）	このブロックは、KSN モードに関する情報を表示するか、KSN が Kaspersky Endpoint Security で使用されていないことを示します。

	［**編集**］をクリックすると、Kaspersky Security Network の使用を設定できるウィンドウが開きます。
クラウドモードを有効にする	このチェックボックスは、Kaspersky Endpoint Security が軽量バージョンのマルウェアデータベースを使用する操作モードを有効または無効にします。 KSN の使用が有効な場合、チェックボックスが使用可能になります。 ポリシーの作成時に Kaspersky Security Network に関する声明の条項に同意し、拡張 KSN モードで使用している場合は、このチェックボックスがオンになります。 このモードは、次回の定義データベースのアップデート後に有効または無効になります。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。
KSN プロキシが使用できない場合、KSN サーバーを使用する	このチェックボックスは、KSN プロキシサービスが使用できない場合に KSN サーバーと直接通信する機能を有効または無効にします。 既定では、このチェックボックスはオンです。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。

Kaspersky Security Network の設定

このウィンドウでは、Kaspersky Security Network の参加を設定できます。

Kaspersky Security Network の設定

設定	説明
詳細...	このリンクをクリックすると、カスペルスキーの Web サイトが開きます。
Kaspersky Security Network を使用しない	このオプションをオンにすることにより、Kaspersky Security Network の使用を拒否します。
基本 KSN モード	このオプションをオンにすることにより、Kaspersky Security Network の利用規約に同意したことになります。Kasperskyのナレッジベースから、ファイル、Web リソース、ソフトウェアの評価情報を取得できるようになります。
拡張 KSN モード	このオプションをオンにすることにより、Kaspersky Security Network の利用規約に同意したことになります。Kasperskyのナレッジベースから、ファイル、Web リソース、ソフトウェアの評価情報を取得できるようになります。また、匿名化された統計情報と様々な脅威の種別と発生源に関する情報がカスペルスキーに送信され、Kaspersky Security Network の改善に役立てられます。
Kaspersky Security Network	このリンクをクリックすると、［**Kaspersky Security Network に関する声明**］**ウィンドウが開き、**Kaspersky Security Network に関する声明の本文を読むことができます。

に関する声明	

Kaspersky Security Network に関する声明

このウィンドウでは、Kaspersky Security Network に関する声明の本文を読み、条項に同意します。

Kaspersky Security Network の設定

設定	説明
Kaspersky Security Network に関する声明をすべて確認し、理解した上で条項に同意する	このオプションをオンにすることにより、Kaspersky Security Network を使用することを確認し、表示される Kaspersky Security Network に関する声明をすべて確認し、理解した上で条項に同意します。 このオプションは、［Kaspersky Security Network の設定］ウィンドウで［**基本 KSN モード**］または［**拡張 KSN モード**］をオンにした場合に使用できます。
Kaspersky Security Network に関する声明の条項に同意しない	このオプションをオンにすることにより、Kaspersky Security Network を使用しないことを確定します。 このオプションは、［Kaspersky Security Network の設定］ウィンドウで［**基本 KSN モード**］または［**拡張 KSN モード**］をオンにした場合に使用できます。

Kaspersky Private Security Network に関する声明

このウィンドウでは、Kaspersky Security Network に関する声明の本文を読み、条項に同意します。

Kaspersky Security Network の設定

設定	説明
Kaspersky Security Network に関する声明をすべて確認し、理解した上で条項に同意する	このオプションをオンにすることにより、Kaspersky Security Network に参加することを確認し、表示される Kaspersky Private Security Network に関する声明をすべて確認し、理解した上で条項に同意します。
Kaspersky Security Network に関する声明の条項に同意しない	このオプションをオンにすることにより、Kaspersky Security Network を使用しないことを確定します。

コマンドラインでの Kaspersky Security Network の使用を設定します。

アプリケーションの全般設定で `UseKSN` オプションを使用すると、コマンドラインで Kaspersky Security Network の使用を有効または無効にできます。

`UseKSN` の値は、コマンドラインスイッチ、またはアプリケーションの全般設定をすべて含む設定情報ファイルを使用して変更できます。

コマンドラインスイッチを使用して Kaspersky Security Network の使用を有効にするには、次のコマンドを実行します：

```
kesl-control --set-app-settings UseKSN=<Extended/Basic> --accept-ksn
```

説明：

- `<Extended / Basic>`：Kaspersky Security Network モード。
- `--accept-ksn`：Kaspersky Security Network に関する声明の条項に同意することを示すキー。Kaspersky Security Network に関する声明をすべて確認し、理解した上で条項に同意します。

Kaspersky Security Network に関する声明が記載されているファイル ksn_license.<言語 ID> は、ディレクトリ /opt/kaspersky/kesl/doc/ にあります。

コマンドラインスイッチを使用して Kaspersky Security Network の使用を無効にするには、次のコマンドを実行します：

```
kesl-control --set-app-settings UseKSN=No
```

設定情報ファイルを使用した Kaspersky Security Network の使用を有効または無効にするには、次のコマンドを実行します：

```
kesl-control --set-app-settings --file <設定情報ファイルの名前> [--json] [--accept-ksn]
```

説明：

- `--file <設定情報ファイルへのパス>`：必要な `UseKSN` 値が設定されているアプリケーションの全般設定を含む設定情報ファイルへの絶対パス。
- `--json`：JSON形式の設定情報ファイルから設定をインポートする場合は、このライセンスを指定します。`--jason` のライセンスが指定されていない場合、設定は INI ファイルからインポートされます。インポートが失敗すると、エラーが表示されます。
- `--accept-ksn`：Kaspersky Security Network に関する声明の条項に同意することを示すキー。Kaspersky Security Network の使用を有効にする場合は、ライセンスを指定する必要があります。

クライアントデバイスにインストールされている Kaspersky Endpoint Security が、Kaspersky Security Center に割り当てられたポリシーに従って動作している場合、`UseKSN` 設定の値は Kaspersky Security Center を使用する場合のみ変更することができます。クライアントデバイスにインストールされている Kaspersky Endpoint Security がポリシーに基づいて実行を停止した場合、`UseKSN=No` の値が設定に割り当てられます。

コマンドラインを使用した Kaspersky Security Network への接続のチェック

Kaspersky Security Network への接続をチェックするには、次のコマンドを実行します：

```
kesl-control --app-info
```

Kaspersky Security Network の使用状況行には、Kaspersky Security Network への接続状況が表示されます：

- 拡張 `KSN` モードが表示されている場合、Kaspersky Endpoint Security は Kaspersky Security Network を使用し、ナレッジベースから情報を取得、および脅威の種別や発生源に関する統計や情報を匿名で送信され

ます。

- 基本 `KSN` モードが表示されている場合、Kaspersky Endpoint Security は Kaspersky Security Network を使用し、ナレッジベースから情報を取得できますが、脅威の種別や発生源に関する統計や情報を匿名で送信されません。

- `Disabled` ステータスが表示されている場合、Kaspersky Endpoint Security は Kaspersky Security Network を使用していません。

Kaspersky Security Network インフラストラクチャ行には、カスペルスキーのレピュテーションデータベースと連携するために使用されるインフラストラクチャソリューション（`Kaspersky Security Network` または `Kaspersky Private Security Network`）に関する情報が表示されます。

Kaspersky Security Network への接続は、以下の理由で確立されないことがあります：

- ユーザーデバイスがインターネットに接続していない。

- Kaspersky Security Network の使用不可。

- 本製品がアクティベートされていない、またはライセンスの有効期間が終了している。

- ライセンスに関する問題が検知された。たとえば、ライセンスが拒否リストに記載されている。

コマンドラインからのクラウドモードの有効化と無効化

*クラウドモード*は、マルウェアデータベースの軽量バージョンを使用する Kaspersky Endpoint Security の操作モードです。

> Kaspersky Endpoint Security が仮想環境を保護するために Light Agent モードで実行されている場合、軽量のマルウェア対策データベースはサポートされません。アプリケーションは、Light Agent の動作に必要な特別なデータベースを保護サーバーから受け取ります。

アプリケーションの全般設定の `CloudMode=Yes/No` オプションを使用して、コマンドラインでクラウドモードを有効または無効にできます。

CloudMode の値は、アプリケーションの全般設定をすべて含む設定情報ファイルを使用するか、コマンドラインオプションを使用して変更できます。

> Kaspersky Security Network の使用が有効になっている場合、クラウドモードを使用できます。

製品の詳細設定

次の追加アプリケーション設定を行うことができます：

- 本製品でプロキシサーバーを使用します。
- グローバル除外 – ファイル脅威対策、アンチクリプター、コンテナ監視コンポーネント、および簡易スキャン、コンテナスキャン、リムーバブルドライブのスキャンタスクのファイル操作遮断からマウント ポイントを除外します。
- スキャンからプロセスメモリを除外
- ファイル操作遮断モード。
- 脅威侵入者がデバイスやデータを侵害するために使用できる正規のアプリケーションを検出します。
- アプリケーションの安定性監視。
- 本製品の起動設定。
- スキャンタスクのメモリとプロセッサリソースの使用制限。
- 本製品による常駐メモリの使用を制限。
- 非特権ユーザーが同時に開始できるオブジェクトスキャンタスク数の制限。
- Kaspersky Security Center の保管領域への情報転送の設定。
- タスク管理許可。

プロキシサーバーの設定

クライアントデバイスのユーザーがプロキシサーバーを使用してインターネットに接続する場合、プロキシサーバーの設定を行うことができます。Kaspersky Endpoint Security は、カスペルスキーのサーバーへの接続にプロキシサーバーを使用する場合があります。たとえば、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時、Kaspersky Security Network および Kaspersky Endpoint Detection and Response（KATA）との通信時などです。

プロキシサーバーは、既定でオフになっています。

Kaspersky Endpoint Security を仮想環境保護用 Light Agent モードで使用する場合、Kaspersky Security Network、SVM、および Integration Server との接続にプロキシサーバーを使用することはサポートされません。

Web コンソールでのプロキシサーバーの設定

管理コンソールでは、ポリシーのプロパティ（**製品設定 → 全般設定 → プロキシサーバー設定**）でプロキシサーバーの使用を設定できます。

設定	説明
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、アプリケーションはプロキシサーバーを使用しません。
プロキシサーバー設定を指定する	このオプションが選択されている場合、アプリケーションは、たとえばKaspersky Endpoint Detection and Response (KATA) との統合のために、指定されたプロキシ サーバー設定を使用します。
アドレス	プロキシサーバーの IP アドレスまたはドメイン名の入力フィールド。 このフィールドは、［**指定したプロキシサーバー設定を使用する**］をオンにすると使用できます。
Port	プロキシサーバーのポート入力用のフィールド。 既定値：3128 このフィールドは、［**指定したプロキシサーバー設定を使用する**］をオンにすると使用できます。
プロキシサーバー認証を使用する	ユーザー名とパスワードを使用したプロキシサーバー認証を使用するかどうかをオンまたはオフにします。 このチェックボックスは、［**指定したプロキシサーバー設定を使用する**］をオンにすると使用できます。 既定では、このチェックボックスはオフです。 HTTP プロキシ経由で接続する場合は、他のシステムへのログインに使用しない別のアカウントを使用することを推奨します。HTTP プロキシがセキュアでない接続を使用しているため、アカウントが危険にさらされている可能性があります。
ユーザー名	プロキシサーバー認証のために使用されるユーザー名の入力フィールド。 この入力フィールドは、**プロキシサーバー認証を使用する**のチェックボックスがオンの場合に使用できます。
編集	プロキシサーバー上で認証するためのパスワードを指定できるようにします。［**パスワード**］フィールドは編集できません。既定では、このパスワードは空です。 パスワードを指定するには、［**編集**］をクリックします。開いたウィンドウにパスワードを入力し、［**OK**］をクリックします。 パスワードの複雑性とブルートフォース攻撃防止メカニズムにより、6 か月以内にパスワードが推測できないようにすることを推奨します。 ［パスワード入力］ウィンドウの、パスワードが見えるように表示されたウィンドウで［**表示**］をクリックします。 このボタンは、**プロキシサーバー認証を使用する**のチェックボックスがオンの場合に使用できます。
Kaspersky Security Center を製品のアクティベーションのプロキシサーバーとして使用する	このチェックボックスでは、Kaspersky Security Center を製品のアクティベーションのプロキシサーバーとして使用するかどうかを選択します。 このチェックボックスをオンにすると、Kaspersky Endpoint Security は製品のアクティベーションのプロキシサーバーとして Kaspersky Security Center を使用します。

	既定では、このチェックボックスはオフです。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。アプリケーションを仮想環境保護用 Light Agent モードで使用する場合、ライセンス情報は Protection Server によって提供されます。

管理コンソールでのプロキシサーバーの設定

管理コンソールでは、ポリシーのプロパティ（**全般設定 → プロキシサーバー設定**）でプロキシサーバーの使用を設定できます。

プロキシサーバー設定

設定	説明
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、アプリケーションはプロキシサーバーを使用しません。
プロキシサーバー設定を指定する	このオプションが選択されている場合、アプリケーションは、たとえば Kaspersky Endpoint Detection and Response (KATA) との統合のために、指定されたプロキシ サーバー設定を使用します。
アドレスとポート	プロキシサーバーの IP アドレスまたはドメイン名、およびポートを入力するフィールド。 既定のポート：3128。 これらのフィールドは、**指定したプロキシサーバー設定を使用する**をオンにすると使用できます。
プロキシサーバー認証を使用する	このチェックボックスでは、ユーザー名とパスワードを使用したプロキシサーバー認証を使用するかどうかを選択します。 このチェックボックスは、［**指定したプロキシサーバー設定を使用する**］をオンにすると使用できます。 既定では、このチェックボックスはオフです。 HTTP プロキシ経由で接続する場合は、他のシステムへのログインに使用しない別のアカウントを使用することを推奨します。HTTP プロキシがセキュアでない接続を使用しているため、アカウントが危険にさらされている可能性があります。
ユーザー名	プロキシサーバー認証のために使用されるユーザー名の入力フィールド。 この入力フィールドは、**プロキシサーバー認証を使用する**のチェックボックスがオンの場合に使用できます。
パスワード	プロキシサーバー認証のためのユーザーパスワードの入力フィールド。 パスワードの複雑性とブルートフォース攻撃防止メカニズムにより、6 か月以内にパスワードが推測できないようにすることを推奨します。

	［**表示**］をクリックすると、［**パスワード**］フィールドでユーザーパスワードが見えるように表示されます。既定では、ユーザーパスワードは非表示で、アスタリスクで示されます。 **プロキシサーバー認証を使用する**のチェック ボックスがオンの場合、テキストボックスとボタンが利用可能になります。
Kaspersky Security Center を製品のアクティベーションのプロキシサーバーとして使用する	このチェックボックスでは、Kaspersky Security Center を製品のアクティベーションのプロキシサーバーとして使用するかどうかを選択します。 このチェックボックスをオンにすると、Kaspersky Endpoint Security は製品のアクティベーションのプロキシサーバーとして Kaspersky Security Center を使用します。 既定では、このチェックボックスはオフです。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。アプリケーションを仮想環境保護用 Light Agent モードで使用する場合、ライセンス情報は Protection Server によって提供されます。

コマンドラインでのプロキシサーバーの設定

アプリケーションコンポーネントによるプロキシサーバーの使用は、アプリケーションの全般設定にある `UseProxy` と `ProxyServer` の設定を使用して、コマンドラインで有効または無効にすることができます。

コマンドラインオプションまたは本製品の全般設定のすべてを含む設定情報ファイルを使用して設定を編集できます。

`UseProxy` の設定は次の値を使用できます：

- `Yes` – プロキシサーバーの使用を有効にします。
- `No` – プロキシサーバーの使用を無効にします。

`ProxyServer` の設定では、プロキシサーバーの設定を次の形式で定義できます：`[< ユーザー >[:< パスワード >]@]< プロキシサーバーアドレス >[:< ポート >]`：

- `< ユーザー >` はプロキシサーバー認証用のユーザー名です。
- `< password >`は、プロキシサーバー認証用のユーザーパスワードです。
- `< proxy server address >` はプロキシサーバーの IP アドレスまたはドメイン名です。
- `< port >`はプロキシサーバーのポートです。

プロキシサーバーへの接続に認証が必要ない場合は、`ProxyServer` を定義する必要はありません。

HTTP プロキシ経由で接続する場合は、他のシステムへのログインに使用しない別のアカウントを使用することを推奨します。HTTP プロキシがセキュアでない接続を使用しているため、アカウントが危険にさらされている可能性があります。

グローバル除外の設定

ファイル脅威対策コンポーネントおよびアンチクリプターコンポーネントのファイル操作遮断からマウントポイントの除外を設定することができます。また、マルウェアのスキャン、簡易スキャン、およびコンテナスキャンのタスクからも除外できます。マウントポイントを除外すると、デバイスにマウントされたローカルディレクトリまたはリモートディレクトリをファイル操作の遮断から除外できます。さらに、グローバル除外は、コンテナ監視コンポーネントとリムーバブルドライブスキャンタスクの動作に影響します。

Web コンソールでのグローバル除外リストの設定

Web コンソールでは、ポリシーのプロパティでグローバル除外の使用を設定できます（**製品設定→全般設定→グローバル除外**）。

グローバル除外セクションの表には、ファイル操作の遮断から除外されるマウントポイントが含まれています。

［**パス**］の列には、除外されたマウントポイントへのパスが表示されます。既定では、表は空です。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

［マウントポイントの除外の追加］ウィンドウ

マウントポイントの設定

設定	説明
ファイルシステム、アクセスプロトコル、パス	このドロップダウンリストでは、スキャンの除外に追加するディレクトリがあるファイルシステムの種別を選択できます： • **Local**：ローカルマウントポイント。 • **Mounted**：Samba または NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **リモートでマウント済みのすべての場所** - Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。
アクセスプロトコル	ドロップダウンリストからリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。

	• **カスタム** – 下のフィールドで指定したデバイスファイルシステムのリソース。 このドロップダウンリストは、ファイルシステムのドロップダウンリストから［**Mounted**］を選択した場合に使用できます。
パス	ファイル操作のインターセプトから除外するマウント ポイントへのパスを入力するフィールド。パスの指定にマスクを使用できます。 アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。 マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。 ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。 このフィールドは、ファイルシステムのドロップダウンリストから［**Local**］を選択した場合に使用できます。
共有リソース名	ファイル システム共有リソースの名前を入力するためのフィールドです。ファイル操作傍受の除外対象に追加するディレクトリが配置されています。 このフィールドは、［ファイルシステム］ドロップダウンリストで［**Mounted**］が選択され、［**アクセスプロトコル**］ドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。

管理コンソールでのグローバル除外リストの設定

管理コンソールでは、ポリシーのプロパティでグローバル除外の使用を設定できます（**全般設定 → グローバル除外**）。

除外されたマウントポイント設定グループには、**設定**ボタンが含まれています。このボタンをクリックすると、［**除外するマウントポイント**］ウィンドウが表示されます。

ウィンドウ内のリストには、除外されたマウントポイントへのパスが含まれています。既定では、このリストは空です。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択した項目が表から削除されます。

このボタンは、少なくとも1つの項目を表から選択している場合に使用できます。

マウントポイントのパス

マウントポイントの設定

設定	説明
ファイルシステム、アクセスプロトコル、パス	これらの設定では、マウントポイントの場所を設定できます。 ファイルシステムのドロップダウンリストで、スキャンの除外に追加するディレクトリがあるファイルシステムの種別を選択できます： • **Local**：ローカルマウントポイント。 • **Mounted**：Samba または NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **リモートでマウント済みのすべての場所** - Samba および NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリ。
	ファイルシステムのドロップダウンリストで **Mounted** を選択した場合は、右側のドロップダウンリストでリモートアクセスプロトコルを選択できます： • **NFS**：NFS プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **Samba**：Samba プロトコルを使用してデバイスにマウントされるリモートディレクトリ。 • **カスタム**：下のフィールドで指定したデバイスファイルシステムのすべてのリソース。
	ファイルシステムのドロップダウンリストで **Local** が選択されている場合は、入力フィールドに、ファイル操作のインターセプトから除外するマウント ポイントへのパスを入力できます。パスの指定にマスクを使用できます。

	アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。 ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」 2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」 アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。 マウントポイント /dir を除外するには、/dir （アスタリスク記号（*）なし）を特に示す必要があります。 マスク /dir/* では、/dir のすぐ下のレベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。/dir/** では、/dir よりも下の全レベルですべてのマウントポイントが除外されますが、/dir 自身は除外されません。 ファイル名またはディレクトリ名には、? 文字で任意の文字（/ を含む）を表示できます。
ファイルシステム名	ファイル操作のインターセプトから除外するディレクトリがあるファイル システムの名前を入力するフィールド。 このフィールドは、ファイルシステムのドロップダウンリストで［**Mounted**］が選択され、右側のドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。

コマンドラインでのグローバル除外リストの設定

アプリケーションの全般設定の ExcludedMountPoint.item_# オプションを使って、コマンドラインでマウントポイントの除外を定義できます。

コマンドラインオプションまたは本製品の全般設定のすべてを含む設定情報ファイルを使用して設定を編集できます。

ExcludedMountPoint.item_# オプションでは、次の値を利用できます：

- AllRemoteMounted — SMB プロトコルと NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリをファイル操作のインターセプトから除外します。
- Mounted:NFS — NFS プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリをファイル操作のインターセプトから除外します。
- Mounted:SMB — SMB プロトコルを使用してデバイスにマウントされるすべてのリモートディレクトリをファイル操作のインターセプトから除外します。

- `Mounted:<` ファイルシステムの種別 `>` - 指定したファイルシステム種別でマウントされるすべてのディレクトリをファイル操作のインターセプトから除外します。

- `/mnt` — /mnt マウントポイント（サブディレクトリを含む）内のオブジェクトをファイル操作傍受から除外します。このディレクトリは、リムーバブルドライブの一時的なマウントポイントとして使用されます。

- `<`「`/mnt/user*`」または「`/mnt/**/user_share`」を含むパス`>` - 指定したマスクを名前に含むマウントポイントのオブジェクトをファイル操作のインターセプトから除外します。

  アスタリスク記号「`*`」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

  ファイル名またはディレクトリ名の「`/`」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「`*`」記号を 1 つ指定することができます。例：「`/dir/*/file`」または「`/dir/*/*/file`」

  2 つの連続する「`*`」記号は、ファイル名またはディレクトリ名における「`/`」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「`/dir/**/file*/`」または「`/dir/file**/`」

  アスタリスク記号を 2 文字連続させた「`**`」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「`/dir/**/**/file`」は不適切なマスク表現となります。

  マウントポイント `/dir` を除外するには、`/dir` （アスタリスク記号（`*`）なし）を特に示す必要があります。

  マスク `/dir/*` では、`/dir` のすぐ下のレベルですべてのマウントポイントが除外されますが、`/dir` 自身は除外されません。`/dir/**` では、`/dir` よりも下の全レベルですべてのマウントポイントが除外されますが、`/dir` 自身は除外されません。

  ファイル名またはディレクトリ名には、`?` 文字で任意の文字（`/` を含む）を表示できます。

複数のマウントポイントを選択して、スキャンから除外することも可能です。

マウントポイントは、`mount` コマンドを実行して出力されるのと同じものを指定する必要があります。

プロセスメモリをスキャンから除外

スキャンからプロセスメモリを除外できます。指定されたプロセスのメモリはスキャンされません。

Web コンソールでの除外リストの設定

Web コンソールでは、ポリシーのプロパティ（**製品設定 → 全般設定 → 製品設定**）で、プロセスメモリをスキャンから除外するように設定できます。

［**プロセスメモリのスキャンからの除外を設定**］の［**プロセスメモリをスキャンから除外**］をクリックすると、［**プロセスメモリをスキャンから除外**］ウィンドウが開き、除外リストを作成できます。

プロセスメモリをスキャンから除外ウィンドウのリストには、アプリケーションがプロセスメモリのスキャンから除外するプロセスへのパスが含まれています。パスの指定にマスクを使用できます。既定では、このリストは空です。

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「**/dir/*/file**」または「**/dir/*/*/file**」

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「**/dir/**/file*/**」または「**/dir/file**/**」

アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「**/dir/**/**/file**」は不適切なマスク表現となります。

マウントポイント **/dir** を除外するには、**/dir** （アスタリスク記号（*）なし）を特に示す必要があります。

マスク **/dir/*** では、**/dir** のすぐ下のレベルですべてのマウントポイントが除外されますが、**/dir** 自身は除外されません。**/dir/**** では、**/dir** よりも下の全レベルですべてのマウントポイントが除外されますが、**/dir** 自身は除外されません。

ファイル名またはディレクトリ名には、**?** 文字で任意の文字（/ を含む）を表示できます。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択したプロセスのパスがリストから削除されます。

このボタンは、少なくとも1つのプロセスのパスをリストから選択している場合に使用できます。

［**編集**］をクリックすると、プロセスのパスを変更できるウィンドウが表示されます。指定されたプロセスのメモリがスキャンから除外されます。

［**追加**］をクリックすると、プロセスへの絶対パスを入力できるウィンドウが表示されます。指定されたプロセスのメモリがスキャンから除外されます。

管理コンソールでの除外リストの設定

管理コンソールでは、ポリシーのプロパティ（**全般設定 → プロセスメモリの除外**）で、プロセスメモリをスキャンから除外するように設定できます。

プロセスメモリをスキャンから除外で**設定**をクリックすると、除外リストを作成できるウィンドウが開きます。

プロセスメモリをスキャンから除外ウィンドウのリストには、アプリケーションがプロセスメモリのスキャンから除外するプロセスへのパスが含まれています。パスの指定にマスクを使用できます。既定では、このリストは空です。

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：「**/dir/*/file**」または「**/dir/*/*/file**」

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「**/dir/**/file*/**」または「**/dir/file**/**」

アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で 1 回のみ使用できます。たとえば、「**/dir/**/**/file**」は不適切なマスク表現となります。

マウントポイント **/dir** を除外するには、**/dir** （アスタリスク記号（*）なし）を特に示す必要があります。

マスク **/dir/*** では、**/dir** のすぐ下のレベルですべてのマウントポイントが除外されますが、**/dir** 自身は除外されません。**/dir/**** では、**/dir** よりも下の全レベルですべてのマウントポイントが除外されますが、**/dir** 自身は除外されません。

ファイル名またはディレクトリ名には、**?** 文字で任意の文字（/ を含む）を表示できます。

表内の項目は、追加、編集、削除できます。

［**削除**］をクリックすると、選択したプロセスのパスがリストから削除されます。

このボタンは、少なくとも 1 つのプロセスのパスをリストから選択している場合に使用できます。

［**編集**］をクリックすると、プロセスのパスを変更できるウィンドウが表示されます。指定されたプロセスのメモリがスキャンから除外されます。

［**追加**］をクリックすると、プロセスへの絶対パスを入力できるウィンドウが表示されます。指定されたプロセスのメモリがスキャンから除外されます。

コマンドラインでの除外リストの設定

アプリケーションの全般設定の **MemScanExcludedProgramPath.item_#** オプションを使用して、コマンドラインでスキャンからのプロセスメモリ除外を設定できます。

コマンドラインオプションまたは本製品の全般設定のすべてを含む設定情報ファイルを使用して設定を編集できます。

MemScanExcludedProgramPath.item_# には、ローカルディレクトリ内のプロセスへの絶対パスが含まれています。パスの指定にマスクを使用できます。

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」

アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。

ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。

複数のプロセスを選択して、スキャンから除外することも可能です。

ファイル操作の遮断モードの選択

ファイル操作遮断モードは、ファイル脅威対策およびデバイスコントロールコンポーネントに影響します。

- スキャン中、アプリケーションは、ファイル脅威対策コンポーネントによってスキャンされているファイルへのアクセスをブロックできます。既定では、アクセスはブロックされています。スキャンされたファイルへのアクセスは、スキャン結果が出るまで待機する必要があります。スキャンでファイル内に脅威が検知されない場合、アプリケーションはファイルへのアクセスを許可します。感染オブジェクトを検知すると、アプリケーションはファイル脅威対策の**最初の処理**（FirstAction）および**次の処理**（SecondAction）設定で指定された処理を実行します。

  ファイル脅威対策コンポーネントによってスキャンされているファイルへのアクセスをブロックしないように選択できます。その場合、スキャンは非同期で実行されます。

- デバイスコントロールコンポーネントがデバイスへのアクセスを許可するかどうかを決定している間、アプリケーションはデバイス上のファイルへのアクセスをブロックできます。既定では、アクセスはブロックされています。管理対象デバイス上のファイルへのアクセスは、スキャン結果が出るまで待機する必要があります。スキャン後にデバイスコントロールがファイルを含むデバイスへのアクセスを許可した場合、アプリケーションはファイルへのアクセスを許可します。

  デバイスコントロールコンポーネントによって監視されるデバイス上のファイルアクセスのブロックを無効にできます。その場合、デバイスコントロールは、デバイスへのアクセスを非同期モードで許可できるかどうかを決定します。

Web コンソールでのポリシーの設定

Web コンソールでは、ポリシーのプロパティ（**製品設定 → 全般設定 → 製品設定**、**ファイル操作遮断モード**セクション）でファイル操作遮断モードを設定できます。

スキャン中のファイルへのアクセスのブロックチェック ボックスは、ファイル脅威対策およびデバイスコントロールコンポーネントによってスキャンされているファイルへのアクセスのブロックを有効または無効にします。

既定では、このチェックボックスはオンです。

チェックボックスをオフにすると、スキャン中はすべてのファイルへのアクセスが許可され、スキャンは非同期モードで実行されます。

管理コンソールでのポリシーの設定

管理コンソールでは、ポリシーのプロパティ（**全般設定 → 製品設定**、**ファイル操作遮断モード**セクション）でファイル操作遮断モードを設定できます。

スキャン中のファイルへのアクセスのブロックチェック ボックスは、ファイル脅威対策およびデバイスコントロールコンポーネントによってスキャンされているファイルへのアクセスのブロックを有効または無効にします。

既定では、このチェックボックスはオンです。

チェックボックスをオフにすると、スキャン中はすべてのファイルへのアクセスが許可され、スキャンは非同期モードで実行されます。

コマンドラインでの設定

アプリケーションの全般設定のFileBlockDuringScan 設定を使用して、コマンドラインでファイル操作遮断モードを設定できます。

コマンドラインオプションまたは本製品の全般設定のすべてを含む設定情報ファイルを使用して設定を編集できます。

`FileBlockDuringScan` オプションでは、次の値を利用できます：

- はい（既定値）を選択すると、ファイル脅威対策およびデバイスコントロールのコンポーネントによるスキャン中、ファイルへのアクセスがブロックされます。
- スキャン中にファイルにアクセスする場合はいいえを選択します。すべてのファイルへのリクエストを許可し、スキャンは非同期に行われます。

> このファイル操作遮断モードはシステムパフォーマンスに与える影響は少ないですが、本製品がファイルの状態を判断する前に、たとえばスキャン中にファイルの名前が変更された場合、ファイル内の脅威が駆除または削除されないリスクがあります。

ハッカーが危害を加えるために使用できるアプリケーションの検知の設定

侵入者がデバイスやデータを侵害するために使用できる正規のアプリケーションの検出を有効または無効にします。

Web コンソールでのポリシーの設定

Web コンソールでは、ポリシーのプロパティ（**製品設定 → 全般設定 → 製品設定**、**スキャン設定**セクション）でデバイスまたはデータを侵害するために使用できる正規のアプリケーションを検知できます。

ユーザーに損害を与える目的で悪用される可能性がある正規のアプリケーションを検知するするチェック ボックスでは、侵入者がユーザーのデバイスやデータに損害を与えるために使用できる正規のアプリケーションの検知を有効または無効にします。

既定では、このチェックボックスはオフです。

管理コンソールでのポリシーの設定

管理コンソールでは、ポリシーのプロパティ（**全般設定 → 製品設定**、**スキャン設定**セクション）でデバイスまたはデータを侵害するために使用できる正規のアプリケーションを検知できます。

ユーザーに損害を与える目的で悪用される可能性がある正規のアプリケーションを検知するするチェック ボックスでは、侵入者がユーザーのデバイスやデータに損害を与えるために使用できる正規のアプリケーションの検知を有効または無効にします。

既定では、このチェックボックスはオフです。

コマンドラインでの設定

コマンドラインでは、アプリケーションの全般設定の `DetectOtherObjects` 設定を使用して、侵入者がデバイスやデータを侵害するために使用できる正規のアプリケーションの検知を有効または無効にできます。

コマンドラインオプションまたは本製品の全般設定のすべてを含む設定情報ファイルを使用して設定を編集できます。

`DetectOtherObjects` では次の値を利用できます：

- `Yes`：侵入者がデバイスやデータを侵害するために使用できる正規のアプリケーションの検出を有効にします。
- `No`：侵入者がデバイスやデータを侵害するために使用できる正規のアプリケーションの検出を有効にしません。

本製品の安定性監視の有効化

本製品が異常終了した回数を追跡し、不安定な動作について管理者に通知することができる Kaspersky Endpoint Security の安定性監視を有効または無効にできます。

Web コンソールでのポリシーの設定

Web コンソールでは、ポリシーのプロパティ（［**製品設定**］→［**全般設定**］→［**製品設定**］の［**製品詳細設定**］セクション）で製品安定性監視を有効または無効にできます。

［**製品安定性監視を有効にする**］チェックボックスをオンにすると、Kaspersky Endpoint Security 製品の状態の監視が有効または無効になります。

既定では、このチェックボックスはオフです。

> 設定を適用するには、本製品を再起動する必要があります。

本製品が不安定な場合は、本製品がインストールされているデバイスのプロパティに次のメッセージが表示されます：*<日時> より本製品の異常停止 <回数> 回。*

管理コンソールでのポリシーの設定

管理コンソールでは、ポリシーのプロパティ（［**全般設定**］→［**製品設定**］の［**製品詳細設定**］セクション）で製品安定性監視を有効または無効にできます。

［**製品安定性監視を有効にする**］チェックボックスをオンにすると、Kaspersky Endpoint Security 製品の状態の監視が有効または無効になります。

既定では、このチェックボックスはオフです。

設定を適用するには、本製品を再起動する必要があります。

本製品が不安定な場合は、本製品がインストールされているデバイスのプロパティに次のメッセージが表示されます：*<日時> より本製品の異常停止 <回数> 回。*

コマンドラインでの設定

コマンドラインでは、`kesl.ini` 設定情報ファイルの `TrackProductCrashes`、`ProductHealthLogFile`、`WarnThreshold`、`WarnAfter_#_crash`、および WarnRemovingThreshold 設定を使用して、本製品の安定性監視を構成できます。

`TrackProductCrashes` 設定を使用すると、本製品の安定性監視を有効または無効にすることができます。この設定は次の値を使用できます：

- `Yes/true` – 本製品の安定性監視を有効にします。
- `No/false` – 本製品の安定性監視を有効にしません。

`ProductHealthLogFile` 設定では、本製品の安定性監視に使用されるファイルへのパスを指定できます。既定値：/var/opt/kaspersky/kesl/private/kesl_health.log.

`WarnThreshold` 設定では、不安定な動作に関する通知を表示する前に、本製品が指定された回数の異常停止を経験する必要がある時間間隔（秒単位）を設定できます。既定値：3600 秒。

`WarnRemovingThreshold` 設定では、本製品の不安定な状態がクリアされるまでの時間間隔 (秒単位) を設定できます。既定値：86400 秒。

`WarnAfter_#_crash` 設定では、不安定な製品動作に関する通知を表示する前に必要な製品の異常停止回数を設定できます。設定できる値は 0 ～ 10 です。既定値：10値が 0 の場合、不安定な製品の通知は表示されません。

本製品の起動設定の構成

次の製品起動設定を行うことができます：

Web コンソールでの制限の設定

Web コンソールでは、ポリシーのプロパティ（［**製品設定**］→［**全般設定**］→［**製品設定**］の［**製品起動設定**］）で本製品の起動設定を構成できます。

本製品の起動設定

設定	説明
本製品の起動失敗の最大試行回数	本製品の起動に連続して失敗する最大回数を入力するフィールド。 既定値：5
本製品の起動を待機する最大時間（分）	本製品の起動を待機する最大時間（分単位）の入力フィールド。この時間が経過すると、kesl プロセスが再起動されます。 既定値：3

管理コンソールでの制限の設定

管理コンソールでは、ポリシーのプロパティ（［［**全般設定**］→［**製品設定**］の［**製品起動設定**］）で本製品の起動設定を構成できます。

［**製品の起動設定**］で［**設定**］ボタンをクリックすると、［**製品の起動設定**］ウィンドウが開き、製品の起動設定を編集できます（次の表を参照）。

本製品の起動設定

設定	説明
本製品の起動失敗の最大試行回数	本製品の起動に連続して失敗する最大回数を入力するフィールド。 既定値：5
本製品の起動を待機する最大時間（分）	本製品の起動を待機する最大時間（分単位）の入力フィールド。この時間が経過すると、kesl プロセスが再起動されます。 既定値：3

コマンドラインでの制限の設定

コマンドラインでは、`kesl.ini` 設定情報ファイルの `MaxRestartCount` および StartupTimeout 設定を使用して、本製品の起動設定を構成できます。

`MaxRestartCount` 設定を使用すると、本製品の起動に連続して失敗する最大回数を設定できます。設定できる値は 1～10 です。既定値：5

`StartupTimeout` の設定で、本製品の起動を待機する最大時間（分単位）を設定できます。この時間が経過すると、kesl プロセスが再起動されます。設定できる値は 1～60 です。既定値：3

メモリーとプロセッサリソースの使用の制限

スキャンタスクの CPU 使用量に制限を設定できます。既定では、制限は設定されていません。スキャンタスクのメモリ使用量制限を設定することもできます。既定の制限は 8192 メガバイトです。

Web コンソールでの制限の設定

Web コンソールでは、ポリシーのプロパティ（**製品設定 → 全般設定 → 製品設定**、**パフォーマンス**セクション）で、CPU 使用率制限を有効または無効にしたり、スキャンタスクのメモリ使用量制限を設定したりできます。

設定

設定	説明
スキャンのメモリ使用率を制限する（MB)	スキャンタスクのメモリ使用量制限（メガバイト単位）の入力フィールド。 既定値：8192
スキャンタスクのCPU使用率を制限する（%）	このチェックボックスは、マルウェアのスキャン、簡易スキャン、インベントリ、およびコンテナのスキャンタスクのCPU使用率制限を有効または無効にします。 チェックボックスをオンにすると、すべてのプロセッサコアの最大使用率が**上限 (%)** で指定した数値を超えなくなります。 既定では、このチェックボックスはオフです。

管理コンソールでの制限の設定

管理コンソールでは、ポリシーのプロパティ（**全般設定 → 製品設定**、**パフォーマンス**セクション）で、CPU使用率制限を有効または無効にしたり、スキャンタスクのメモリ使用量制限を設定したりできます。

［**パフォーマンス**］の下にある［**設定**］をクリックすると、［**CPU およびメモリの使用率**］ウィンドウが開き、制限を設定できます（下の表を参照）。

設定

設定	説明
スキャンタスクのCPU使用率を制限する（%）	このチェックボックスは、マルウェアのスキャン、簡易スキャン、インベントリ、およびコンテナのスキャンタスクのCPU使用率制限を有効または無効にします。 チェックボックスをオンにすると、すべてのプロセッサコアの最大使用率が右のフィールドでで指定した率を超えなくなります。 既定では、このチェックボックスはオフです。
スキャンのメモリ使用率を制限する（MB)	スキャンタスクのメモリ使用量制限（メガバイト単位）の入力フィールド。 既定値：8192

コマンドラインでの制限の設定

コマンドラインでは、*アプリケーションの全般設定*の *UseOnDemandCPULimit* および *OnDemandCPULimit* 設定を使用する `ODS`、`ContainerScan`、および InventoryScan タスクでCPU使用率の制限を設定できます。

コマンドラインオプションまたは本製品の全般設定のすべてを含む設定情報ファイルを使用して設定を編集できます。

`UseOnDemandCPULimit` では次の値を利用できます：

- `Yes`：*ODS*、*ContainerScan*、および *InventoryScan* タスクの CPU 使用量制限を有効にします。
- `No`：タスクの CPU 使用量制限を無効にします。

`OnDemandCPULimit` オプションは、*ODS*、*ContainerScan*、および *InventoryScan* タスクを実行するときのすべてのプロセッサコアの最大使用率レベルを（パーセンテージで）設定します。このオプションは 10 ～ 100 の値を利用できます。既定値は 100 です。

コマンドラインでは、*kesl.ini 設定情報ファイルの ScanMemoryLimit* 設定を使用する *ODS*、`ContainerScan`、および InventoryScan タスクでメモリ使用量の制限を設定できます。既定値：8192

本製品による常駐メモリの使用の制限

本製品の常駐メモリの使用に制限を設定できます。既定では、制限は自動的に設定されます。

Web コンソールでの制限の設定

Web コンソールでは、ポリシーのプロパティ（［**アプリケーション設定**］→［**全般設定**］→［**アプリケーション設定**］の［**製品詳細設定**］セクション）で常駐メモリの使用量制限を有効または無効にできます。

［**製品詳細設定**］セクションで、［**メモリ使用量の設定**］リンクをクリックすると、常駐メモリの使用量制限を設定できるウィンドウが開きます（次の表を参照）。

設定

設定	説明
本製品による常駐メモリ使用量	ドロップダウンリストでは、常駐メモリの使用量を制限する方法を選択できます。 • **無制限**。この項目を選択すると、常駐メモリの使用量は制限されません。 • **合計に対する割合に制限されます**。この項目を選択すると、［**メモリ使用量制限（%）**］フィールドが使用可能になり、必要な値をパーセンテージで指定できます。 • **MB 単位の値に制限されます**。この項目を選択すると、［**メモリ使用量制限（MB）**］フィールドが使用可能になり、希望の値をメガバイト単位で指定できます。 • **どちらか低い方（%、MB）に制限されます**。この項目を選択すると、［**メモリ使用量制限（%）**］および［**メモリ使用量の制限（MB）**］フィールドが使用可能になり、必要な値を指定できます。 • **どちらか高い方（%、MB）に制限されます**。この項目を選択すると、［**メモリ使用量制限（%）**］および［**メモリ使用量の制限（MB）**］フィールドが使用可能になり、必要な値を指定できます。 • **自動的に制限します（推奨）**。この項目を選択すると、常駐メモリの使用量が自動的に制限されます（規定値）。
メモリ使用量制限（%）	メモリ使用量制限（パーセンテージ）を入力するフィールド。 既定値：50
メモリ使用量制限（MB）	メモリ使用量制限（メガバイト単位）の入力フィールド。 既定値：2000

管理コンソールでの制限の設定

管理コンソールでは、ポリシーのプロパティ内で常駐メモリ使用量の制限を設定できます（**全般設定 → 製品設定**）。

［**製品の詳細設定**］セクションで［**設定**］ボタンをクリックすると［**追加設定**］ウィンドウが開き、常駐メモリの使用量制限を設定できます（次の表を参照）。

設定

設定	説明
アプリケーションのメモリ使用量	ドロップダウンリストでは、常駐メモリの使用量を制限する方法を選択できます。 • **無制限**。この項目を選択すると、常駐メモリの使用量は制限されません。 • **自動的に制限します（推奨）**。この項目を選択すると、常駐メモリの使用量が自動的に制限されます（規定値）。 • **合計に対する割合に制限されます**。この項目を選択すると、［**メモリ使用量制限（%）**］フィールドが使用可能になり、必要な値をパーセンテージで指定できます。 • **MB 単位の値に制限されます**。この項目を選択すると、［**メモリ使用量制限（MB）**］フィールドが使用可能になり、希望の値をメガバイト単位で指定できます。 • **どちらか低い方（%、MB）に制限されます**。この項目を選択すると、［**メモリ使用量制限（%）**］および［**メモリ使用量の制限（MB）**］フィールドが使用可能になり、必要な値を指定できます。 • **どちらか高い方（%、MB）に制限されます**。この項目を選択すると、［**メモリ使用量制限（%）**］および［**メモリ使用量の制限（MB）**］フィールドが使用可能になり、必要な値を指定できます。
メモリ使用量制限（%）	メモリ使用量制限（パーセンテージ）を入力するフィールド。 既定値：50
メモリ使用量制限（MB）	メモリ使用量制限（メガバイト単位）の入力フィールド。 既定値：2000

コマンドラインでの制限の設定

コマンドラインでは、`kesl.ini` 設定情報ファイルの MaxMemory 設定を使用して、常駐メモリの使用量制限を構成できます。

`MaxMemory` の設定は次の値を使用できます：

- `off` – 常駐設定のサイズは制限されません。
- `<value>%` – メモリのパーセンテージの値（1～100）。
- `<value>MB` – メガバイト単位の値。
- `lowest/<value>%/<value>MB` – パーセンテージで表した値とメガバイトで表した値の、小さい方の値。
  |
- `highest/<値>%/<値>MB` – パーセンテージで表した値とメガバイトで表した値の、大きい方の値。
- `auto` – 使用可能なメモリの最大 50%、ただし 2 GB 以上 16 GB 以下。

既定値：auto

オブジェクトスキャンタスク数の制限

特権のないユーザーがデバイス上で同時に実行できるオブジェクトスキャンタスクの数に制限を設定できます。root 権限を持つユーザーが実行できるタスクの数に制限はありません。

アプリケーションの全般設定の LimitNumberOfScanFileTasks オプションを使用して、コマンドラインで同時オブジェクトスキャンタスクの数の制限を有効または無効にできます。

コマンドラインオプションまたは本製品の全般設定のすべてを含む設定情報ファイルを使用して設定を編集できます。

`LimitNumberOfScanFileTasks` は 0 ～ 4294967295 の値を利用できます。既定値：0

0 を指定すると、権限のないユーザーはオブジェクトスキャンタスクを開始できません。

製品のインストール時に GUI パッケージをインストールした場合、`LimitNumberOfScanFileTasks` 設定の既定値は `5` になります。

Kaspersky Security Center Backup への情報送信の設定

Kaspersky Security Center では、未処理のファイルおよび接続されているデバイスに関する情報の Kaspersky Security Center 保管領域への転送を有効または無効にすることができます。

未処理のファイルに関する情報は、Web コンソール（**操作 → 保管領域 → アクティブな脅威**）および管理コンソール（**詳細設定 → 保管領域 → アクティブな脅威**）のアクティブな脅威のリストに表示されます。

インストールされているデバイス、またはクライアントデバイスに接続されているデバイスに関する情報は、Web コンソール（**操作 → 保管領域 → ハードウェア**）および管理コンソール（**詳細設定 → 保管領域 → ハードウェア**）のハードウェアリストに表示されます。デバイスコントロールが有効な場合、情報が転送されます。

Web コンソールでの情報の転送の有効化または無効化

Web コンソールでは、ポリシーのプロパティ（**製品設定 → 全般設定 → 保管領域設定**）で情報の送信を有効または無効にできます。

Kaspersky Security Center の保管領域への情報転送の設定

設定	説明
未処理ファイルの通知の有効化 / 無効化	この切り替えボタンでは、スキャン中に処理できないファイルに関する通知を管理サーバーに送信するかどうかを選択します。 この切り替えボタンは既定でオンになっています。
インストールされているデバイスの通知の有効化 / 無効化	この切り替えボタンは、クライアントデバイスにインストールされているデバイスまたはクライアントデバイスに接続されているデバイスに関する情報の管理サーバーへの転送を有効または無効にします。 この切り替えボタンは既定でオンになっています。

管理コンソールでの情報の転送の有効化および無効化

管理コンソールでは、ポリシーのプロパティ（**全般設定 → 保管領域設定**）で情報の送信を有効または無効にできます。

Kaspersky Security Center の保管領域への情報転送の設定

設定	説明
処理されていないファイルについて通知する	このチェックボックスでは、スキャン中に処理できないファイルに関する通知を管理サーバーに送信するかどうかを選択します。 既定では、このチェックボックスはオンです。
インストールされているデバイスについて通知する	このチェックボックスは、クライアントデバイスにインストールされているデバイスまたはクライアントデバイスに接続されているデバイスに関する情報の管理サーバーへの転送を有効または無効にします。 既定では、このチェックボックスはオンです。

タスク管理の許可設定

Kaspersky Security Center では、次のユーザー権限を定義できます：

- Kaspersky Endpoint Security で作成されたタスクの表示
- Kaspersky Security Center で作成されたタスクのクライアントデバイスでの表示

Web コンソールでのポリシーの設定

Web コンソールでは、ポリシーのプロパティ（**製品設定 → ローカルタスク → タスク管理**）でタスクを表示する権限を設定できます。

タスク管理の設定

設定	説明
ローカルタスクの表示と管理をユーザーに許可する	このチェックボックスでは、Kaspersky Endpoint Security で作成されたローカルタスクの表示と、管理対象クライアントデバイスでのこれらタスクの管理を、ユーザーに対して許可またはブロックすることができます。 既定では、このチェックボックスはオフです。
KSC で作成されたタスクの表示と管理をユーザーに許可する	このチェックボックスを使用すると、Kaspersky Security Center Web コンソールで作成したタスクの表示、管理対象クライアントデバイスでのこれらのタスクの管理をユーザーに対して許可または禁止することができます。 既定では、このチェックボックスはオフです。

管理コンソールでのポリシーの設定

管理コンソールでは、ポリシーのプロパティ（**ローカルタスク → タスク管理**）でタスクを表示する権限を設定できます。

タスク管理の設定

設定	説明
ローカルタスクの表示と管理をユーザーに許可する	このチェックボックスでは、Kaspersky Endpoint Security で作成されたローカルタスクの表示と、管理対象クライアントデバイスでのこれらタスクの管理を、ユーザーに対して許可またはブロックすることができます。

	既定では、このチェックボックスはオフです。
KSC で作成されたタスクの表示と管理をユーザーに許可する	このチェックボックスで、Kaspersky Security Center で作成されたタスクの表示と、管理対象クライアントデバイスでのそれらの管理を、ユーザーに対して許可または禁止することができます。 既定では、このチェックボックスはオフです。

バックアップ

Kaspersky Endpoint Security が保護されたデバイスのスキャン中にファイル内に悪意のあるコードを検知した場合、アプリケーションはファイルをブロックし、ファイルに*感染*ステータスを割り当て、バックアップにコピーを配置して、ファイルの駆除を試みることができます。

*バックアップ*では、駆除中に削除または変更されたファイルのコピーが保存されます。ファイルを駆除または削除する前に、*バックアップコピー*が作成されます。ファイルのバックアップコピーは特別な形式で保存され、脅威となることはありません。

ファイルが正常に駆除されると、バックアップコピーのステータスが*駆除済み*に変わります。駆除中に、ファイルの整合性を維持できないことがあります。駆除後に、駆除されたファイルの重要な情報に部分的または完全にアクセスできなくなった場合は、駆除されたファイルのコピーから、元のディレクトリへのファイルの復元を試行できます。

ファイルのステータスが*駆除済み*である場合にのみ、バックアップコピーからファイルを復元することをお勧めします。感染しているオブジェクトを復元すると、デバイスへの感染の原因となる可能性があります。

バックアップファイルのコピーには個人データが含まれる場合があります。バックアップオブジェクトにアクセスするには、root 権限が必要です。

次のバックアップ設定を行うことができます：

- バックアップのオブジェクトの保管期間。オブジェクトは既定で 90 日間保管されます。
- バックアップの最大サイズ。バックアップは既定で無制限のサイズに対応しています。
- バックアップへのパス。既定では、バックアップ保管領域はディレクトリ /var/opt/kaspersky/kesl/common/objects-backup/ にあります。

指定された保持期間が経過するか、バックアップの最大サイズに達すると、アプリケーションはステータスに関係なくバックアップコピーを自動的に削除します。

復元されたファイルまたは復元されていないファイルのバックアップコピーを手動で削除できます。

クライアントデバイス上のカスペルスキーのアプリケーションによるバックアップに配置されるファイルの一般的なリストは、Kaspersky Security Center で生成され、管理コンソール（**詳細設定 → 保管領域 → バックアップ**）および Web コンソール（**動作 → 保管領域 → バックアップ**）で利用できます。保護されたデバイス上のバックアップコピーのプロパティを表示したり、バックアップでマルウェアのスキャンを実行したり、ファイルを削除したりできます。Kaspersky Security Center は、バックアップから管理サーバーにファイルをコピーしません。すべてのファイルは、保護対象デバイスのバックアップ保管領域に保存されます。ファイルの復元は保護対象デバイス上で行われます。

Web コンソールでのバックアップの設定

Web コンソールでは、ポリシーのプロパティ（**製品設定 → 全般設定 → 保管領域設定**）でバックアップ設定を構成できます。

バックアップ設定

設定	説明
バックアップ内のファイル	この切り替えボタンでは、バックアップ保管領域のファイルについての

に関する通知が有効/無効	通知を管理サーバーに送信するかどうかを選択します。 この切り替えボタンは既定でオンになっています。
オブジェクトの保存期間（日）	バックアップの保管領域にオブジェクトを保存する期間を指定する入力フィールド。 使用できる値：0～3653。 既定値：900 を指定すると、バックアップ保管領域でのオブジェクトの保存期間は無制限になります。
バックアップのサイズを制限する（MB）	バックアップ保管領域の最大サイズ（MB単位）を指定する入力フィールド。 使用できる値：0 ～ 999999。既定値：0（無制限）。

管理コンソールでのバックアップの設定

管理コンソールでは、ポリシーのプロパティ（**全般設定 → 保管領域設定**）でバックアップ設定を構成できます。

バックアップ設定

設定	説明
バックアップに関するファイルについて通知する	このチェックボックスでは、バックアップ保管領域のファイルについての通知を管理サーバーに送信するかどうかを選択します。 既定では、このチェックボックスはオンです。
オブジェクトの保存期間（日）	このチェックボックスは、バックアップ保管領域内のオブジェクトの保存期間制限（日単位）を有効または無効にします。 使用できる値：0～3653。 既定値：900 を指定すると、バックアップ保管領域でのオブジェクトの保存期間は無制限になります。
バックアップのサイズを制限する（MB）	このチェックボックスは、バックアップ保管領域の最大サイズ（メガバイト単位）を有効または無効にします。 使用できる値：0 ～ 999999。既定値：0（無制限）。

コマンドラインでのバックアップの設定

*バックアップ*の事前定義済みタスクを使用して、コマンドラインでバックアップを構成できます。

バックアップ管理タスクは既定で開始されます。手動で開始および停止できません。

バックアップの管理の事前定義済みタスクの設定を編集することで、バックアップを設定できます。

バックアップの管理タスクの設定

設定	説明	値
`DaysToLive`	バックアップの保管領域にオブジェクトを保存する期間（日単位）。 オブジェクトの保持制限を削除するには、0 を設定します。	0: 無制限の保持。 既定値：90

`BackupSizeLimit`	最大バックアップサイズ（MB単位）。バックアップの保管領域の最大サイズに到達すると、最も古いオブジェクトが削除されます。 バックアップのサイズ制限を削除するには、0 を設定します。	0 ～ 999999 0: 無制限のサイズ。 既定値：0
`BackupFolder`	バックアップディレクトリのパス。既定のディレクトリとは異なるカスタムのバックアップの保管領域のディレクトリを指定できます。任意のコンピューターのディレクトリをバックアップの保管領域として使用できます。Samba プロトコルや NFS プロトコルでマウントされているような、リモートデバイスにあるディレクトリは割り当てないでください。 設定を変更して Kaspersky Endpoint Security を再起動した後、Kaspersky Endpoint Security は指定されたディレクトリへオブジェクトの移動を開始します。 指定したディレクトリが存在しない、または使用できない場合、既定のディレクトリが使用されます。	既定値：/var/opt/kaspersky/kesl/common/objects-backup/ 既定のバックアップの保管領域のディレクトリにアクセスするには、root 権限が必要です。

コマンドラインでのバックアップオブジェクトの操作

コマンドラインでバックアップ管理コマンドを使用して、バックアップオブジェクトに対して次の処理を実行できます：

- バックアップオブジェクトの詳細を表示します。
- バックアップから一部または全部のオブジェクトを削除します。
- バックアップからオブジェクトを復元します。

感染しているオブジェクトを復元すると、デバイスへの感染の原因となる可能性があります。

バックアップオブジェクトの詳細の表示

バックアップのオブジェクトの詳細を表示するには、次のコマンドを実行します：

```
kesl-control -B --query ["<フィルター条件>"] [-n <数値>] [--json]
```

説明：

- <フィルター条件>：<フィールド> <比較演算子> '<値>' 形式の1つまたは複数の論理式。論理演算子と組み合わせて、結果を限定します。 フィルター条件を指定しない場合、バックアップ内のすべてのオブジェクトの詳細を表示します。

- <数値>：表示する最新のオブジェクトの数。 -n スイッチを指定しない場合は、最後の 30 個のオブジェクトが表示されます。0 を指定してすべてのオブジェクトを表示します。

- --json：データを JSON 形式で出力します。

ObjectId 行には、オブジェクトをバックアップに配置するときにオブジェクトに割り当てた数値識別子が表示されます。ID は、オブジェクトをバックアップ保管領域から復元または削除するなど、オブジェクトに対して処理を実行する場合に使用されます。

バックアップからのオブジェクトの復元

オブジェクトを元の名前で元の場所に復元するには、次のコマンドを実行します：

```
kesl-control --restore <オブジェクト ID>
```

<オブジェクト ID> は、オブジェクトをバックアップに配置するときにオブジェクトに割り当てた数値識別子です。

オブジェクトを新しい名前で指定したディレクトリに復元するには、次のコマンドを実行します：

```
kesl-control --restore <オブジェクト ID> --file <ファイル名とパス>
```

--file <ファイル名とパス> は、ファイルの新しい名前と、ファイルを保存するディレクトリへのパスです。指定されたディレクトリが存在しない場合は、ディレクトリが作成されます。

バックアップからのオブジェクトの削除

選択したオブジェクトをバックアップから削除するには、次のコマンドを実行します：

```
kesl-control --mass-remove --query "<フィルター条件>"
```

<フィルター条件>は、<フィールド> <比較演算子> '<値>' 形式の1つまたは複数の論理式。論理演算子と組み合わせて、結果を限定します。

例：
ID=15 のオブジェクトを削除するには：

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

名前またはパスに「test」を含むオブジェクトを削除するには：

```
kesl-control -B --mass-remove --query "FileName like '%test%'"
```

すべてのオブジェクトをバックアップから削除するには、次のコマンドを実行します：

```
kesl-control -B --mass-remove
```

Detection and Response ソリューションとの連携

カスペルスキーの Detection and Response ソリューションは、組織のインフラストラクチャの様々なレベルで高度な脅威や攻撃の兆候を検知するように設計されたセキュリティシステムです。検知および対応ソリューションは、検知された脅威に関する情報を提供し、検知への対応を管理します。

Kaspersky Endpoint Security は、次の Kaspersky Detection and Response ソリューションと相互運用できます：

- Kaspersky Anti Targeted Attack Platform (Kaspersky Endpoint Detection and Response コンポーネント)Kaspersky Endpoint Detection and Response (KATA) との連携は、Kaspersky Endpoint Security コンポーネントで Endpoint Detection and Response (KATA) (EDR (KATA)) によって促進されます。
- Kaspersky Endpoint Detection and Response Optimum連携は、Kaspersky Endpoint Security コンポーネントである Endpoint Detection and Response Optimum (EDR Optimum) によって促進されます。
- Kaspersky Managed Detection and Response連携は、Kaspersky Endpoint Security コンポーネントである Managed Detection and Response (MDR) によって促進されます。

Kaspersky Endpoint Security と Kaspersky Managed Detection and Response および Kaspersky Anti Targeted Attack Platform が連携されている場合、systemd ログに大量のイベントが書き込まれる可能性があります。監査イベントのログ記録を無効にする場合、systemd-journald-audit ソケットを無効にし、オペレーティングシステムを再起動します。

systemd-journald-audit ソケットを無効にするには、次のコマンドを実行します：

```
systemctl stop systemd-journald-audit.socket

systemctl disable systemd-journald-audit.socket

systemctl mask systemd-journald-audit.socket
```

既定では、SintezM-Client オペレーティングシステムでは、auditd サービスの設定は変更から保護されており、`enabled 2` モードになっています。Kaspersky Endpoint Security が Kaspersky Managed Detection and Response および Kaspersky Anti Targeted Attack Platform ソリューションと連携されている場合にふるまい検知コンポーネントを正しく動作させるには、設定情報ファイルの auditd モードを `enabled 1`（設定ブロックなし）に変更し、オペレーティングシステムを再起動します。

Detection and Response ソリューションのコマンドに対する応答処理について

Kaspersky Endpoint Security は、セキュリティ機能の提供を目的とした応答処理を実行できます。

- Kaspersky Endpoint Detection and Response (KATA) と対話する場合は、Kaspersky Anti Targeted Attack Platform ソリューションのコンポーネントです。
- Kaspersky Endpoint Detection and Response Optimum と対話する場合：

Kaspersky Anti Targeted Attack Platform と Kaspersky Endpoint Detection and Response Optimum の応答処理設定は異なります。

Kaspersky Endpoint Security は次の応答処理を実行できます：

- デバイスからファイルを取得します。

  この処理は、*ファイルの取得*タスクを使用して実行されます。たとえば、サードパーティのプログラムによって生成されたイベントログファイルを取得するようにアプリケーションを設定できます。

- デバイスからファイルを削除します。

  この処理は、*ファイルの削除*タスクを使用して実行されます。

- デバイス上でプロセスをリモートで実行します。

  この処理は、*プロセスの実行*タスクを使用して実行されます。

  たとえば、デバイスの設定情報ファイルを作成するユーティリティをリモートで実行し、*ファイルの取得*タスクでファイルを取得します。

- デバイス上のプロセスをリモートで終了します。

  この処理は、*プロセスの終了*タスクを使用して実行されます。

  たとえば、「プロセスの実行」タスクを使用して起動されたインターネットスピードテストユーティリティをリモートで終了できます。

- デバイス上の*侵害の兆候*を検出し、脅威への対応処理を実行します。

  この処理は、*IOC スキャン*タスクを使用して実行されます。

  *IOC スキャン*タスクは、オペレーティングシステムの主要な名前空間でのみ、IOC 用語（IOC オブジェクトのプロパティ、たとえばファイルハッシュ）をチェックします。*IOC スキャン*タスクでは、200 MB を超えるファイルのハッシュは計算されません。

- デバイスのネットワーク分離を有効または無効にします。

  Kaspersky Endpoint Security が Kaspersky Endpoint Detection and Response Optimum と連携すると、次の操作が可能になります：

  - Web コンソールでのネットワーク分離の有効化または無効化
  - コマンドラインでのネットワーク分離の無効にします。
  - Web コンソールでネットワーク分離の自動無効化を設定します。

  Kaspersky Endpoint Security が Kaspersky Endpoint Detection and Response (KATA) と連携すると、次の操作が可能になります：

  - コマンドラインでのネットワーク分離の無効にします。
  - Kaspersky Endpoint Detection and Response (KATA) ソリューションでネットワーク分離を有効または無効にします。

    詳細は、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

ネットワーク分離の制限

ネットワーク分離を使用する時は、以下に説明する制限をよく理解しておくことを強く推奨します。

ネットワーク分離を行うには、Kaspersky Endpoint Security が実行されている必要があります。Kaspersky Endpoint Security に不具合がある場合（かつアプリケーションが実行されていない場合）、 Kaspersky Anti Targeted Attack Platform または Kaspersky Endpoint Detection and Response Optimum によってネットワーク分離が有効になっていると、トラフィックのブロックは保証されません。

ネットワーク分離が有効になっているトランジットトラフィックは制限付きでサポートされており、フィルタリングされる場合があります。

DHCP と DNS はネットワーク分離の例外に自動的に追加されないため、ネットワーク分離中に発生源のネットワークアドレスが変更された場合、Kaspersky Endpoint Security はその発生源にアクセスできなくなります。フォールトトレラント KATA サーバーのノードにも同じことが当てはまります。Kaspersky Endpoint Security との連絡が途絶えないように、アドレスを変更しないことを推奨します。

また、プロキシサーバーはネットワーク分離の除外対象に自動的に追加されないため、Kaspersky Endpoint Security が KATA サーバーとの接続を失わないように、手動で除外対象に追加する必要があります。

プロセスをネットワーク分離に追加したり、名前でプロセスをネットワーク分離から除外したりすることはサポートされていません。

Kaspersky Endpoint Security を標準モードで使用する場合、ネットワーク分離を使用するときは次の操作を実行することを推奨します：

- Kaspersky Security Network と対話するには、KSN プロキシサーバーを使用します。
- Kaspersky Security Center を製品のアクティベーションのプロキシサーバーとして使用します。

  Kaspersky Security Center をプロキシサーバーとして使用できない場合は、必要なプロキシサーバーの設定を設定し、除外に追加してください。
- データベース更新ソースとして Kaspersky Security Center を指定します。

これらの推奨事項は、Kaspersky Endpoint Security が Light Agent モードで使用される場合には適用されません。

Kaspersky Endpoint Detection and Response（KATA）統合

Kaspersky Endpoint Detection and Response (KATA) は、Kaspersky Anti Targeted Attack Platform ソリューションのコンポーネントです。Kaspersky Endpoint Detection and Response (KATA) コンポーネントとの連携は、Kaspersky Endpoint Security コンポーネントである Endpoint Detection and Response (KATA) (EDR (KATA)) によって促進されます。

Kaspersky Endpoint Security は、組織の IT インフラを保護し、ゼロデイ攻撃、標的型攻撃、高度持続型脅威（APT）などの脅威をプロンプトリーに検知することを目的とした Kaspersky Anti Targeted Attack Platform ソリューションと互換性があります。詳細は、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

この機能は、KESL コンテナではサポートされていません。

Kaspersky Endpoint Detection and Response (KATA) と対話する場合、Kaspersky Endpoint Security では次の操作が可能になります：

- デバイス上のイベントに関するデータ（テレメトリ）を、セントラルノードコンポーネントのある Kaspersky Anti Targeted Attack Platform サーバー（「KATA サーバー」）に送信します。Kaspersky Endpoint Security は、プロセス、オープンネットワーク接続、変更されたファイルに関する監視データを、KATA サーバーに送信するとともに、アプリケーションが検知した脅威のデータと脅威の処理結果のデータを送信します。

- Kaspersky Anti Targeted Attack Platform からコマンドを受信したときに、応答処理を実行してセキュリティを確保します。

Kaspersky Endpoint Detection and Response (KATA) との連携には、ふるまい検知コンポーネントを有効にする必要があります。

Kaspersky Endpoint Security アプリケーションと Kaspersky Endpoint Security および EDR (KATA) の連携は、ふるまい検知が有効になっている場合にのみ可能です。そうしないと、必要なテレメトリーデータを送信することができません。

Kaspersky Endpoint Detection and Response (KATA) は、さらに次のコンポーネントから受信したデータを使用できます：

- ファイル脅威対策。

- ネットワーク脅威対策。

- ウェブ脅威対策。

Kaspersky Managed Detection and Response との連携では、Kaspersky Endpoint Security を搭載したデバイスは、HTTPS プロトコルで KATA サーバーとの安全な接続を確立します。安全な接続を実現するため、KATA サーバーが発行する次の証明書を使用しています：

- KATA サーバー証明書。接続はサーバーの TLS 証明書を使用して暗号化されます。接続のセキュリティレベルは、Kaspersky Endpoint Security 側のサーバー証明書を検証することで上げられます。Kaspersky Managed Detection and Response (KATA) との連携を有効にする前に、連携サーバー証明書を追加します。

- クライアント証明書。この証明書は、双方向認証を使用した接続の追加保護に使用されます（Kaspersky Endpoint Security KATA サーバーを使用するスキャンデバイス）。同一のクライアント証明書を複数のデバイスで使用することができます。既定では、KATA サーバーはクライアント証明書をチェックしませんが、Kaspersky Anti Targeted Attack Platform 側で双方向認証を有効にすることができます。この場合、Kaspersky Managed Detection and Response (KATA) との連携設定で双方向認証を有効にし、クライアント証明書（証明書と秘密鍵の入った暗号コンテナ）を追加する必要があります。

KATA サーバーとの接続を確保するための証明書は、Kaspersky Anti Targeted Attack Platform の管理者から提供されます。

Kaspersky Endpoint Security のアプリケーション全般設定で、プロキシサーバーの使用が設定されている場合、KATA サーバーへの接続にプロキシサーバーが使用されます。

既定では、 Kaspersky Endpoint Detection and Response (KATA) の連携は無効になっています。コマンドライン、Web コンソール、および管理コンソールを使用して、連携を有効または無効にし、次の連携設定を構成できます。

- KATA サーバー接続の全般設定を構成します。

- KATA サーバー証明書を追加または削除します。

- KATA サーバーに接続するときに双方向認証を設定し、クライアント証明書を追加します。

- イベントの転送を設定します。
- テレメトリーの送信を有効または無効にします。

> Kaspersky Endpoint Security と Kaspersky Managed Detection and Response の統合が有効になっている場合、テレメトリーの送信の際はプロセスの除外は適用されません。

Kaspersky Security Center Cloud コンソールでのKaspersky Endpoint Detection and Response (KATA) の連携設定の管理には対応していません。

Web コンソールで Kaspersky Endpoint Detection and Response (KATA) の連携の設定

Web コンソールでは、Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response (KATA) の連携を有効または無効にし、ポリシーのプロパティ（**製品設定 → Detection and Response → Endpoint Detection and Response (KATA)**）で連携の設定を構成できます。

Kaspersky Security Center Cloud コンソールでのKaspersky Endpoint Detection and Response (KATA) の連携設定の管理には対応していません。

Kaspersky Endpoint Detection and Response（KATA）連携設定

設定	説明
Endpoint Detection and Response (KATA) は有効/無効になっています	Kaspersky Endpoint Security アプリケーションと Kaspersky Endpoint Detection and Response (KATA) の連携を有効または無効にします。 連携サーバーは、既定でオフになっています。
サーバー接続設定	**設定**リンクをクリックすると、KATA サーバーに接続するための全般設定を設定したり、サーバー証明書を追加したり、KATA サーバーへの接続に関して二要素認証を設定したりできるウィンドウが開きます。
KATA サーバー	この表には、接続が設定されている KATA サーバーのリストが含まれています。 ［**追加**］を押すと、KATA サーバーへの接続を設定するウィンドウが開きます。 以前に設定した接続設定の編集および削除は、表の上にあるボタンを使用して行えます。
イベント送信時の最大遅延（秒）	KATA サーバーにイベントを送信する際の最大遅延時間（秒）。 既定値は `30` です。
イベントスロットリングをオンにする	KATA サーバーに送信されるイベント数の規制をオンまたはオフにします。
1時間あたりの最大イベント数	1時間あたりの最大イベント数 既定値は `3000` です。
イベントスロットルのしきい値（%）	イベントスロットルの閾値（パーセント）。イベントの総数に占める1種類のイベント（たとえば、レジストリ変更に関するイベントなど）の割合が設定した閾値（割合）を超えた場合、イベントの送信を制限します。

	既定値は 15 です。

[サーバー接続設定] ウィンドウ

このウィンドウでは、KATA サーバーに接続するための全般設定を設定したり、サーバー証明書を追加したり、KATA サーバーへの接続に関して二要素認証を設定したりできます。

KATA サーバー接続設定

設定	説明
KATA サーバーに同期リクエストを送信する間隔（分）	KATA サーバーへの同期リクエストの送信頻度（分）。 既定値は 5 です。
サーバーとの接続を待つ最大時間（秒）	KATA サーバーへの接続を待つ最大時間（秒）。 既定値は 10 です。
サーバーからの応答を待つ最大時間（秒）	KATA サーバーからの応答を待つ最大時間（秒）。 既定値は 10 です。
テレメトリの送信を許可する	デバイスのイベントに関するデータ（テレメトリ）の KATA サーバーへの送信をオンまたはオフにします。 既定で、テレメトリーの送信はオンです。
サーバー証明書	サーバー証明書の追加後、証明書に関する情報が表示されます： • 証明書のシリアル番号 • 証明書のサブジェクト • 証明書の発行者 • 証明書の開始日 • 証明書の有効期間が終了する日
選択	標準のファイル選択ウィンドウを開き、KATA サーバー証明書のパスを指定することができます。 サーバー証明書が追加されている場合、サーバー証明書は Kaspersky Endpoint Security 側で検証されます。これで接続のセキュリティレベルが上がります。
Remove	以前に追加したサーバー証明書を削除します。 このボタンはサーバー証明書が追加済みの場合にのみ表示されます。
追加接続保護	設定セクションでは、KATA サーバーに接続する際の双方向認証のオンまたはオフの設定や、クライアント証明書の追加を行うことができます。
二要素認証を使用する	KATA サーバーへの接続をさらに安全にするために、双方向認証の使用をオンまたはオフにします。 KATA サーバー側で双方向認証がオンになっている必要があります。

	二要素認証を使用するためには、クライアント証明書を追加する必要があります。
クライアント証明書を追加する	標準のファイル選択ウィンドウを開き、クライアント証明書と秘密鍵の入った暗号化コンテナ（PFX archive）へのパスを指定します。 このボタンは［**二要素認証を使用する**］がオンの時に使用可能です。
編集	クライアント証明書を含む暗号コンテナのパスワードを指定できるようになります。「**Cryptocontainer のパスワード**」フィールドは編集できません。既定では、このパスワードは空です。 パスワードを指定するには、［**編集**］をクリックします。開いたウィンドウにパスワードを入力し、［**OK**］をクリックします。［パスワード入力］ウィンドウの、パスワードが見えるように表示されたウィンドウで［**表示**］をクリックします。 パスワードの複雑性とブルートフォース攻撃防止メカニズムにより、6か月以内にパスワードが推測できないようにすることを推奨します。 このボタンは［**二要素認証を使用する**］がオンの時に使用可能です。

KATA サーバーに接続するための設定ウィンドウ

このウィンドウでは、KATA サーバーへの接続設定を指定することができます。

KATA サーバー接続設定

設定	説明
アドレス	KATA サーバーアドレス　連携サーバーの IP アドレス（IPv4 または IPv6）または完全修飾ドメイン名（FQDN）を指定することができます。 デバイスのネットワーク分離が有効になっている時にアプリケーションが失敗した場合でも、KATA サーバーとの通信が中断されないように、サーバーの IP アドレスを指定することを推奨します。 既定値：`127.0.0.1`。
Port	KATA サーバーに接続するためのポート。 既定値は `443` です。

管理コンソールで Kaspersky Endpoint Detection and Response (KATA) の連携の設定

Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response (KATA) の連携は、管理コンソールのポリシーのプロパティで有効化、無効化、または設定できます（**Detection and Response → Endpoint Detection and Response (KATA)**）。

Kaspersky Endpoint Detection and Response（KATA）連携設定

設定	説明
Endpoint Detection and Response（KATA）との連携。	Kaspersky Endpoint Security アプリケーションと Kaspersky Endpoint Detection and Response (KATA) の連携を有効または無効にします。 連携サーバーは、既定でオフになっています。
KATA サーバー	**設定**ボタンをクリックすると**KATA サーバー**ウィンドウが開きます。このウィン

	ドウでは、KATA サーバーへの接続を設定したり、接続設定先のサーバーのリストを確認したりできます。
サーバー接続設定	**設定**ボタンをクリックすると、KATA サーバーに接続するための全般設定を設定したり、サーバー証明書を追加したり、KATA サーバーへの接続に関して二要素認証を設定したりできるウィンドウが開きます。
データ転送設定	**設定**ボタンをクリックすると、ウィンドウが開き、KATA サーバーへのデータ設定を行えます。

［KATA サーバー］ウインドウ

ウィンドウ内の表には KATA サーバーに接続するための設定のリストが表示されています。表には、接続が設定された各サーバーについて、IP アドレス（IPv4 または IPv6）またはサーバーの完全修飾ドメイン名（FQDN）およびポートが表示されています。

ボタンおよび表上にあるメニューを使用して次の処理を実行できます：

- KATA サーバー接続設定の追加
- 以前に設定した接続設定の編集または削除
- 設定した接続設定のリストのエクスポートまたはインポート

KATA サーバーに接続するための設定ウィンドウ

このウィンドウでは、KATA サーバーへの接続設定を指定することができます。

KATA サーバー接続設定

設定	説明
アドレス	KATA サーバーアドレス　連携サーバーの IP アドレス（IPv4 または IPv6）または完全修飾ドメイン名（FQDN）を指定することができます。 デバイスのネットワーク分離が有効になっている時にアプリケーションが失敗した場合でも、KATA サーバーとの通信が中断されないように、サーバーの IP アドレスを指定することを推奨します。 既定値：`127.0.0.1`。
Port	KATA サーバーに接続するためのポート。 既定値は 443 です。

［サーバー接続設定］ウィンドウ

このウィンドウでは、KATA サーバーに接続するための全般設定を設定できます。

KATA サーバー接続設定

設定	説明
KATA サーバーに同期リクエストを送信する間隔	KATA サーバーへの同期リクエストの送信頻度（分）。

（分）	既定値：5
サーバーとの接続を待つ最大時間（秒）	KATA サーバーへの接続を待つ最大時間（秒）。 既定値は 10 です。
サーバーからの応答を待つ最大時間（秒）	KATA サーバーからの応答を待つ最大時間（秒）。 既定値は 10 です。
テレメトリの送信を許可する	デバイスのイベントに関するデータ（テレメトリ）の KATA サーバーへの送信をオンまたはオフにします。 既定で、テレメトリーの送信はオンです。
二要素認証を使用する	KATA サーバーへの接続をさらに安全にするために、双方向認証の使用をオンまたはオフにします。 二要素認証を使用するためには、クライアント証明書を追加する必要があります。 KATA サーバー側で双方向認証がオンになっている必要があります。
クライアント証明書の**追加**	KATA サーバーとの接続のためのセキュリティを強化するための［クライアント証明書を追加する］ウィンドウが開きます。 このボタンはクライアント証明書が追加されていない場合に表示されます。 接続用の追加保護を設定する場合、KATA サーバー側でクライアント証明書の認証を有効にし、このウィンドウで［**二要素認証を使用する**］をオンにします。
クライアント証明書の**削除**	クライアント証明書を削除する。 このボタンはクライアント証明書が追加されている場合に表示されます。
追加（サーバー証明書）	［サーバー証明書の追加］ウィンドウが開きます。 このボタンはサーバー証明書が追加されていない場合に表示されます。
サーバー証明書の**削除**	サーバー証明書を削除する。 このボタンはサーバー証明書が追加済みの場合にのみ表示されます。

［サーバー証明書の追加］ウィンドウ

このウィンドウでは、次のいずれかの方法で KATA サーバー証明書を追加できます：

- ［**ファイルから追加**］フィールドで証明書ファイルへのパスを指定します。［**参照**］をクリックすると、標準のファイル選択ウィンドウが表示されます。証明書を含むファイル（DER または PEM 形式）へのパスを指定します。
- ［**証明書の詳細を入力**］フィールドに証明書ファイルの内容をコピーします。

サーバー証明書が追加されている場合、サーバー証明書は Kaspersky Endpoint Security 側で検証されます。これで接続のセキュリティレベルが上がります。

［クライアント証明書の追加］ウィンドウ

このウィンドウでは、クライアント証明書を追加することで KATA サーバーとの接続をよりセキュアにできます。

接続に追加の保護を設定する場合、KATA サーバー側でクライアント証明書の検証を有効にし、「サーバー接続設定」ウィンドウで［**二要素認証を使用する**］をオンにします。

クライアント証明書を追加するには、クライアント証明書および秘密鍵を含む暗号コンテナ（PFX アーカ）へのパスを指定します。［**参照**］をクリックすると、標準のファイル選択ウィンドウが表示されます。アーカイブがパスワードで保護されている場合、［**Cryptocontainer のパスワード**］フィールドにパスワードを入力します。

［データ転送設定］ウィンドウ

このウィンドウでは、KATA サーバーにデータを送信するための設定を設定できます。

KATA サーバーへのデータ送信設定

設定	説明
イベント送信時の最大遅延（秒）	KATA サーバーにイベントを送信する際の最大遅延時間（秒）。 既定値は `30` です。
イベントスロットリングをオンにする	KATA サーバーに送信されるイベント数の規制をオンまたはオフにします。
1時間あたりの最大イベント数	1時間あたりの最大イベント数 既定値は `3000` です。
イベントスロットルのしきい値（%）	イベントスロットルの閾値（パーセント）。イベントの総数に占める1種類のイベント（たとえば、レジストリ変更に関するイベントなど）の割合が設定した閾値（割合）を超えた場合、イベントの送信を制限します。 既定値は `15` です。

コマンドラインで Kaspersky Endpoint Detection and Response (KATA) の連携の設定

Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response (KATA) の連携は、Kaspersky Endpoint Detection and Response (KATA) Integration (*KATAEDR*) の事前定義済みタスクを使用してコマンドラインで管理できます。

Kaspersky Endpoint Detection and Response (KATA) との連携はデフォルトでは実行されません。このタスクは、手動で開始および停止できます。

事前定義済みタスクの設定を編集することで、Kaspersky Endpoint Detection and Response (KATA) の連携設定を構成できます。

Kaspersky Endpoint Detection and Response (KATA) との連携の設定を管理するコマンドを使用して、KATA サーバーへの接続に使用する証明書を管理できます。

Kaspersky Endpoint Detection and Response（KATA）との連携タスク設定

この表では、Kaspersky Managed Detection and Response（KATA）との連携タスクで指定できるすべての設定と、その既定値について説明します。

Kaspersky Endpoint Detection and Response（KATA）との連携タスク設定

設定	説明	値
アドレス	KATA サーバーのアドレス Integration Server の IP アドレス（IPv4 または IPv6）または完全修飾ドメイン名（FQDN）を指定することができます。 デバイスのネットワーク分離が有効になっている時にアプリケーションが失敗した場合でも、KATA サーバーとの通信が中断されないように、サーバーの IP アドレスを指定することを推奨します。	既定値：`127.0.0.1`。
`Port`	KATA サーバーに接続するためのポート。	既定値は `443` です。
`UseClientPinnedCertificate`	KATA サーバーへの接続をさらに安全にするために、双方向認証をオンまたはオフにします。 KATA サーバー側で双方向認証が有効な場合、タスクを開始する前に、Kaspersky Endpoint Detection and Response（KATA）との連携のタスクの設定で双方向認証を有効にし、クライアント証明書を追加する必要があります。	`Yes` – KATA サーバーとの接続をさらに安全にするために、二要素認証を使用します。 `No`（既定値）- 二要素認証は使用しません。
`SynchronizationPeriod`	KATA サーバーへの同期リクエストの送信頻度（分）。	既定値は `5` です。
`ConnectionTimeout`	KATA サーバーへの接続を待つ最大時間（秒）。	既定値は `10` です。
`RequestTimeout`	KATA サーバーからの応答を待つ時間（秒）。	既定値は `10` です。
`MaximumDataTransferTime`	KATA サーバーにイベントを送信する際の最大遅延時間（秒）。	既定値は `30` です。
`UseRequestCountLimits`	KATA サーバーに送信されるイベント数の規制をオンまたはオフにします。	`Yes`（既定値）- 送信されるイベント数を規制します。 `No` – イベント数を規制しません。
`MaximumNumberOfEventsInHour`	1 時間あたりの最大イベント数	既定値は `3000` です。
`EventLimitExceededPercentage`	イベントスロットルの閾値（パーセント）。特定のタイプのイベントの総数に対する比率が設定されたしきい値（パーセンテージ）を	既定値は `15` です。

	超える場合、イベントの送信は制限されます。	
`EnableTelemetry`	KATA サーバーへのイベントデータ（テレメトリ）の送信をオンおよびオフにします。	`Yes`（既定値）– KATA サーバーにテレメトリを送信します。 `No` – テレメトリを送信しません。

KATA サーバーに接続するための証明書の管理

証明書を管理するには、root 権限が必要です。

KATA サーバーへの接続に使用する証明書を、コマンドを使用して管理することができます。証明書で可能なこと：

- サーバー証明書を追加または交換する
- サーバー証明書に関する情報を表示する
- サーバー証明書を削除する
- クライアント証明書を追加または交換する
- クライアント証明書に関する情報を表示する
- クライアント証明書を削除する

サーバー証明書を追加または交換する場合は、次のコマンドを実行します：

```
kesl-control [-R] --add-kataedr-server-certificate <ファイル名とパス>
```

<ファイル名とパス>は、サーバー証明書を含むファイルの名前とパスです。

クライアント証明書を追加または変更するには：

1. コマンドを実行します：

   ```
   kesl-control [-R] --add-kataedr-client-certificate <ファイル名とパス>
   ```

   <ファイル名とパス>は、クライアント証明書と秘密鍵を含む暗号コンテナ（PFX アーカイブ）の名前とパスです。

2. 暗号コンテナがパスワードで保護されている場合、要求されたらパスワードを入力します。

KATA サーバーの設定でクライアント証明書の検証を有効にし、［Kaspersky Endpoint Detection and Response (KATA) との連携のタスク設定で `UseClientPinnedCertificate` の設定に `yes` 値が設定されている場合、クライアント証明書は KATA サーバーへの接続の追加保護に使用されます。

証明書情報を表示するには、次のコマンドを実行します：

- サーバー証明書の場合：

  `kesl-control [-R] --query-kataedr-server-certificate`

- クライアント証明書の場合：

  `kesl-control [-R] --query-kataedr-client-certificate`

コマンドを実行すると、次のような証明書情報が表示されます：

- 証明書のシリアル番号
- 証明書のサブジェクト
- 証明書の発行者
- 証明書の開始日
- 証明書の有効期間が終了する日
- SHA1 および SHA256 証明書のフィンガープリント

サーバー証明書情報を削除するには、次のコマンドを実行します：

```
kesl-control [-R] --remove-kataedr-server-certificate
```

クライアント証明書情報を削除するには、次のコマンドを実行します：

```
kesl-control [-R] --remove-kataedr-client-certificate
```

Kaspersky Endpoint Detection and Response（KATA）との連携のタスクの設定で証明書の使用が設定されており、タスクが実行されている場合、この証明書の削除はエラーで終了します。

Kaspersky Endpoint Detection and Response Optimumの連携

Kaspersky Endpoint Detection and Response Optimum は、エクスプロイト、ランサムウェア、ファイルレス攻撃、デバイスやデータを侵害するために攻撃者が使用する正規のシステムツールなどの脅威から組織の IT インフラストラクチャを保護するソリューションです。

Kaspersky Endpoint Detection and Response Optimum は、脅威の進化を監視および分析し、潜在的な攻撃に関する情報をセキュリティ担当者または管理者に提供して、適切なタイミングで対応処理を実行できるようにします。

Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response Optimum ソリューションの連携は、Kaspersky Endpoint Security コンポーネントである Endpoint Detection and Response Optimum (EDR Optimum) によって促進されます。

Kaspersky Endpoint Security 12.1 for Linux は、Kaspersky Endpoint Detection and Response Optimum バージョン 3.0 と互換性があります。

Kaspersky Endpoint Security for Linux の12.1 より前のバージョンには、EDR Optimum コンポーネントは含まれていません。

Kaspersky Endpoint Detection and Response Optimum は、次の脅威インテリジェンスツールを使用します。

- Kaspersky Security Network（以降「KSN」とも表記）は、カスペルスキーのファイル、Web サイト、ソフトウェアレピュテーションのオンラインナレッジ ベースへのアクセスを提供するクラウドサービスインフラストラクチャです。
- ファイルと Web サイトのレピュテーションに関する情報を格納および表示する Kaspersky Threat Intelligence Portal との連携。
- Kaspersky Threats データベース。

Kaspersky Endpoint Detection and Response Optimum と対話する場合、Kaspersky Endpoint Security では次の操作が可能になります：

- デバイス上のイベントに関するデータを Kaspersky Security Center に送信します。Kaspersky Endpoint Security は、プロセス、オープンネットワーク接続、変更されたファイルに関する監視データを、Kaspersky Security Center に送信するとともに、アプリケーションが検知した脅威のデータと脅威の処理結果のデータを送信します。
- Kaspersky Security Center からコマンドを受信したときに、セキュリティを確保するための対応処理を実行します。

Kaspersky Endpoint Detection and Response Optimum との連携には、次の手順が含まれます：

1. **Kaspersky Endpoint Security の必須コンポーネントの有効化**

   Kaspersky Endpoint Security の次のコンポーネントが有効になっていて、実行されていることを確認します。

   - ファイル脅威対策。
   - ウェブ脅威対策。
   - ふるまい検知。

2. **脅威分析ツールの有効化**

   Kaspersky Security Network が標準モードまたは拡張モードで有効になっていることを確認します。

   Kaspersky Endpoint Detection and Response Optimum を最も効果的に動作させるには、拡張された Kaspersky Security Network モードを推奨します。

3. **EDR Optimum コンポーネントの有効化**

   以下の条件のいずれかが満たされていることを確認してください：

   - Kaspersky Endpoint Security は、Kaspersky Endpoint Detection and Response Optimum 機能を含むライセンスに基づいて使用されています。
   - Kaspersky Endpoint Detection and Response Optimum 機能を使用するための別のライセンスを購入し、EDR Optimum ライセンスをアプリケーションに追加しました。

4. **Kaspersky Endpoint Detection and Response Optimum の連携の有効化**

既定では、Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response Optimum の連携は無効になっています。連携を有効化、無効化、または設定できます。

- Web コンソールの使用。
- コマンドラインを使用します。

> Kaspersky Security Center 管理コンソールを使用した EDR Optimum コンポーネントの管理には対応していません。

EDR Optimum コンポーネントのステータスを確認できます。

- Web コンソールで *アプリケーションコンポーネントのステータスレポート*を使用します。

  Endpoint Detection and Response Optimum コンポーネントが Kaspersky Endpoint Security コンポーネントのリストに追加されました。レポートの詳細は、Kaspersky Security Center のヘルプを参照してください。

- Web コンソールのデバイスプロパティで操作。
- コマンドラインを使用して行います。

5. **管理サーバーへのデータ転送の有効化**

Kaspersky Endpoint Detection and Response Optimum のすべての機能を使用するには、次の設定を有効にする必要があります。

- **バックアップ内のファイルに関する通知が有効/無効**。

  この設定は、ポリシーのプロパティ（**製品設定 → 全般設定 → 保管領域の設定**）で有効にできます。

  この設定を有効にすると、Kaspersky Endpoint Security がデバイス上のバックアップに移動したファイルに関する情報が Kaspersky Security Center に送信できるようになります。

- **EDRアラートを表示します**。

  この設定は、Kaspersky Security Center Web コンソールのメインウィンドウの［**設定**］→［**インターフェイス設定**］で有効にできます。

  この設定を有効にすると、アラートのリストが表示されるようになります。

  > **EDR アラートの表示**設定は、Web コンソールバージョン 15.1 より前のバージョンでは使用できません。

Kaspersky Endpoint Detection and Response Optimum 連携の有効化または無効化

Kaspersky Endpoint Detection and Response Optimum Integration を有効または無効にすることができます。

- Web コンソールの使用。
- コマンドラインを使用します。

管理コンソールは、Kaspersky Endpoint Detection and Response Optimum を連携するための設定の管理に対応していません。

Web コンソールでの Kaspersky Endpoint Detection and Response Optimum の連携の有効化または無効化

Web コンソールで、Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response Optimum の連携を有効または無効にし、連携の設定を構成できます。

- ポリシーのプロパティ（［**製品設定**］→［**Detection and Response**］→［**Endpoint Detection and Response Optimum**］）
- デバイスのプロパティ（［**アセット（デバイス）**］→［**管理対象デバイス**］）→［<デバイス名> リンク］→［**製品**］［<Kaspersky Endpoint Security アプリケーションの名前> リンク］→［**製品設定**］→［**Detection and Response**］→［**Endpoint Detection and Response Optimum**］）

ポリシーがデバイスに適用されている場合、デバイスのプロパティで Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response Optimum の連携を有効または無効にすることはできません。

Kaspersky Endpoint Detection and Response (KATA) 連携設定

設定	説明
Endpoint Detection and Response Optimum は有効/無効になっています	Kaspersky Endpoint Security アプリケーションと Kaspersky Endpoint Detection and Response Optimum の連携を有効または無効にします。 連携サーバーは、既定でオフになっています。
ネットワーク分離	［**デバイスのブロック解除の設定**］リンクをクリックすると、［**デバイスのブロック解除の設定**］ウィンドウが開き、デバイスのブロック期間を設定できます。
除外	［**除外**］リンクをクリックすると、［**除外**］ウィンドウが開き、ネットワーク分離の除外を設定できます。

コマンドラインでの Kaspersky Endpoint Detection and Response Optimum の連携の有効化または無効化

コマンドラインでは、製品の全般設定の UseEdrOptimum 設定を使用して、Kaspersky Endpoint Detection and Response Optimum との連携を有効または無効にできます。

コマンドラインオプションまたは本製品の全般設定のすべてを含む設定情報ファイルを使用して設定を編集できます。

コマンドラインのオプションを使用して Kaspersky Endpoint Detection and Response Optimum の連携を有効にするには、次のコマンドを実行します：

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

コマンドラインを使用して Kaspersky Endpoint Detection and Response Optimum の連携を有効にするには、次のコマンドを実行します：

```
kesl-control --set-app-settings UseEdrOptimum=No
```

Kaspersky Endpoint Detection and Response Optimum の連携ステータスの表示

Web コンソールでの連携ステータスの表示

Web コンソールで、［**アセット（デバイス）**］セクション → ［**管理対象デバイス**］ → <デバイス名> リンク → ［**アプリケーション**］ → ［<Kaspersky Endpoint Security アプリケーション名> リンク → ［**全般**］ → **コンポーネント** の順に選択して、Kaspersky Endpoint Detection and Response Optimum and Response Optimum の連携ステータスを表示できます。

コマンドラインでの連携ステータスの表示

`kesl-control --app-info` コマンドを実行すると、コマンドラインを使用して Kaspersky Endpoint Detection and Response Optimum との連携ステータスを表示できます。

連携ステータス

EDR Optimum コンポーネントには、次のいずれかのステータスが表示されます：

- *実行中*。
  このステータスは、次の条件が同時に満たされた場合に表示されます：
  - EDR Optimum に必要なライセンスが追加されている場合。
  - 現在の日付がライセンスの有効期限よりも前の場合。
  - EDR Optimum に必要な 1 つ以上の Kaspersky Endpoint Security コンポーネントが有効になっている場合。
  - デバイス上で Kaspersky Endpoint Detection and Response Optimum Integration が有効になっている場合。
- *停止*。
  このステータスは次の場合に表示されます：
  - Kaspersky Endpoint Detection and Response Optimum の連携が無効になっている場合。
  - Kaspersky Endpoint Security アプリケーションが停止されていない場合。
- *ライセンスではサポートされていません*。
  このステータスは次の場合に表示されます：
  - 現在の日付がライセンスの有効期限より後の場合。
  - 現在のライセンスに EDR Optimum 機能が含まれていない場合。

- *誤動作*。

  このステータスは、次の条件が同時に満たされた場合に表示されます：

  - 現在の日付がライセンスの有効期限よりも前の場合。
  - EDR Optimum に必要な 1 つ以上のKaspersky Endpoint Security コンポーネントでエラーが発生した場合。

検知された脅威と対応処理に関する情報の表示

検知された脅威に関するすべての情報を表示し、適切な脅威対応処理を実行するには、次の内容を含む［アラート］詳細ウィンドウを使用します：

- 脅威の発展連鎖グラフ
- 選択した処理を実行するための UI を使用して脅威に対応するための推奨事項
- 脅威検知の詳細（検知モードなど）
- 保護対象デバイスに関する情報
- 検知されたオブジェクトに関する情報
- デバイスに表示されるファイルの履歴
- アプリケーションによって実行される脅威対応処理に関する情報

アラートの詳細における管理の詳細については、Kaspersky Endpoint Detection and Response Optimum ヘルプを参照してください。

IOC スキャンの結果は 30 日間保存されます。この時間が経過すると、Kaspersky Endpoint Security は古いエントリを自動的に削除します。

侵害の兆候の調査

IOC スキャンタスクを使用して、デバイス上の*侵害の兆候*を検索し、脅威への対応処理を実行できます。

侵害の兆候を検索するために、Kaspersky Endpoint Security はユーザーが準備した IOC ファイルを使用します。IOC ファイルは IOC ファイル要件に準拠する必要があります。

Web コンソールで、［*IoC スキャン*］タスクを作成して実行したり、その設定を編集したりできます。

- ［**アセット（デバイス）**］→［**タスク**］セクション
- **アセット（デバイス）**→**管理対象デバイス**→<デバイス名> リンク→**タスク**セクション
- アラート詳細ウィンドウで操作

コマンドラインで［*IOC スキャン*］タスクを作成、実行、または設定することはできません。Web コンソールで作成された［*IoC スキャン*］タスクを、`kesl-control --get-task-list` コマンドを使用してコマンドラインで表示することはできません。

このタスクでは、スケジュール設定の Wake-on-LAN 機能は使用できません。タスクを実行するには、デバイスの電源がオンになっていることを確認してください。

［*IOC スキャン*］タスクの設定

設定	説明
IOC ファイルの再設定	このボタンで、［**IOC ファイルの再設定**］パネルが開きます。 ［**IOC ファイルの再設定**］パネルにある［**IOC ファイルの追加**］ボタンをクリックすると、侵害の兆候を検索するために必要なデバイス上の IOC ファイルを選択してダウンロードできるウィンドウが開きます。IOC ファイルをアップロードすると、IOC ファイルからインジケーターのリストを表示できます。
IOC コレクションのエクスポート	このボタンをクリックすると、IOC ファイルがデバイスにダウンロードされます。
IOC 検知時の応答処理を適用する	このチェックボックスは、侵害の兆候が検知された場合に応答処理の適用を有効または無効にします。 チェックボックスをオンにすると、侵害の兆候が検知されると、アプリケーションは選択した処理を実行します。 • **デバイスをネットワークから分離する**。 このチェックボックスをオンにすると、侵害の兆候が検知されると、アプリケーションはデバイスをネットワークから分離し、脅威の拡散を防ぎます。分離期間を設定できます。 • **簡易スキャン**。 このチェックボックスをオンにすると、侵害の兆候が検知されると、アプリケーションは［*簡易スキャン*］タスクを開始します。 既定では、Kaspersky Endpoint Security はカーネル メモリ、実行中のプロセス、およびブートセクターをスキャンします。 チェックボックスをオフにすると、侵害の兆候が検知されてもアプリケーションは応答処理を実行しません。検知された侵害の兆候に関する情報は、［アラートの詳細］ウィンドウとタスクのプロパティに表示されます。
スキャン範囲	ファイルスキャン領域（システムディスクの重要な領域と IOC からのパス）が表示されます。

このタスクを開始した後は、IOC ファイルを追加または削除しないことは推奨します。これにより、以前に実行したタスクの IOC スキャン結果が正しく表示されない可能性があります。新しい IOC ファイルに基づいて IOC スキャンを実行するための新しいタスクを追加することを推奨します。

*IOC スキャン*の結果は、［**資産（デバイス）**］セクション → ［**タスク**］ → ［**製品設定**］ → ［**IOC スキャン結果**］で確認できます。

［**IOC スキャン結果**］セクションの表には、［*IOC スキャン*］タスクが実行されたデバイスのリストと、タスクの結果が含まれています。［**デバイス**］ドロップダウンリストでは、管理グループ内のすべての管理対象デバイスまたは特定のデバイスのタスク結果を選択できます。

表には次の列があります：

- **ステータス**：
  侵害の兆候の検知のステータスがアイコンとして表示されます。
- **ホスト**。
  ［*IOC スキャン*］タスクが実行されたデバイスの名前。
- **時間**。
  ［*IOC スキャン*］タスクが実行された日時
- **結果**。
  ［IOC スキャン］ タスクの結果に関する情報。完了したタスクのステータスは次のいずれかになります：
  - *IOC が検出されました*。
    このステータスはリンクとして表示され、リンクをクリックするとアラートの詳細を示すウィンドウが開きます。
  - *IOC は検出されませんでした*

タスクの結果は、［**アセット（デバイス）**］→［**タスク**］→［<タスク名>］セクションの［**結果**］タブの［**説明**］列でも確認できます。

IOC スキャンの結果は 30 日間保存されます。この時間が経過すると、Kaspersky Endpoint Security は古いエントリを自動的に削除します。

IOC ファイルの要件

［IOC スキャン］タスクを作成するときは、次のIOC ファイルの要件と制限を考慮してください：

- アプリケーションは、IOC および XML 拡張子の IOC ファイルに対応しています。これらのファイルは、IOC 記述にオープンスタンダード（OpenIOC バージョン 1.0 および 1.1）を使用します。
- IOC ファイル内のセマンティックエラーやサポートされていない IOC 用語およびタグによってタスクが失敗することはありません。IOC ファイルのこのようなセクションについては、本製品は一致がないことを登録します。
- ［IOC スキャン］タスクで使用されるすべての IOC ファイルの ID は一意である必要があります。ID が重複すると、タスク結果の正確性に影響する可能性があります。
- 脅威ごとに IOC ファイルを作成することを推奨します。これにより、［*IOC スキャン*］タスクの結果が読みやすくなります。

以下のリンクをクリックしてダウンロードできるファイルには、OpenIOC 標準の IOC 用語の完全なリストを含む表が含まれています。

IOC_TERMS.XLSX のダウンロード

本製品が OpenIOC 標準をサポートする方法に関する特別な考慮事項と制限事項を以下の表に示します。

OpenIOC 標準バージョン 1.0 および 1.1 の機能と制限

対応条件	OpenIOC 1.0： • `is` • `isnot`（セットからの除外として） • `contains` • `containsnot`（セットからの除外として） OpenIOC 1.1： • `is` • `contains` • `starts-with` • `ends-with` • `matches` • `greater-than` • `less-than`
条件の対応属性	OpenIOC 1.1： • `preserve-case` • `negate`
対応オペレーター	`AND` `OR`
対応データ種別	「`date`」：日付（適用可能な条件：`is`、`greater-than`、`less-than`） 「`int`」：整数（適用可能な条件：`is`、`greater-than`、`less-than`） 「`string`」：文字列（適用可能な条件：`is`、`contains`、`matches`、`starts-with`、`ends-with`） 「`duration`」：秒単位の期間（適用可能な用語：`is`、`greater-than`、`less-than`）

データ種別の解釈に関する特別な考慮事項	「ブール文字列」、「制限付き文字列」、「`md5`」、「`IP`」、「`sha256`」、「`base64Binary`」のデータ種別は文字列として解釈されます。
	本製品は、間隔として指定された `int` および `date` データ種別の `Content` パラメータの解釈に対応しています。
	• OpenIOC 1.0：
	コンテンツフィールドで `TO` 演算子を使用します：
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	• OpenIOC 1.1：
	• `greater-than` と `less-than` の条件の使用

	• コンテンツフィールドで `TO` の演算子の使用 本製品は、インジケーターが `ISO 8601`、ズールータイムゾーン、`UTC` 形式で指定されている場合、日付と期間のデータ種別の解釈に対応しています。

デバイスのネットワーク分離の有効化または無効化

デバイスのネットワーク分離を有効にするには、次の方法があります：

- *IOC スキャンタスクの使用*。
  ［**IOC の検知時の処理**］で［IOCスキャン］タスク設定を作成および構成する際には、［**IOC が検知されたときに対応処理を適用する**］および［**デバイスをネットワークから分離する**］チェックボックスをオンにした場合、アプリケーションが侵害の兆候（IOC）を検知すると、ネットワーク分離が自動的に有効になります。
- アラート詳細ウィンドウで操作
- Web コンソールのデバイスプロパティで操作。

ネットワーク分離の有効化は、Kaspersky Endpoint Detection and Response Optimum との連携が有効になっており、EDR Optimum コンポーネントが進行中 ステータスである場合にのみ利用可能です。

次の方法でデバイスのネットワーク分離を無効にすることができます。

- Web コンソールのデバイスプロパティで手動操作。
- コマンドラインで手動操作。
- アラート詳細ウィンドウで操作。
- デバイスのプロパティまたはポリシーのプロパティでの自動無効化の設定。

デバイスのプロパティおよびコマンドラインでのネットワーク分離の無効化は、Kaspersky Endpoint Detection and Response Optimum との連携や EDR Optimum コンポーネントが有効であるかどうか、またはデバイスにポリシーが適用されているかどうかに関係なく利用可能です。

ネットワーク分離が有効になっている場合、分離する必要のないネットワーク接続の除外を設定できます。

コマンドラインでネットワーク分離ステータスを確認できます。

ネットワーク分離を有効にすると、アプリケーションはデバイス上のすべての有効なネットワーク接続を切断し、以下に一覧表示されている接続を除くすべての新しい TCP/IP ネットワーク接続をブロックします：

- ネットワーク分離から除外される接続。
- Kaspersky Endpoint Security サービスによって開始された接続。
- Kaspersky Security Center ネットワークエージェントによって開始された接続。

- アプリケーションが Light Agent モードで使用されている場合の SVM および Integration Server への接続。

分離された EDR Optimum デバイスは、自動的に［**ISOLATED FROM NETWORK**］タグを取得します。ネットワーク分離が無効になっている場合、このタグは自動的に削除されます。

タグ別に分離されたデバイスのリストを取得する一般的な情報については、 Kaspersky Endpoint Detection and Response Optimum のヘルプを参照してください。

Web コンソールでデバイスのネットワーク分離を手動で有効または無効にします

デバイスのネットワーク分離を有効または無効にします：

1. Web コンソールのメインウィンドウで、**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. 必要なデバイスを含む管理グループを選択します。そのためには、管理対象デバイス上部の**現在のパス**フィールドのリンクをクリックし、開いたウィンドウで管理グループを選択します。
   リストには、選択した管理グループに管理対象デバイスのみが表示されます。
3. リストからデバイスを見つけて、その名前をクリックします。
4. これにより、管理対象デバイスの［プロパティ］ウィンドウが開きます。そのウィンドウで、［**アプリケーション**］タブに移動します。
5. 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一覧で、**Kaspersky Endpoint Security 12.1 for Linux** のアプリケーション名をクリックします。
   アプリケーションのプロパティウィンドウが表示されます。
6. ［**アプリケーション設定**］タブに移動します。
7. ［**Detection and Response**］→［**Endpoint Detection and Response Optimum**］セクションに移動します。
8. ［**ネットワーク分離**］で、次のいずれかを実行します。
   - デバイスのネットワーク分離を有効にするには、［**デバイスをネットワークから分離する**］ボタンをクリックします
   - デバイスのネットワーク分離を無効にするには、［**分離されたデバイスのブロックを解除する**］ボタンをクリックします

デバイスのネットワーク分離を有効にした場合、Kaspersky Endpoint Security はデバイスに［**ISOLATED FROM NETWORK**］タグを割り当てます。デバイスのネットワーク分離を無効にした場合、Kaspersky Endpoint Security はデバイスからこのタグを削除します。

ネットワーク分離の自動無効化の設定

次の操作によって、指定した期間が経過するとネットワーク分離が自動的に無効になるように設定できます：

- デバイスのプロパティで操作。

ポリシーがデバイスに適用されている場合、デバイスのプロパティでネットワーク分離の自動無効化を設定することはできません。

- ポリシーのプロパティで操作。

ポリシーのプロパティで指定されたネットワーク分離を自動的に無効にする設定は、［*IOC スキャン*］タスク中に検知された侵害の兆候（IOC）の結果として分離されたデバイスにのみ適用されます。

既定では、ネットワーク分離を有効にしてから 5 時間後に無効にします。ネットワーク分離を無効にすると、デバイスはネットワーク上で制限なく動作できます。

デバイスのプロパティでのネットワーク分離の自動無効化の設定

デバイスのネットワーク分離の自動無効化を設定します：

1. Web コンソールのメインウィンドウで、**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. 必要なデバイスを含む管理グループを選択します。そのためには、管理対象デバイス上部の**現在のパス**フィールドのリンクをクリックし、開いたウィンドウで管理グループを選択します。
   リストには、選択した管理グループに管理対象デバイスのみが表示されます。
3. リストからデバイスを見つけて、その名前をクリックします。
4. これにより、管理対象デバイスの［プロパティ］ウィンドウが開きます。そのウィンドウで、［**アプリケーション**］タブに移動します。
5. 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一覧で、**Kaspersky Endpoint Security 12.1 for Linux** のアプリケーション名をクリックします。
   アプリケーションのプロパティウィンドウが表示されます。
6. ［**アプリケーション設定**］タブに移動します。
7. ［**Detection and Response**］→［**Endpoint Detection and Response Optimum**］セクションに移動します。
8. ［**ネットワーク分離**］→［**デバイスのブロック解除の設定**］の順にクリックします。
9. これにより、［**デバイスのブロック解除の設定**］ウィンドウが開きます。そのウィンドウで、［デバイスのブロック解除の設定］を指定します。

デバイスのブロック解除の設定

設定	説明
自動的に分離されたデバイスのブロックを解除するには、次の操作を実行します：	このチェックボックスは、［**時間**］入力フィールドで指定された期間後に分離されたデバイスの自動ブロック解除を有効または無効にします。 既定では、このチェックボックスはオンです。
時間	分離されたデバイスが自動的にブロック解除されるまでの時間（時間単位）を入力するフィールド。 このフィールドは、［**自動的に分離されたデバイスのブロックを解除する**］チェック ボックスが選択されている場合にのみ有効になります。

10. 変更を保存します。

ポリシーのプロパティでのネットワーク分離の自動無効化の設定

デバイスのネットワーク分離の自動無効化を設定します：

1. Web コンソールのメインウィンドウで、**アセット（デバイス）** → **ポリシーとポリシープロファイル**タブを順に選択します。

   ポリシーのリストが表示されます。

2. ポリシーを適用するデバイスを含む管理グループを選択します。そのためには、ウィンドウ上部の**現在のパス**フィールドのリンクをクリックし、開いたウィンドウで管理グループを選択します。

   リストには、選択した管理グループに設定されているポリシーが表示されます。

3. リスト内の必要な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が表示されます。

4. ［**アプリケーション設定**］タブに移動します。

5. ［**Detection and Response**］→［**Endpoint Detection and Response Optimum**］セクションに移動します。

6. ［**ネットワーク分離**］→［**デバイスのブロック解除の設定**］の順にクリックします。

7. これにより、［**デバイスのブロック解除の設定**］ウィンドウが開きます。そのウィンドウで、［デバイスのブロック解除の設定］を指定します。

デバイスのブロック解除の設定

設定	説明
自動的に分離されたデバイスのブロックを解除するには、次の操作を実行します：	このチェックボックスは、［**時間**］入力フィールドで指定された期間後に分離されたデバイスの自動ブロック解除を有効または無効にします。 既定では、このチェックボックスはオンです。
時間	分離されたデバイスが自動的にブロック解除されるまでの時間（時間単位）を入力するフィールド。 このフィールドは、［**自動的に分離されたデバイスのブロックを解除する**］チェック ボックスが選択されている場合にのみ有効になります。

8. 変更を保存します。

コマンドラインでのデバイスのネットワーク分離の無効化

コマンドラインを使用してデバイスのネットワーク分離を無効にするには、次のコマンドを実行します：

```
kesl-control [-R] --isolation-off
```

次のコマンドを使用すると、ネットワーク分離のステータスを確認し、ネットワーク分離の除外リストを表示できます：

```
kesl-control [-R] --isolation-stat
```

次のいずれかのネットワーク分離ステータスがコマンドラインに表示されます：

- *ネットワーク分離が有効です。*
- *ネットワーク分離が無効です。*

ネットワーク分離除外の設定

次の操作によって除外を設定できます：

- ポリシープロパティで操作
- デバイスのプロパティで操作

設定されたルールの対象となるネットワーク接続は、ネットワーク分離が有効になった後もデバイス上でブロックされません。

既定では、DNS/DHCP サーバーおよび DNS/DHCP クライアントの役割を持つデバイスの中断のない動作を保証するルールで設定されるネットワークプロファイルは、ネットワーク分離から除外されます。

ポリシープロパティで定義された除外は、侵害の兆候（IOC）の検知に反応した結果としてアプリケーションによってネットワーク分離が自動的に有効にされた場合にのみ適用されます。

デバイスプロパティで定義された除外は、デバイス プロパティまたは［アラート詳細］ウィンドウでネットワーク分離が手動で有効になっている場合にのみ適用されます。

現在のポリシーでは、デバイスのプロパティで定義されたネットワーク分離除外の適用は回避できません。

次の操作でネットワーク分離除外のリストを表示できます：

- ポリシーのプロパティ（［**アプリケーション設定**］→［**Detection and Response**］→［**Endpoint Detection and Response Optimum**］→**除外**リンク）
- デバイスのプロパティ（［**アセット（デバイス）**］→［**管理対象デバイス**］）→［<デバイス名> リンク］→［<Kaspersky Endpoint Security アプリケーションの名前> リンク］→［**アプリケーション設定**］→［**Detection and Response**］→［**Endpoint Detection and Response Optimum**］→［**除外**］リンク）
- コマンドラインで

Web コンソールのポリシープロパティでのネットワーク分離除外の追加または削除

Web コンソールでは、ポリシープロパティのネットワーク分離除外を追加または削除できます：［**アプリケーション設定**］→［**Detection and Response**］→［**Endpoint Detection and Response Optimum**］→［**除外**］リンク。

［**除外**］ウィンドウでは、表の上にあるボタンをクリックして、次の処理を実行できます。

- 除外されたネットワーク接続に関する情報を、次のいずれかの方法で追加します：
  - ［**追加**］をクリックし、ネットワーク接続に関する情報を入力します
  - ［**プロファイルから追加**］をクリックし、辞書からネットワークプロファイルを選択します
- ネットワーク接続に関する情報を削除します

デバイスのプロパティでのネットワーク分離除外の追加または削除

デバイスにポリシーが適用されている場合、デバイスのプロパティでネットワーク分離の除外を追加または削除することはできません。

デバイスのプロパティでネットワーク分離の除外を追加または削除します：

1. Web コンソールのメインウィンドウで、**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. 必要なデバイスを含む管理グループを選択します。そのためには、管理対象デバイス上部の**現在のパス**フィールドのリンクをクリックし、開いたウィンドウで管理グループを選択します。
   リストには、選択した管理グループに管理対象デバイスのみが表示されます。

3. リストからデバイスを見つけて、その名前をクリックします。

4. これにより、管理対象デバイスの［プロパティ］ウィンドウが開きます。そのウィンドウで、［**アプリケーション**］タブに移動します。

5. 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一覧で、**Kaspersky Endpoint Security 12.1 for Linux** のアプリケーション名をクリックします。
   アプリケーションのプロパティウィンドウが表示されます。

6. ［**アプリケーション設定**］タブに移動します。

7. ［**Detection and Response**］→［**Endpoint Detection and Response Optimum**］セクションに移動します。

8. ［**ネットワーク分離**］で、［**除外**］をクリックして［**除外**］ウィンドウを開きます。

9. 開くウィンドウで、表の上にあるボタンを使用して必要な処理を実行します。

   - 除外されたネットワーク接続に関する情報を追加する場合は、次のいずれかの方法で追加します：

     - ［**追加**］ボタンをクリックし、ネットワーク接続に関する情報を入力します。

     - ［**プロファイルから追加**］ボタンをクリックし、辞書からネットワークプロファイルを選択します。

   - 除外されたネットワーク接続に関する情報を削除する場合は、削除するネットワーク接続の横にあるチェックボックスをオンにして、［**削除**］をクリックします。

10. 変更を保存します。

ネットワーク分離除外ウィンドウの追加

このウィンドウでは、ネットワーク分離が有効になっているときにブロックしたくないネットワーク接続に関する情報を入力できます。

ネットワーク接続設定

設定	説明
名前	ネットワーク接続の名前。
通信方向	ネットワーク接続の方向
プロトコル	ネットワーク接続で使用されるプロトコル。
番号	ネットワーク接続の番号。
ローカルポート / 範囲	ローカルポート番号または範囲。
リモートポート / 範囲	リモートポート番号または範囲。
リモートアドレス	リモートデバイスの IP アドレス

ネットワークプロファイル辞書ウィンドウ

このウィンドウでは、除外するネットワーク接続のプロファイルを選択できます。

ネットワーク接続プロファイル

ネットワーク接続プロファイル	説明
DNS サーバー	IP アドレスを取得する要求や DNS レコードを更新する要求に応答して DNS 名前解決を提供するサービス。
DNS クライアント	DNS 名クエリを実行して DNS 名解決を提供するサービス。
Active Directory 証明書サービス	組織内で内部使用するための公開鍵証明書を作成、検証、および取り消すために使用されるサービス。
Active Directory フェデレーション サービス	一元的に保存された連携された一連の資格情報を通じて、ユーザーに複数の Web サービスまたはネットワークリソースへのアクセスを許可するために使用されるサービス。
Active Directory ライトウェイトディレクトリサービス	Active Directory ドメインサービスと同じ機能を提供しますが、ドメインやドメインコントローラーを作成する必要のないサービスです。
Active Directory Rights Management Services	ドキュメントへのユーザーアクセスを制御するために使用されるサービス。
DHCP サーバー	このサービスは、動的ホスト構成プロトコル（DHCP）を使用して IP アドレスを自動的に割り当てます。
ファイル転送プロトコル（FTP）	ネットワークを介してクライアントとサーバー間でファイルを転送するための標準ネットワークプロトコル。
Kerberos キー配布センター	Active Directory ドメイン内のユーザーとデバイスにチケット（TGS）と一時セッションキーを提供するために使用されるネットワーク サービス。
セキュアシェル（SSH）	オペレーティングシステムのリモート制御と TCP 接続のトンネリングを可能にするプロトコル。
Linux システムコンポーネント	Linux システムコンポーネント。

プロセスの開始

*プロセスの開始*タスクを使用すると、デバイス上のプロセスと実行可能ファイルをリモートで開始できます。

たとえば、次のように実行できます：

- デバイス上の悪意のあるアクティビティの結果としてプロセスが停止しました。
- ユーザーによって停止されたプロセス。
  たとえば、停止したプロセスをリモートで開始するには、プロセスの終了 *タスク*を使用できます。
- スクリプト。

たとえば、スクリプトを実行してデバイスからデータを収集し、脅威を調査できます。

- ユーティリティ。
  たとえば、デバイス設定情報をファイルに保存するユーティリティを実行できます。
- アプリケーション。

SELinux が `Enforcing` モードでオペレーティングシステムにインストールされている場合、［*プロセスの開始*］タスクを開始するには、SELinux の追加設定が必要です。

Web コンソールで、プロセスの開始タスクを作成して*実行*したり、その設定を編集したりできます。

コマンドラインを使用して［*プロセスの開始*］タスクを作成、実行、または設定することはできません。Web コンソールで作成された［*プロセスの開始*］タスクを、`kesl-control --get-task-list` コマンドを使用してコマンドラインで表示することはできません。

プロセスタスク設定の開始

設定	説明
実行コマンド	プロセスを開始するコマンドを入力するフィールド。 たとえば、管理サーバーへの接続をチェックする `klnagchk` ツールを実行する場合は、コマンド `/<`作業ディレクトリへの絶対パス`>/klnagchk` を実行し、下の表に記載されている他のフィールドに入力する必要があります。 ［**作業ディレクトリパス（任意）**］フィールドに作業ディレクトリへの絶対パスを入力することもできます。その場合は、［**実行コマンド**］フィールドに作業ディレクトリへの絶対パスを入力しないでください。
コマンドライン引数（省略可能）	起動時にスクリプト、ユーティリティ、またはアプリケーションに追加の入力を渡すためのコマンドライン引数を入力するフィールド。 たとえば、`-logfile klnagchk.log` 引数を入力できます。この引数は、ツールに結果を `klnagchk.log` という名前のファイルに保存するように指示します。 複数の引数を渡す必要がある場合は、スペースで区切ります。 たとえば、`-logfile klnagchk.log -savecert certificate.cer` 引数を入力できます。これらの引数は、ツールに結果を `klnagchk.log` という名前のファイルに保存し、管理サーバーへのアクセスを確認するために使用された証明書を `certificate.cer` ファイルに保存するように指示します。
作業用ディレクトリのパス（省略可能）	スクリプト、ユーティリティ、またはアプリケーションの実行可能ファイルが配置されている作業ディレクトリへのパスを入力するフィールド。 たとえば、`/opt/kaspersky/klnagent64/bin/` と入力できます。 ［**実行コマンド**］フィールドに作業ディレクトリへの絶対パスを入力した場合は、［**作業ディレクトリパス（任意）**］フィールドには入力しないでください。

タスクの結果は、［**アセット（デバイス）**］→［**タスク**］→［<タスク名>］セクションの［**結果**］タブの［**説明**］列で確認できます。

プロセスの終了

［*プロセスの終了*］タスクを使用して、デバイス上のプロセスをリモートで終了できます。

たとえば、次のように終了できます：

- 悪意のあるアクティビティの結果としてデバイス上で開始されたプロセス。
- ユーザーによって開始されたプロセス。
  たとえば、［*プロセスの開始*］タスクを使用して開始したプロセスをリモートで終了できます。
- スクリプト。
  たとえば、［*プロセスの開始*］タスクを使用して開始したスクリプトをリモートで終了できます。
- ユーティリティ。
  たとえば、［*プロセスの開始*］タスクを使用して起動されたインターネットスピードテストユーティリティをリモートで終了できます。
- アプリケーション。

システムクリティカルオブジェクト（SCO）のプロセスを終了することはできません。SCO には、オペレーティング システムと Kaspersky Endpoint Security アプリケーションの動作に必要なファイルが含まれています。

Web コンソールで、プロセスの終了タスクを作成して*実行*したり、その設定を編集したりできます。コマンドラインで*プロセスの終了*タスクを作成、実行、または設定することはできません。Web コンソールで作成された*プロセスの終了*タスクを、`kesl-control --get-task-list` コマンドを使用してコマンドラインで表示することはできません。

プロセスタスク設定の終了

設定	説明
プロセスを終了させたいファイルを指定します	ドロップダウンリストで、ファイルへのパスを指定する方法を選択できます： • **ディレクトリおよびチェックサムへのパスによる** • **完全パス** • **PID 別** ［**PID 別**］の値は、デバイスプロパティで作成されたタスクのドロップダウンリストにのみ表示されます。
ファイルへの完全パス	ファイルへの絶対パスを入力するフィールド。 このフィールドは、［**プロセスを終了させたいファイルを指定してください**］ドロップダウンリストで［**絶対パス**］を選択した場合にのみ表示されます。

チェックサム種別	このドロップダウンリストでは、ファイルのチェックサム種別を選択できます： • **MD5**。 • **SHA256**。 このドロップダウンリストは、**ディレクトリへのパスを選択し**、**プロセスの終了を希望するファイルの指定**ドロップダウンリストで**チェックサム**を選択します。
ファイルのチェックサム	ファイルチェックサムを入力するフィールド。 このフィールドは、［**プロセスを終了させたいファイルを指定してください**］ドロップダウンリストで、［**ディレクトリおよびチェックサムへのパスによる**］を選択し、［**チェックサム種別**］ドロップダウンリストで［**MD5**］を選択した場合にのみ表示されます。
ディレクトリパス	ファイルディレクトリへのパスを入力するフィールド。 このフィールドは、［**プロセスを終了させたいファイルを指定してください**］ドロップダウンリストで［**ディレクトリおよびチェックサムへのパスによる**］を選択した場合にのみ表示されます。
プロセス ID	プロセス ID（PID）入力フィールド。 このフィールドは、［**プロセスを終了させたいファイルを指定してください**］ドロップダウンリストで［**PID**］を選択した場合にのみ表示されます。

タスクの結果は、［**アセット（デバイス）**］→［**タスク**］→［<タスク名>］セクションの［**結果**］タブの［**説明**］列で確認できます。

デバイスからのファイルの受信

［*デバイスからファイルを受信*］タスクを使用して、ユーザーのデバイスからファイルを受信できます。

たとえば、サードパーティのアプリケーションによって生成されたイベントログファイルを受信することができます。

Web コンソールで、［*デバイスからファイルを受信*］タスクを作成して実行したり、その設定を編集したりできます。

コマンドラインで［*デバイスからファイルを受信*］タスクを作成、実行、または設定することはできません。Web コンソールで作成された*デバイスからのファイルの受信*タスクを、`kesl-control --get-task-list` コマンドを使用してコマンドラインで表示することはできません。

［**製品設定**］タブの「**ファイルの受信**」の表には、次の列が含まれています：

- **ディレクトリパス**。

デバイス上のファイルのディレクトリへのパス。

- **チェックサム検証種別**。
  デバイス上のファイルのチェックサム検証種別。

表の上にあるボタンをクリックすると、デバイス上のファイルのデータを追加、編集、または削除できます。［*デバイスからファイルを受信*］タスクは、「**ファイルの受信**」の表で選択されたファイルに対して実行されます。

［**追加**］ボタンをクリックすると、［**ファイルの受信**］ウィンドウが開き、［*デバイスからファイルを受信*］タスクの設定を構成できます。

デバイスタスク設定からのファイルの受信

設定	説明
受信するファイルを指定します	ドロップダウンリストで、ファイルへのパスを指定する方法を選択できます： • **ディレクトリおよびチェックサムへのパスによる** • **完全パス**
ファイルへの完全パス	ファイルへの絶対パスを入力するフィールド。 このフィールドは、［**取得するファイルを指定してください**］ドロップダウンリストで［**絶対パス**］を選択した場合にのみ表示されます。
チェックサムタイプ	このドロップダウンリストでは、ファイルのチェックサム種別を選択できます： • **MD5**。 • **SHA256** 。 このドロップダウンリストは、**ディレクトリへのパスを選択し**、**受信するファイルの指定**ドロップダウンリストで**チェックサム**を選択します。
ファイルのチェックサム	ファイルチェックサムを入力するフィールド。 このフィールドは、［**取得するファイルを指定してください**］ドロップダウンリストで［**ディレクトリおよびチェックサムへのパスによる**］を選択した場合にのみ表示されます。
ファイルディレクトリへのパス	ファイルディレクトリへのパスを入力するフィールド。 このフィールドは、［**取得するファイルを指定してください**］ドロップダウンリストで［**ディレクトリおよびチェックサムへのパスによる**］を選択した場合にのみ表示されます。

*デバイスからのファイルの受信*タスクの結果として、ファイルのコピーがデバイスのバックアップに保存されます。Web コンソールを使用して、このコピーをバックアップからダウンロードを開始したデバイスにダウンロードできます。

ファイルサイズは 100 MBを超えてはなりません。

ユーザーデバイス上の元のファイルは元のディレクトリに残ります。

*デバイスからファイルを受信*タスクを通じて受信されたすべてのファイルは、ファイルスキャンの結果に関係なく、Kaspersky Security Center Backup で*感染*ステータスになります。

タスクの結果は、［**アセット（デバイス）**］→［**タスク**］→［<タスク名>］セクションの［**結果**］タブの［**説明**］列で確認できます。

デバイスからのファイルの削除

［*デバイスからファイルを削除*］タスクを使用して、デバイスからファイルを削除できます。これは、たとえば脅威への対応の一環として必要になる場合があります。

システムクリティカルオブジェクト（SCO）は削除できません。SCO には、オペレーティング システムと Kaspersky Endpoint Security アプリケーションの動作に必要なファイルが含まれています。

Web コンソールで、［*デバイスからファイルを削除*］タスクを作成して実行したり、その設定を編集したりできます。

コマンドラインで［*デバイスからファイルを削除*］タスクを作成、実行、または設定することはできません。Web コンソールで作成された*デバイスからのファイルの削除*タスクを、 `kesl-control --get-task-list` コマンドを使用してコマンドラインで表示することはできません。

デバイスタスク設定からのファイルの削除

設定	説明
削除するファイルを指定する	ドロップダウンリストで、削除するファイルへのパスを指定する方法を選択できます： • **パスとチェックサム** • **絶対パス**
ファイルへの絶対パス	削除するファイルへの絶対パスを入力するフィールド。 このフィールドは、［**削除するファイルを指定する**］ドロップダウンリストで［**絶対パス**］を選択した場合にのみ表示されます。
チェックサム種別	ドロップダウンリストでは、削除するファイルのチェックサムの種別を選択できます： • **MD5**。

	• **SHA256** 。 このドロップダウンリストは、［**ディレクトリへのパス**］を選択し、［**削除するファイルの指定**］ドロップダウンリストでチェックサムを選択します。
ファイルチェックサム	削除するファイルチェックサムを入力するフィールド。 このフィールドは、［**削除するファイルを指定する**］ドロップダウンリストで［**パスとチェックサム**］を選択した場合にのみ表示されます。
ディレクトリパス	削除するファイルディレクトリへのパスを入力するフィールド。 このフィールドは、［**削除するファイルを指定する**］ドロップダウンリストで［**パスとチェックサム**］を選択した場合にのみ表示されます。
サブディレクトリを含む	このチェックボックスでは、サブディレクトリを有効にするかどうかを選択します。

ファイルが別のプロセスによってブロックされている場合、タスクは*完了*ステータスで表示されますが、ファイル自体はデバイスの再起動後にのみ削除されます。デバイスを再起動した後、ファイルが削除されたことを確認してください。

実行中の実行可能ファイルを削除しようとすると、*デバイスからのファイルの削除*タスクが*アクセス拒否*エラーで終了することがあります。そのファイルに対して*プロセスの終了タスクを*作成して実行し、再試行してください。

タスクの結果は、［**アセット（デバイス）**］→［**タスク**］→［<タスク名>］セクションの［**結果**］タブの［**説明**］列で確認できます。

Kaspersky Managed Detection and Response との連携

Kaspersky Managed Detection and Response は、組織を狙った脅威を継続的に検索、検出、排除します。Kaspersky Managed Detection and Response ソリューションとの連携は、 Kaspersky Endpoint Security コンポーネントである Managed Detection and Response (MDR) によって促進されます。

Kaspersky Managed Detection and Response との対話時に、Kaspersky Endpoint Security では次の機能を実行できます：

- テレメトリデータを Kaspersky Managed Detection and Response に送信して、脅威を検知します。
- Kaspersky Managed Detection and Response のコマンドを実行して、セキュリティ機能を提供します。

Kaspersky Endpoint Security と Kaspersky Managed Detection and Response との連携を設定するには、次の処理を実行します：

- ファイル脅威対策と動作検知が有効になっていることを確認してください。これらのコンポーネントが無効になっている場合、Kaspersky Managed Detection and Response ではデバイスは赤色のステータスになります。

また、ウェブ脅威対策とネットワーク脅威対策も有効にすることを推奨します。これらのコンポーネントが無効になっている場合、Kaspersky Managed Detection and Response ではデバイスは黄色のステータスになります。

デバイスのステータスの詳細については、Kaspersky Managed Detection and Response のヘルプを参照してください。

- 拡張モードでの Kaspersky Security Network の使用を有効にします。

  Kaspersky Security Network は、コマンドライン、Web コンソール、または管理コンソールで有効にできます。

- Kaspersky Security Network を設定します。テレメトリの送信には KPSN が必要です。

  Kaspersky Private Security Network は、Web コンソールまたは管理コンソールでのみ設定できます。

  > Kaspersky Endpoint Security コマンドを使用して KPSN を設定する方法はありません。

- Kaspersky Managed Detection and Response コンポーネントを有効にし、MDR 設定情報ファイルの ZIP アーカイブにある BLOB 設定情報ファイルをアップロードします。

  Managed Detection and Response コンポーネントを有効にして、コマンドライン、Web コンソール、または管理コンソールで BLOB 設定情報ファイルをアップロードできます。

Kaspersky Managed Detection and Response の連携を有効にする KPSN の設定

Web コンソールまたは管理コンソールに限って、Kaspersky Private Security Network を Kaspersky Managed Detection and Response との連携を設定できます。

KPSN を設定するには、MDR 設定ファイルの ZIP アーカイブから Kaspersky Security Network .pkcs7 設定ファイルを Kaspersky Security Center 管理サーバーにアップロードします。

Kaspersky Security Network の設定情報ファイルをダウンロードすることで、Kaspersky Endpoint Security がインストールされたデバイスのデータが自動的にカスペルスキーに送信され、処理されることに同意したものとみなされます。送信されたデータが処理されることに同意しない場合は、設定情報ファイルを読み込まないでください。送信されるデータの詳細は、Kaspersky Managed Detection and Response のヘルプを参照してください。

Web コンソールで KPSN と Kaspersky Managed Detection and Response の連携を設定します：

1. Web コンソールのメインウィンドウで、管理サーバーのプロパティウィンドウを開きます。
2. 左のリストから［**KSN プロキシサーバー設定**］セクションを選択します。
3. ［**KSN プロキシサーバーを管理サーバーでプロキシサーバーとして有効にする**］の切り替えボタンをオンにして、KSN プロキシサーバーサービスを有効にします。
4. ［**Kaspersky Private Security Network を使用する**］の切り替えボタンをオンにします。
5. ウィンドウが表示され、以前のバージョンの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使用する際の特定の問題に関する警告が表示されます。［**OK**］をクリックします。

6. ［**KSN プロキシサーバー設定でファイル**］をクリックします。

7. Kaspersky Security Network .pkcs7 設定ファイルを選択し、**開く**をクリックします。

8. ［**保存**］をクリックします。

管理コンソールでプライベート KSN と Kaspersky Managed Detection and Response の連携を設定します：

1. 管理コンソールのツリーで、管理サーバーのプロパティウィンドウを開きます。

2. **KSN プロキシサーバー → KSN プロキシ サーバー設定**を選択します。

3. ［**管理サーバーをプロキシサーバーとして使用する**］をオンにして、KSN プロキシサーバーサービスを有効にします。

4. ［**プライベート KSN の設定**］をオンにします。

5. ウィンドウが表示され、以前のバージョンの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使用する際の特定の問題に関する警告が表示されます。［**OK**］をクリックします。

6. ［**KSN プロキシサーバー設定でファイル**］をクリックします。

7. Kaspersky Security Network .pkcs7 設定ファイルを選択し、**開く**をクリックします。

8. ［**適用**］をクリックします。

Web コンソールでの Kaspersky Managed Detection and Response の連携の設定

Web コンソールでは、Kaspersky Endpoint Security と Kaspersky Managed Detection and Response の連携を有効または無効にしたり、ポリシープロパティ（**製品設定 → Detection and Response → Managed Detection and Response**）で BLOB 設定情報ファイルを読み込むことができます。

MDR 連携の設定

設定	説明
Managed Detection and Response の有効化 / 無効化	切り替えスイッチは、Kaspersky Endpoint Security と Kaspersky Managed Detection and Response ソリューションを連携するために必要な Managed Detection and Response コンポーネントを有効または無効にします。 この切り替えボタンは既定でオフになっています。
ダウンロード	このボタンをクリックすると、標準のウィンドウが表示され、BLOB 設定情報ファイルを選択できます。

BLOB 設定ファイルは、Kaspersky Managed Detection and Response の配布キットに含まれる ZIP アーカイブ内にあります。

BLOB 設定ファイルをダウンロードすることで、Kaspersky Endpoint Security がインストールされたデバイスのデータが自動的にカスペルスキーに送信され、処理されることに同意したものとみなされます。送信されたデータが処理されることに同意しない場合は、設定情報ファイルを読み込まないでください。送信されるデータの詳細は、Kaspersky Managed Detection and Response のヘルプセクションを参照してください。

管理コンソールでの Kaspersky Managed Detection and Response の連携の設定

管理コンソールでは、Kaspersky Endpoint Security と Kaspersky Managed Detection and Response の連携を有効または無効にし、ポリシーのプロパティ（**Detection and Response → Managed Detection and Response**）で BLOB 設定情報ファイルを読み込むことができます。

MDR 連携の設定

設定	説明
Managed Detection and Response を有効にする	このチェックボックスは、Kaspersky Endpoint Security と Kaspersky Managed Detection and Response ソリューションを連携するために必要な Managed Detection and Response コンポーネントを有効にします。 既定では、このチェックボックスはオフです。
ダウンロード	このボタンをクリックすると、Microsoft Windows 標準のウィンドウが表示され、BLOB 設定情報ファイルを選択できます。

BLOB 設定ファイルは、Kaspersky Managed Detection and Response の配布キットに含まれる ZIP アーカイブ内にあります。

BLOB 設定ファイルをダウンロードすることで、Kaspersky Endpoint Security がインストールされたデバイスのデータが自動的にカスペルスキーに送信され、処理されることに同意したものとみなされます。送信されたデータが処理されることに同意しない場合は、設定情報ファイルを読み込まないでください。送信されるデータの詳細は、Kaspersky Managed Detection and Response のヘルプセクションを参照してください。

コマンドラインで Kaspersky Managed Detection and Response の連携の設定

コマンドラインでは、次の操作が可能です：

- Managed Detection and Response コンポーネントを有効または無効にします。
- 統合に必要な BLOB 設定情報ファイルをアップロードまたは削除します。
- Kaspersky Endpoint Security が Managed Detection and Response と正常に統合された後に自動的に作成される *Mdr_Autostart_Scan* サービスタスクの開始時間を編集します。

管理コンソールまたは Web コンソールで、Kaspersky Endpoint Security と Kaspersky Managed Detection and Response の連携を設定することをお勧めします。

アプリケーションの全般設定の UseMDR パラメータを使用して、Managed Detection and Response コンポーネントを有効または無効にすることができます。コマンドラインオプションまたは本製品の全般設定のすべてを含む設定情報ファイルを使用して設定を編集できます。

`UseMDR` では次の値を利用できます：

- Managed Detection and Response コンポーネントを有効にするには、 はいを選択します。
- いいえを選択すると、Managed Detection and Response コンポーネントが無効になります。

ライセンス管理コマンド経由で、BLOB 設定情報ファイルをアップロードまたは削除できます。

BLOB 設定情報ファイルを読み込むには、次のコマンドを実行します：

```
kesl-control --load-mdr-blob <MDR BLOB 設定情報ファイルのパス>
```

BLOB 設定情報ファイルを削除するには、次のコマンドを実行します：

```
kesl-control --remove-mdr-blob
```

統合を有効にすると、1日に1回実行される *Mdr_Autostart_Scan* サービスタスクが作成されます。必要に応じて開始時間を設定できます。他のタスク設定やスケジュールオプションは編集できません。

Light Agent モードで本製品を使用する際の設定

このセクションで説明する設定は、Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合にのみ適用されます。

Kaspersky Endpoint Security を Light Agent モードで実行するには、Light Agent と SVM にインストールされている Protection Server との間の継続的な対話が要求されます。Protection Server に接続されていない場合、Light Agent はスキャンのためにファイルフラグメントを Protection Server に転送することができず、スキャンは実行されません。

Protection Server と対話するために、Light Agent は、この Protection Server がインストールされている SVM への接続を確立して維持します。

Web コンソールまたは管理コンソールで、Light Agent を SVM に接続するための設定を行うことができます。コマンドラインで設定を構成することはできません。アプリケーションの使用状況に関する情報を表示できるのは、Light Agent モードのみです。

Light Agent を SVM に接続する際、次の設定を指定できます：

- SVM の検出方法。Light Agent が接続可能な SVM を検出するために使用する方法を選択できます。Light Agent は、次のいずれかの方法でネットワーク上で実行されている SVM を検出できます：
  - Integration Server の使用する。SVM は、それ自体に関する情報を Integration Server に送信します。Integration Server は、接続可能な SVM のリストを生成し、Light Agent に提供します。

    この方法で SVM を検出するには、SVM と Light Agent を Integration Server に接続する必要があります。
  - SVM アドレスのリストの使用。Light Agent が接続できる SVM アドレスのリストを指定できます。
- 接続するSVMを選択するアルゴリズム。使用可能な SVM に関する情報を受信した後、Light Agent は SVM 選択アルゴリズムに従って接続する最適な SVM を選択します。接続先の SVM を選択する時に Light Agent が使用するアルゴリズムを指定できます。
- 接続タグ。接続タグを使用して、SVM への Light Agent の接続を制御できます。接続タグを使用する場合、Light Agent はその接続タグを使用するように設定された SVM にのみ接続できます。
- Light Agent と Protection Server 間の接続のセキュリティ。暗号化を使用して、Light Agent と Protection Server 間の接続を保護できます。

Light Agent と SVM の接続設定の詳細については、Kaspersky Hybrid Cloud Security for Virtualization Light Agent のヘルプを参照してください。

Web コンソールでの Light Agent の設定

Web コンソールでは、ポリシーのプロパティ（**製品設定 → Light Agent モード**）で、Light Agent を SVM に接続するための設定を構成できます。

SVM 検出設定

このセクションで説明する設定は、Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合にのみ適用されます。

このウィンドウでは、Light Agent が接続可能な SVM を検出するために使用する方法を選択できます。

SVM 検出設定

設定	説明
Integration Server を使用する	このオプションがオンにされている場合、Light Agent は Integration Server に接続し、接続可能な SVM のリストとそれらに関する情報を取得します。 Integration Server を使用する場合は、Light Agent を Integration Server に接続するための設定を行う必要があります。
SVM アドレスのカスタムリストを使用する	このオプションを選択する場合は、このポリシーによって管理される Light Agent が接続できる SVM のリストを指定できます。Light Agent は、リストで指定された SVM にのみ接続します。
SVM アドレスのリスト	ポリシーの対象となる Light Agent が接続できる SVM の IPv4 形式の IP アドレスまたは完全修飾ドメイン名（FQDN）のリスト。 ［**追加**］をクリックするとウィンドウが開き、IPv4 形式の IP アドレスまたは SVM の完全修飾ドメイン名（FQDN）を指定できます。SVM の複数の IP アドレスまたは FQDN を新しい行に入力できます。 単一の IP アドレスにマップされる完全修飾ドメイン名（FQDN）のみを指定します。複数の IP アドレスに対応する完全修飾ドメイン名を使用すると、アプリケーションでエラーが発生する可能性があります。 ［**削除**］をクリックすると、リストで選択したアドレスを削除できます。 ［**SVM アドレスのカスタムリストを使用する**］が選択されている場合は、SVM アドレスのリストが表示されます。

［**SVM アドレスのカスタムリストを使用する**］をオンにした場合、Light Agent は高度な SVM 選択アルゴリズムを使用し、SVM で大規模インフラストラクチャ保護モードが有効になります（詳細については、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください）。この場合、SVM パスが無視された場合にのみ、Light Agent をこの SVM に接続できます。［**SVM 選択アルゴリズム**］セクションで、［**SVM パス**］設定を［**SVM パスを無視**］に設定する必要があります。それ以外の値に設定した場合、Light Agent は SVM に接続できなくなります。

Integration Server 接続設定

このセクションで説明する設定は、Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合にのみ適用されます。

Light Agent が統合サーバーを通じて SVM に関する情報を受信する場合、または保護サーバーと Light Agent 間の接続を保護する場合は、統合サーバーへの接続が要求されます。

このウィンドウには、Light Agent を Integration Server に接続するための現在の設定（接続用のアドレスとポート）が表示されます。［**編集**］をクリックすると、［**Integration Server への接続**］ウィンドウが開き、Integration Server への接続を設定できます。

［Integration Server への接続］ウィンドウ

このウィンドウでは、Light Agent を Integration Server に接続するための設定を指定または変更できます。

Integration Server 接続設定

設定	説明
アドレス	Integration Server がインストールされているデバイスの IPv4 形式の IP アドレスまたは完全修飾ドメイン名（FQDN）。 アドレスとして NetBIOS 名、「localhost」、または 127.0.0.1 が指定されている場合、Integration Server への接続はエラーが発生して失敗します。
Port	Integration Server に接続するためのポート。 ポート 7271 が既定で使用されます。
確認する	ボタンをクリックした時、Web プラグインは Integration Server から受信した SSL 証明書を確認します。 このボタンは、Integration Server に接続するためのアドレスとポートを入力した後に使用可能になります。 証明書にエラーが含まれている場合、または信頼できない場合は、［**Integration Server への接続**］ウィンドウに対応するメッセージが表示されます。
受信済みの証明書を見る	行をクリックすると、Integration Server から受信した証明書に関する情報が表示されます。
無視する	受信した証明書を保存し、Integration Server への接続を続けるには、このオプションを選択します。 SSL 証明書で問題が発生した場合は、使用しているデータ伝送チャネルがセキュアであることを確認することを推奨します。
キャンセル	Integration Server への接続を終了するには、このオプションを選択します。
パスワード	Integration Server の管理者アカウントのパスワード（管理者アカウントのパスワード）。 パスワードの複雑性とブルートフォース攻撃防止メカニズムにより、6か月以内にパスワードが推測できないようにすることを推奨します。
確認す	ボタンをクリックすると、Web プラグインが Integration Server に接続されます。

る	管理者権限で Integration Server に接続した後、ポリシーはエージェントアカウントのパスワードを自動的に受け取り、このパスワードは Light Agent を Integration Server に接続するために使用されます。パスワードは暗号化された形式で保存されます。

SVM 接続タグ

このウィンドウでは、Light Agent がタグを使用できるようにし、Light Agent が接続に使用するタグを割り当てることができます。

接続タグの使用が Protection Server 設定でも設定されていることを確認してください：詳細については、『Kaspersky Security for Virtualization Light Agent のヘルプ』を参照してください。タグが割り当てられた Light Agent は、そのタグを持つ Light Agent への接続が許可されている SVM にのみ接続できます。

接続タグを使用するための設定

設定	説明
Light Agent 接続用のタグを使用	チェックボックスは、Light Agent による SVM 接続タグの使用を有効または無効にします。
タグ	Light Agent に割り当てられるタグ。 タグとして 255 文字までの文字列を入力できます。**;** を除く任意の記号が使用できます。 このフィールドは、［**Light Agent 接続用のタグを使用**］をオンにする場合に使用できます。

SVM 選択アルゴリズム

このウィンドウでは、Light Agents for Linux が使用する SVM 選択アルゴリズムを指定し、高度な SVM 選択アルゴリズムを使用するための設定を構成できます。

SVM 選択アルゴリズム

設定	説明
標準の SVM 選択アルゴリズムを使用する	このオプションが選択されている場合は、仮想マシンにインストールして実行した後、Light Agent は、Light Agent にローカルな接続先の SVM を選択します。詳細については、Kaspersky Hybrid Cloud Security for Virtualization Light Agent のヘルプを参照してください。 接続に使用可能なローカル SVM がない場合、Light Agent は、仮想インフラストラクチャ内の SVM の場所に関係なく、接続されている Light Agent が最も少ない SVM を選択します。 既定では、このオプションがオンです。
拡張 SVM 選択アルゴリズムを使用する	このオプションを選択した場合は、［**SVM パス**］スライダーを使用して、SVM が Light Agent に対してローカルであるかどうかを判断する時に、仮想インフラストラクチャ内の SVM の場所をどのように考慮するかを指定できます。Light Agent はローカルの SVM にのみ接続できます。 また、接続先の SVM を選択する時に、仮想インフラストラクチャ内の SVM パスを考慮しないように指定することもできます。 SVM を選択する時、Light Agent は SVM に接続されている Light Agent の数を考慮して、接続に使用可能な SVM 間で Light Agent が均等に分散されるようにします。
SVM パ	仮想インフラストラクチャ内の SVM パスの種別を指定することができ、接続する SVM を選

ス	択する時に考慮されます： • ［**ハイパーバイザー**］。Light Agent は、基準を満たす接続先の SVM を選択します（仮想インフラストラクチャの種別に応じて）： ◦ SVM は、Light Agent がインストールされた仮想マシンと同じハイパーバイザー上に導入されます（Microsoft Hyper-V プラットフォーム、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、Alt Virtualization Server、Astra Linux、または Numa vServer 上の仮想インフラストラクチャ内）。 ◦ SVM は、Light Agent がインストールされている仮想マシンと同じサーバーグループ内に配置されます（OpenStack Platform、VK Cloud プラットフォームまたは TIONIX Cloud Platform によって管理される仮想インフラストラクチャ内）。 Light Agent を含む仮想マシンが配置されている同じハイパーバイザー上または同じサーバーグループ内に接続に使用可能な SVM がない場合、Light Agent は SVM に接続しません。 • ［**クラスター**］。Light Agent は、基準を満たす接続先の SVM を選択します（仮想インフラストラクチャの種別に応じて）： ◦ SVM は、Light Agent がインストールされた仮想マシンと同じハイパーバイザークラスター内に導入されます（Microsoft Hyper-V プラットフォーム、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、Alt Virtualization Server、Astra Linux、または Numa vServer 上の仮想インフラストラクチャ内）。 ◦ SVM は、Light Agent がインストールされている仮想マシンと同じOpenStack プロジェクト内に導入されます（OpenStack Platform、VK Cloud プラットフォームまたは TIONIX Cloud Platform によって管理される仮想インフラストラクチャ内）。 Light Agent を含む仮想マシンが配置されている同じハイパーバイザークラスター内または同じ OpenStack プロジェクト内に接続に使用可能な SVM がない場合、Light Agent は SVM に接続しません。 • ［**データセンター**］。Light Agent は、基準を満たす接続先の SVM を選択します（仮想インフラストラクチャの種別に応じて）： ◦ SVM は、Light Agent がインストールされた仮想マシンと同じデータセンター内に導入されます（Microsoft Hyper-V プラットフォーム、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、Alt Virtualization Server、Astra Linux、または Numa vServer 上の仮想インフラストラクチャ内）。 ◦ SVM は、Light Agent がインストールされている仮想マシンと同じアベイラビリティゾーン内に配置されます（OpenStack Platform、VK Cloud プラットフォームまたは TIONIX Cloud Platform によって管理される仮想インフラストラクチャ内）。 Light Agent を含む仮想マシンが配置されている同じデータセンターまたはアベイラビリティゾーン内に接続に使用可能な SVM がない場合、Light Agent は SVM に接続しません。 • ［**SVM パスを無視**］。SVM を選択する時、Light Agent はその場所を考慮しません。 既定では［**ハイパーバイザー**］が選択されています。 このオプションは、［**拡張 SVM 選択アルゴリズムを使用**］が選択されている場合に使用できます。

Light Agent は高度な SVM 選択アルゴリズムを使用し、SVM アドレスのリストが SVM 発見方法として選択され、SVM で大規模インフラストラクチャ保護モードが有効になります（詳細については、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください）。この場合、SVM パスが無視された場合にのみ、Light Agent をこの SVM に接続できます。［**SVM パス**］設定を［**SVM パスを無視**］に設定する必要があります。それ以外の値に設定した場合、Light Agent は SVM に接続できなくなります。

接続の保護

このウィンドウでは、Light Agent と Protection Server 間のデータ伝送チャネルの暗号化を有効にすることができます

SVM の Protection Server 設定で、Light Agent と Protection Server 間のデータ伝送チャネルの暗号化が有効になっていることを確認してください。詳細については、『Kaspersky Hybrid Cloud Security for Virtualization Light Agent のヘルプ』を参照してください。

接続保護設定

設定	説明
Light Agent と Protection Server 間のデータチャネルの暗号化	暗号化を使用して、Light Agent と Protection Server の間の接続を保護します。 このチェックボックスをオンにすると、ポリシーによって管理される Light Agent と、Light Agent が接続している SVM 上の Protection Server との間にセキュアな接続が確立されます。接続保護が有効になっている Light Agent は、接続保護が有効になっているか、Protection Server への保護されていない接続が許可されている SVM にのみ接続できます。 このチェックボックスをオフにすると、Light Agent と、Light Agent が接続している SVM 上の Protection Server との間に保護されていない接続が確立されます。 既定では、このチェックボックスはオフです。

管理コンソールでの Light Agent の設定

管理コンソールでは、ポリシーのプロパティ（**Light Agent モード**）で、Light Agent を SVM に接続するための設定を構成できます。

Integration Server への接続

このセクションで説明する設定は、Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合にのみ適用されます。

Light Agent が統合サーバーを通じて SVM に関する情報を受信する場合、または保護サーバーと Light Agent 間の接続を保護する場合は、統合サーバーへの接続が要求されます。

このウィンドウには、Light Agent を Integration Server に接続するための現在の設定（接続用のアドレスとポート）が表示されます。［**編集**］をクリックすると、［**Integration Server への接続**］ウィンドウが開き、Integration Server への接続を設定できます。

［Integration Server への接続］ウィンドウ

このウィンドウでは、Light Agent を Integration Server に接続するための設定を指定または変更できます。

Integration Server 接続設定

設定	説明
アドレス	Integration Server がインストールされているデバイスの IPv4 形式の IP アドレスまたは完全修飾ドメイン名（FQDN）。 Kaspersky Security Center 管理コンソールがインストールされているデバイスがドメインの一部である場合、既定ではフィールドにこのデバイスのドメイン名が表示されます。 Kaspersky Security Center 管理コンソールがインストールされているデバイスがドメインの一部ではない場合、または Integration Server が別のデバイスにインストールされている場合は、フィールドに手動で入力する必要があります。 アドレスとして NetBIOS 名、「localhost」、または 127.0.0.1 が指定されている場合、Integration Server への接続はエラーが発生して失敗します。
Port	Integration Server に接続するためのポート。 ポート 7271 が既定で使用されます。

［Integration Server の証明書を検証］ウィンドウ

このウィンドウは、Integration Server から受信した SSL 証明書にエラーが含まれているか、信頼されていない場合に表示されます。

ウィンドウ内のリンクをクリックすると、受信した証明書の詳細を表示できます。

SSL 証明書で問題が発生した場合は、使用しているデータ伝送チャネルがセキュアであることを確認することを推奨します。

Integration Server への接続を続行するには、［**無視する**］をクリックします。受信した証明書は、Kaspersky Security Center 管理コンソールがインストールされているデバイスに信頼できる証明書としてインストールされます。

［Integration Server での認証］ウィンドウ

このウィンドウは、Kaspersky Security Center 管理コンソールをホストしているデバイスがドメインに属していない場合、またはアカウントが KLAdmins ローカルグループ、ドメイングループ、またはローカル管理者グループに属していない場合に表示されます。

Integration Server の管理者パスワード（`admin` アカウントのパスワード）を指定し、［**OK**］をクリックします。

パスワードの複雑性とブルートフォース攻撃防止メカニズムにより、6か月以内にパスワードが推測できないようにすることを推奨します。

管理者権限で Integration Server に接続した後、ポリシーは agent アカウントのパスワードを自動的に受け取り、このパスワードは Light Agent を Integration Server に接続するために使用されます。

SVM 検出設定

このセクションで説明する設定は、Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合にのみ適用されます。

このウィンドウでは、Light Agent が接続可能な SVM を検出するために使用する方法を選択できます。

SVM 検出設定

設定	説明
Integration Server を使用する	このオプションがオンにされている場合、Light Agent は Integration Server に接続し、接続可能な SVM のリストとそれらに関する情報を取得します。 Integration Server を使用する場合は、Light Agent を Integration Server に接続するための設定を行う必要があります。
SVM アドレスのカスタムリストの使用	このオプションを選択する場合は、このポリシーによって管理される Light Agent が接続できる SVM のリストを指定できます。Light Agent は、リストで指定された SVM にのみ接続します。
SVM のリスト	ポリシーによって管理されている Light Agent が接続できる SVM の IPv4 形式の IP アドレスまたは完全修飾ドメイン名（FQDN）のリスト。 ［**追加**］をクリックするとウィンドウが開き、IPv4 形式の IP アドレスまたは SVM の完全修飾ドメイン名（FQDN）を指定できます。SVM の複数の IP アドレスまたは FQDN を新しい行に入力できます。 単一の IP アドレスにマップされる完全修飾ドメイン名（FQDN）のみを指定します。複数の IP アドレスに対応する完全修飾ドメイン名を使用すると、アプリケーションでエラーが発生する可能性があります。 ［**削除**］をクリックすると、リストで選択したアドレスを削除できます。 ［**SVM アドレスのカスタムリストを使用する**］が選択されている場合は、SVM アドレスのリストが表示されます。

［**SVM アドレスのカスタムリストを使用する**］をオンにした場合、Light Agent は高度な SVM 選択アルゴリズムを使用し、SVM で大規模インフラストラクチャ保護モードが有効になります（詳細については、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください）。この場合、SVM パスが無視された場合にのみ、Light Agent をこの SVM に接続できます。［**SVM 選択アルゴリズム**］セクションで、［**SVM パス**］設定を［**SVM パスを無視**］に設定する必要があります。それ以外の値に設定した場合、Light Agent は SVM に接続できなくなります。

SVM 接続タグ

このウィンドウでは、Light Agent がタグを使用できるようにし、Light Agent が接続に使用するタグを割り当てることができます。

接続タグの使用が Protection Server 設定でも設定されていることを確認してください：詳細については、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください。タグが割り当てられた Light Agent は、そのタグを持つ Light Agent への接続が許可されている SVM にのみ接続できます。

接続タグを使用するための設定

設定	説明
Light Agent 接続用のタグを使用	チェックボックスは、Light Agent による SVM 接続タグの使用を有効または無効にします。
タグ	Light Agent に割り当てられるタグ。 タグとして 255 文字までの文字列を入力できます。**;** を除く任意の記号が使用できます。 このフィールドは、［**Light Agent 接続用のタグを使用**］をオンにする場合に使用できます。

SVM 選択アルゴリズム

このウィンドウでは、Light Agents for Linux が使用する SVM 選択アルゴリズムを指定し、高度な SVM 選択アルゴリズムを使用するための設定を構成できます。

SVM 選択アルゴリズム

設定	説明
標準の SVM 選択アルゴリズムを使用する	このオプションが選択されている場合は、仮想マシンにインストールして実行した後、Light Agent は、Light Agent にローカルな接続先の SVM を選択します。詳細については、Kaspersky Hybrid Cloud Security for Virtualization Light Agent のヘルプを参照してください。 接続に使用可能なローカル SVM がない場合、Light Agent は、仮想インフラストラクチャ内の SVM の場所に関係なく、接続されている Light Agent が最も少ない SVM を選択します。 既定では、このオプションがオンです。
拡張 SVM 選択アルゴリズムを使用する	このオプションを選択した場合は、［**SVM パス**］スライダーを使用して、SVM が Light Agent に対してローカルであるかどうかを判断する時に、仮想インフラストラクチャ内の SVM の場所をどのように考慮するかを指定できます。Light Agent はローカルの SVM にのみ接続できます。 また、接続先の SVM を選択する時に、仮想インフラストラクチャ内の SVM パスを考慮しないように指定することもできます。 SVM を選択する時、Light Agent は SVM に接続されている Light Agent の数を考慮して、接続に使用可能な SVM 間で Light Agent が均等に分散されるようにします。
SVM パス	仮想インフラストラクチャ内の SVM パスの種別を指定することができ、接続する SVM を選択する時に考慮されます： • ［**ハイパーバイザー**］。Light Agent は、基準を満たす接続先の SVM を選択します（仮想インフラストラクチャの種別に応じて）：

- SVM は、Light Agent がインストールされた仮想マシンと同じハイパーバイザー上に導入されます（Microsoft Hyper-V プラットフォーム、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、Alt Virtualization Server、Astra Linux、または Numa vServer 上の仮想インフラストラクチャ内）。

- SVM は、Light Agent がインストールされている仮想マシンと同じサーバーグループ内に配置されます（OpenStack Platform、VK Cloud プラットフォームまたは TIONIX Cloud Platform によって管理される仮想インフラストラクチャ内）。

Light Agent を含む仮想マシンが配置されている同じハイパーバイザー上または同じサーバーグループ内に接続に使用可能な SVM がない場合、Light Agent は SVM に接続しません。

- ［**クラスター**］。Light Agent は、基準を満たす接続先の SVM を選択します（仮想インフラストラクチャの種別に応じて）：

  - SVM は、Light Agent がインストールされた仮想マシンと同じハイパーバイザークラスター内に導入されます（Microsoft Hyper-V プラットフォーム、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、Alt Virtualization Server、Astra Linux、または Numa vServer 上の仮想インフラストラクチャ内）。

  - SVM は、Light Agent がインストールされている仮想マシンと同じOpenStack プロジェクト内に導入されます（OpenStack Platform、VK Cloud プラットフォームまたは TIONIX Cloud Platform によって管理される仮想インフラストラクチャ内）。

Light Agent を含む仮想マシンが配置されている同じハイパーバイザークラスター内または同じ OpenStack プロジェクト内に接続に使用可能な SVM がない場合、Light Agent は SVM に接続しません。

- ［**データセンター**］。Light Agent は、基準を満たす接続先の SVM を選択します（仮想インフラストラクチャの種別に応じて）：

  - SVM は、Light Agent がインストールされた仮想マシンと同じデータセンター内に導入されます（Microsoft Hyper-V プラットフォーム、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、Alt Virtualization Server、Astra Linux、または Numa vServer 上の仮想インフラストラクチャ内）。

  - SVM は、Light Agent がインストールされている仮想マシンと同じアベイラビリティゾーン内に配置されます（OpenStack Platform、VK Cloud プラットフォームまたは TIONIX Cloud Platform によって管理される仮想インフラストラクチャ内）。

Light Agent を含む仮想マシンが配置されている同じデータセンターまたはアベイラビリティゾーン内に接続に使用可能な SVM がない場合、Light Agent は SVM に接続しません。

- ［**SVM パスを無視**］。SVM を選択する時、Light Agent はその場所を考慮しません。

既定では［**ハイパーバイザー**］が選択されています。

このオプションは、［**拡張 SVM 選択アルゴリズムを使用**］が選択されている場合に使用できます。

Light Agent は高度な SVM 選択アルゴリズムを使用し、SVM アドレスのリストが SVM 発見方法として選択され、SVM で大規模インフラストラクチャ保護モードが有効になります（詳細については、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください）。この場合、SVM パスが無視された場合にのみ、Light Agent をこの SVM に接続できます。［**SVM パス**］設定を［**SVM パスを無視**］に設定する必要があります。それ以外の値に設定した場合、Light Agent は SVM に接続できなくなります。

接続の保護

このウィンドウでは、Light Agent と Protection Server 間のデータ伝送チャネルの暗号化を有効にすることができます

SVM の Protection Server 設定で、Light Agent と Protection Server 間のデータ伝送チャネルの暗号化が有効になっていることを確認してください。詳細については、『Kaspersky Hybrid Cloud Security for Virtualization Light Agent のヘルプ』を参照してください。

接続保護設定

設定	説明
Light Agent と Protection Server 間のデータチャネルの暗号化	暗号化を使用して、Light Agent と Protection Server の間の接続を保護します。 このチェックボックスをオンにすると、ポリシーによって管理される Light Agent と、Light Agent が接続している SVM 上の Protection Server との間にセキュアな接続が確立されます。接続保護が有効になっている Light Agent は、接続保護が有効になっているか、Protection Server への保護されていない接続が許可されている SVM にのみ接続できます。 このチェックボックスをオフにすると、Light Agent と、Light Agent が接続している SVM 上の Protection Server との間に保護されていない接続が確立されます。 既定では、このチェックボックスはオフです。

コマンドラインで Light Agent モードのアプリケーション使用に関する情報を表示する

コマンドラインでは、仮想環境を保護する Light Agent モードでのアプリケーションの使用について、以下の情報を表示できます：

- Light Agent モードで本製品を使用する際の設定
- Light Agent と Integration Server の接続
- Light Agent と SVM の接続

Light Agent モードでアプリケーションを使用するための設定に関する情報を表示するには、次を実行します：

```
kesl-control [-V] --ksvla-info
```

コマンドは次の情報をコンソールに出力します：

- 仮想環境を保護する Light Agent モード：有効 / 無効。

  Light Agent モードが有効な場合、アプリケーションは Kaspersky Hybrid Cloud Security for Virtualization Light Agent の一部として Light Agent として使用されます。Light Agent モードが無効の場合、アプリケーションは標準モードで使用されます。

- VDI 保護モード：有効 / 無効。

VDI 保護モードは、一時的な仮想マシン上での Kaspersky Endpoint Security の動作を最適化します。VDI 保護モードが有効な場合、保護された仮想マシンの再起動が必要なアップデートは一時的な仮想マシンにはインストールされません。再起動が必要なアップデートを受信すると、一時的な仮想マシンにインストールされた Light Agent から Kaspersky Security Center に対して、保護された仮想マシンのテンプレートを更新する必要がある旨のメッセージが送信されます。

- 保護対象の仮想マシンの種別：一時的または永続的。
- 仮想インフラストラクチャにおける仮想マシンの役割：サーバーまたはワークステーション。
- 保護対象の仮想マシンの識別子（UUID）。

Light Agent を Integration Server に接続するための情報を表示するには、次を実行します：

```
kesl-control [-V] --viis-info
```

コマンドは次の情報をコンソールに出力します：

- Light Agent が接続する Integration Server のアドレスとポート。
- Integration Server への接続のステータスです。
- Light Agent と Integration Server 間の最終接続日時。

Light Agent と SVM の接続に関する情報を表示するには、次を実行します：

```
kesl-control [-V] --svm-info
```

コマンドは次の情報をコンソールに出力します：

- Light Agent が接続されている SVM のアドレスと、Light Agent に対する仮想インフラストラクチャ内の SVM の場所：ローカルまたはローカル以外。
- Light Agent が SVM を検出する方法：Integration Server を使用するか、または手動で定義した SVM アドレスのリストを使用します。
- 選択された SVM 検出方法が SVM アドレスのリストである場合、SVM アドレスのリスト。
- Light Agent を SVM に接続するためのタグ。
- SVM の選択アルゴリズム：標準または高度。高度な SVM 選択アルゴリズムが使用されている場合は、仮想インフラストラクチャ内の SVM の場所の種別も表示されます。
- Light Agent と Protection Server 間の接続の保護。

Light Agent と Integration Server および SVM の接続設定については、Kaspersky Security for Virtualization Light Agent のヘルプ を参照してください。

イベントとレポートの表示

製品の実行中は、様々なイベントが発生する可能性があります。イベントは情報提供である場合もあれば、重要なデータが含まれている場合もあります。たとえば、製品はイベントを使用して、定義データベースのアップデートが成功したことを通知したり、削除する必要のある製品コンポーネントの動作のエラーについて通知したりします。

Kaspersky Endpoint Security は、アプリケーション イベントに関する情報を次のログに保存します：

- 製品のイベントログ。既定では、イベントに関する情報は、データベース /var/opt/kaspersky/kesl/private/storage/events.db に保存されます。コマンドラインでアプリケーションイベントログを設定できます。
- オペレーティングシステムログ（syslog）。オペレーティングシステムログは、既定では使用されていません。このログへのイベントの保存を有効化できます。

アプリケーションイベントログとオペレーティングシステムログにアクセスするには、root 権限が必要です。

Kaspersky Endpoint Security が Kaspersky Security Center によって管理されている場合、イベントに関する情報が Kaspersky Security Center 管理サーバーに送信される場合があります。特定のイベントには集約ルールが適用されます。アプリケーションの実行中に短時間で大量の同じタイプのイベントが作成された場合は、アプリケーションはイベント集約モードに切り替え、イベント設定の説明とともに集約された 1 つのイベントを Kaspersky Security Center に送信します。異なるイベントには、異なる集約ルールを使用することができます。イベントの詳細は、Kaspersky Security Center のヘルプを参照してください。

本製品に関する情報は、次の方法で受け取ることができます：

- 管理コンソールと Web コンソールで
- コマンドラインで
- Kaspersky Endpoint Security グラフィカルユーザーインターフェイスを使用している場合、製品のポップアップウィンドウで

一部のイベントにはファイルパスが含まれる場合があります。出力の場合、ファイルパスは UTF-8 文字列として扱われます。パス内のいずれかのバイトが UTF-8 エンコード規則に準拠していない場合、そのバイトは ? 文字に置き換えられます。Unicode 範囲外の文字コード（0x10FFFF より大きい）をエンコードする 4 バイトシーケンスも、? 文字に置き換えられます。特殊文字は特定の方法でエスケープ（置換）されます。

`kesl-control -E --query` の出力内のイベント内のファイルパスの文字をエスケープする場合は、次のルールが適用されます：

- '\a'、'\b'、'\t'、'\n'、'\v'、'\f'、'\r' の文字は、次の 2 文字に置き換えられます：

  '\a' -> "\\a"

  '\b' -> "\\b"

  '\t' -> "\\t"

  '\n' -> "\\n"

  '\v' -> "\\v"

  '\f' -> "\\f"

  '\r' -> "\\r"

- その他の特殊文字はすべて変更されずに出力されます。

`kesl-control -E --query --json` の出力内のイベント内のファイルパスの文字をエスケープする場合は、次のルールが適用されます：

- JSON 形式に従って、'\b'、'\f'、'\n'、'\r'、'\t'、'"'、'\\' 文字は次のようにエスケープされます：

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\\""

  '\\' -> "\\\\"

- その他の特殊文字は、特殊文字をエスケープするための一般的な JSON ルールに従ってエスケープされます（'\a' -> '\u0007 '）。

syslog に送信する際のイベント内のファイルパス内の文字をエスケープするためのルール：

- JSON 形式に従って、'\b'、'\f'、'\n'、'\r'、'\t'、'"'、'\\' 文字は次のようにエスケープされます：

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\\""

  '\\' -> "\\\\"

- その他の特殊文字は、特殊文字をエスケープするための一般的な JSON ルールに従ってエスケープされます（'\a' -> '\u0007 '）。

ルールを記述する際のシーケンス内の最初のバックスラッシュはエスケープ文字です。

例：
`'\a'` は 1 文字（制御文字）です。

`'\\a'` は 2 文字（バックスラッシュ + a 文字）です。

`'\\'` は 1 文字（バックスラッシュ）で、`'\\\\'` は 2 文字（バックスラッシュ + バックスラッシュ）です。

製品の実行中に発生するイベントの様々な種別のレポートを生成できます。各 Kaspersky Endpoint Security コンポーネントの動作、各タスクの結果、および製品の全体的な動作に関する情報は、レポートに含まれます。

レポートは、次の方法で表示できます：

- Kaspersky Security Center レポートは、管理コンソールと Web コンソールで利用できます。これらを使用すると、感染したファイル、ライセンスや定義データベースの使用状況などに関する情報を取得できます。Kaspersky Security Center を使用した管理に関する詳細は、Kaspersky Security Center のヘルプを参照してください。

- アプリケーションレポートは、Kaspersky Endpoint Security のグラフィカルユーザーインターフェイスで利用できます。

イベントとレポートには、以下の個人データが含まれる場合があります：

- オペレーティングシステムユーザーのユーザー名とユーザー ID
- ユーザーファイルへのパス
- アンチクリプターコンポーネントによってスキャンされるリモートデバイスの IP アドレス
- ファイアウォール管理コンポーネントによってスキャンされるネットワークパケットの送信者と受信者の IP アドレス
- アップデート元の URL
- 全般的な製品設定値
- コマンドラインタスクの名前と設定
- 悪意のあるフィッシング、アドウェアの URL、および侵入者がデバイスやデータを侵害するために使用できる正規のアプリケーションを含む URL の検知
- コンテナとイメージの名前
- コンテナとイメージへのパス
- デバイスの名前と ID
- リポジトリの URL
- ファイル名、ファイルへのパス、実行ファイルのハッシュ値
- アプリケーションカテゴリの名前

オペレーティングシステムログへのイベントログの記録設定

既定では、Kaspersky Endpoint Security の動作中に発生したイベントはオペレーティングシステムのログには記録されません。Web コンソール、管理コンソール、またはコマンド ラインを使用して、このログへのイベントの記録を有効にできます。

Kaspersky Security Center では、オペレーティングシステムログに保存するイベントを選択することもできます。

Web コンソールでのポリシーの設定

Web コンソールでは、ポリシープロパティ（**製品設定 → 全般設定 → 製品設定**）でオペレーティングシステムログへのイベントのログ記録を設定できます。

通知セクションの**通知を設定**リンクをクリックすると、**通知**ウィンドウが開きます。このウィンドウでは、チェックボックスを使用して、アプリケーションがオペレーティングシステムログに記録するイベントを選択できます。

個々のイベント種別を選択することも、特定の重大度レベルを持つすべてのイベント種別を選択することもできます。

既定では、すべてのチェックボックスがオフになっています。

管理コンソールでのポリシーの設定

管理コンソールでは、ポリシープロパティ（**全般設定 → 製品設定**）でオペレーティングシステムログへのイベントのログ記録を設定できます。

通知から**設定**をクリックすると、**通知設定**ウィンドウが表示されます。このウィンドウでは、チェックボックスを使用して、アプリケーションがオペレーティングシステムログに記録するイベントを選択できます。

個々のイベント種別を選択することも、特定の重大度レベルを持つすべてのイベント種別を選択することもできます。

既定では、すべてのチェックボックスがオフになっています。

コマンドラインでの設定

アプリケーションの全般設定の`UseSyslog`オプションを使用して、コマンドラインでオペレーティングシステムログにイベントを保存するかどうかを設定できます。

コマンドラインスイッチまたはアプリケーションの全般設定のすべてを含む設定情報ファイルを使ってオプションを編集できます。

`UseSyslog` では次の値を利用できます：

- `Yes`：Syslog へイベントの保存を有効にする。
- `No`（規定）：Syslog へイベントの保存を無効にする。

アプリケーションのイベントログの設定方法

既定では、イベントに関する情報は、デバイス上にあるアプリケーションイベントログに保存されます。次のアプリケーションイベントログのオプションは、アプリケーションの全般設定を介して、コマンドラインから定義できます：

- `EventsStoragePath` のオプションを介して、アプリケーションイベントログデータベースにパスを変更します。既定値：/var/opt/kaspersky/kesl/private/storage/events.db
- `MaxEventsNumber` のオプションで、アプリケーションが保存するイベントの最大数を指定します。既定値：500000指定されたイベントの数を超えると、最も古いイベントから削除されます。

コマンドラインスイッチまたはアプリケーションの全般設定をすべて含む設定情報ファイルを使用して、設定値を変更できます。

Kaspersky Security Center でのイベントの表示

すべての Kaspersky Endpoint Security イベントのリストが Web コンソールと管理コンソールに表示されます。

イベント通知を設定できます。*通知*は、保護対象デバイスで発生したイベントに関する情報を含むメッセージです。通知により、アプリケーションイベントに関する情報がタイムリーに提供されます。本製品からのイベント受信時、またはイベント通知のメール受信時に、スクリプトの実行を設定できます。

Kaspersky Security Center 通知の詳細については、Kaspersky Security Center のヘルプを参照してください。

コマンドラインのイベントの表示

コマンドラインでは、次の内容を表示できます：

- 現在の製品イベント
- 製品のイベントログのイベント

現在のイベントの表示

現在のすべてのアプリケーションイベントに関する情報、または指定したタスクの開始または停止に関連する現在のイベントに関する情報を出力できます。フィルターを使用して、特定の現在のイベント（指定した種別のイベントなど）を出力できます。

現在のすべてのアプリケーションイベントに関する情報を出力するには、次のコマンドを実行します：

```
kesl-control -W
```

このコマンドにより、イベント名、およびイベントに関する追加情報が表示されます。

実行中のタスクに関連付けられた現在のイベントに関する情報のみを出力するには、次のコマンドを実行します：

```
kesl-control --start-task <タスク ID / 名> -W
```

例：
ID が「1」の実行中のタスクの、現在のイベントの表示を有効にします：

```
kesl-control --start-task 1 -W
```

フィルター条件に一致する現在のイベントに関する情報を出力するには、次のコマンドを実行します：

```
kesl-control -W --query "<フィルター条件>"
```

フィルター条件は、<フィールド> <比較演算子> '<値>' 形式の1つまたは複数の論理式によって設定されています。論理演算子と組み合わせて。

例：
TaskStateChanged イベントを表示します：

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

例：
「User」ユーザーによって開始された TaskSettingsChanged イベントを表示します：

```
kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'""
```

イベントログからのイベントの表示

イベントに関する情報をアプリケーションイベントログからコンソールまたはファイルに出力できます。フィルターを使用して、特定のイベントのみを表示できます。

アプリケーションイベントログ内のすべてのイベントに関する情報を出力するには、次のコマンドを実行します：

```
kesl-control -E --query [--db <データベースファイル>]
```

説明：

- <データベースファイル> は、イベントの出力元となるイベントログデータベースファイルへの絶対パスです。既定では、イベントに関する情報は、データベース /var/opt/kaspersky/kesl/private/storage/events.db に保存されます。データベースの場所は、EventsStoragePath のアプリケーショングローバル設定によって決まります。

`less` を使用して、表示されたイベントのリストを操作できます。既定では、保存可能なイベントの数は最大で 500 000 です。アプリケーションが保存するイベントの最大数は、 アプリケーションの全般設定にある `MaxEventsNumber` によって決まります。

イベントログが既定のデータベースにある場合は、次のコマンドを使用してすべてのイベントに関する情報を出力できます：

```
kesl-control -E
```

特定の条件を満たすイベントに関する情報をアプリケーションイベントログに出力するには、次のコマンドを実行します：

```
kesl-control -E --query "<フィルター条件>" [--db <データベースファイル>] [-n <数値>] [--json] [--reverse]
```

説明：

- <フィルター条件>：<フィールド> <比較演算子> '<値>' 形式の 1 つまたは複数の論理式。論理演算子と組み合わせて、結果を限定します。
- <数値> - 表示される選択の最新のイベントの数（選択の最後からのレコードの数）。
- `--json`：イベントを JSON 形式で出力します。
- `--reverse`：イベントを逆の順序で表示します（最新のイベントが上に表示され、最も古いイベントが下に表示されます）。

特定の条件を満たすイベントに関する情報をアプリケーションイベントログをファイルに出力するには、次のコマンドを実行します：

```
kesl-control -E --query "<フィルター条件>" [--db <データベースファイル>] [-n <数値>] --file <ファイル名とパス> [--json]
```

`--file` <ファイル名とパス> は、イベントを出力するファイルへの絶対パスです。

アプリケーションコンポーネントの変更チェック

本製品には、様々なバイナリモジュールが多数含まれています。モジュールの形式は、ダイナミックリンクライブラリ、実行ファイル、設定情報ファイル、インターフェイスファイルです。侵入者により、1個以上のアプリケーションの実行モジュールまたはファイルが、悪意のあるコードを含む別のファイルに置換される可能性があります。モジュールやファイルの置換を防止するために、本製品はアプリケーションコンポーネントの変更をチェックできます。モジュールとファイルに不正な変更または破損がないかをチェックします。モジュールまたはファイルチェックサムが正しくない場合、破損していると認識されます。

デバイスに以下のアプリケーションコンポーネントがインストールされている場合は、それに対する完全性チェックを実行します：

- 製品パッケージ
- グラフィカルユーザーインターフェイスパッケージ
- Kaspersky Security Center ネットワークエージェントパッケージ
- Kaspersky Endpoint Security 管理プラグイン

*マニフェストファイル*と呼ばれる特別なリスト内のファイルの変更をチェックします。製品コンポーネントが正しく動作するためには、アプリケーションファイルの整合性が重要であり、各製品コンポーネントにはそのアプリケーションファイルのリストを含む独自のマニフェストファイルがあります。マニフェストファイルの名前は各コンポーネントで同じですが、マニフェストファイルの内容は異なります。マニフェストファイルはデジタル署名されており、その変更もチェックされます。

製品コンポーネントの変更は、整合性チェックユーティリティを使用してチェックされます。

変更チェックユーティリティは、root 権限を持つアカウントで実行する必要があります。

変更を確認するには、本製品とともにインストールされたユーティリティ、または認定済みの CD で配布されたユーティリティを使用できます。

認定済みの CD から変更チェックユーティリティを実行し、ユーティリティの整合性を確認することを推奨します。CD からユーティリティを実行する場合は、マニフェストファイルへの絶対パスを指定します。

製品と一緒にインストールされる変更チェックユーティリティは、以下のパスにあります：

- 製品パッケージ、グラフィカルユーザーインターフェイスパッケージ、ネットワークエージェントをチェック：/opt/kaspersky/kesl/bin/integrity_checker
- Kaspersky Endpoint Security 管理プラグインをチェック - 管理プラグインの実行モジュール（DLL）があるディレクトリ：
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<プラグインのバージョン>.plg\integrity_checker.exe - 32 ビットオペレーティングシステムの場合
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<プラグインのバージョン>.plg\integrity_checker.exe - 64 ビットオペレーティングシステムの場合

マニフェストファイルは、以下のパスにあります：

- /opt/kaspersky/kesl/bin/integrity_check.xml - 製品パッケージの変更をチェック。
- /opt/kaspersky/kesl/bin/gui_integrity_check.xml - グラフィカルユーザーインターフェイスの変更をチェック。
- /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml - 32 ビットオペレーティングシステムのネットワークエージェントをチェック。
- /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml - 64 ビットオペレーティングシステムのネットワークエージェントをチェック。

製品コンポーネントの変更をチェックするには、次のコマンドを実行します：

- 製品 パッケージとグラフィカル ユーザー インターフェイス パッケージを確認するには:

  `integrity_checker [<manifest ファイルへのパス>] --signature-type kds-with-filename`

- Kaspersky Endpoint Security 管理プラグインとネットワーク エージェントを確認するには：

  `integrity_checker [<manifest ファイルへのパス>]`

  既定のパスは、システム変更チェックユーティリティと同じディレクトリに配置された manifest ファイルへのパスです。

ユーティリティは、以下のオプション設定を使用して実行できます：

- `--crl <ディレクトリ>` - 証明書失効リストを含むディレクトリへのパス。
- `--version` - ユーティリティのバージョンを表示します。
- `--verbose` - 実行動作と結果に関する詳細な情報を表示します。この設定を指定しない場合、エラー、チェックをパスしなかったオブジェクト、スキャン統計のサマリーのみが表示されます。
- `--trace <ファイル名>` - `<ファイル名>`は、スキャン中に間に発生したイベントが DEBUG 詳細レベルでログに記録されるファイル名です。
- `--signature-type kds-with-filename` – チェックする署名のタイプ（この設定は、アプリケーションのパッケージ、グラフィカルユーザーインターフェイスのパッケージ、ネットワークエージェントのチェックに必要です）。
- `--single-file <ファイル>` - マニフェスト内の 1 つのファイルだけをスキャンし、他のオブジェクトを無視します。

`integrity_checker --help` コマンドを実行すると、ユーティリティオプションのヘルプで使用可能なすべての変更チェックユーティリティ設定の説明を表示できます。

マニフェストファイルのチェック結果は、次のように表示されます：

- `SUCCEEDED` - ファイルの整合性が確認されました（リターンコード 0）。
- `FAILED` - ファイルの整合性が確認されませんでした（リターンコードが 0 以外）。

製品の起動時にアプリケーションまたはネットワークエージェントの整合性違反が検出された場合、Kaspersky Endpoint Security はイベントログと Kaspersky Security Center で *IntegrityCheckFailed* イベントを生成します。

グラフィカルユーザーインターフェイス経由のアプリケーション管理

仮想環境の保護に Kaspersky Endpoint Security を Light Agent モードで使用している場合、グラフィカルユーザーインターフェイスには対応していません。

Kaspersky Endpoint Security のグラフィカルユーザーインターフェイスを使用して、次の操作ができます：

- デバイスの保護ステータスに関する情報を表示。
- 製品コンポーネントの有効化または無効化：
  - ファイル脅威対策。
  - リムーバブルドライブスキャン。
  - ウェブ脅威対策。
  - ネットワーク脅威対策。
  - アンチクリプター。
  - ファイアウォール管理。
  - アプリケーションコントロール。
  - デバイスコントロール。
  - ふるまい検知。
  - システム変更監視。
- スキャンタスクの開始と停止：
  - マルウェアのスキャン。
  - 簡易スキャン。
  - コンテナのスキャン。
- アップデートおよびロールバックタスクの開始と停止。
- スキャンするファイルまたはディレクトリをクリックしてオブジェクトスキャンを実行。
- Kaspersky Security Network を有効化または無効化。
- アプリケーションの統計とレポートを表示。
- 製品のライセンスを管理し、使用されているライセンスとライセンスに関連付けられているライセンスに関する情報を表示します。
- Backup に配置されたオブジェクトの情報を表示。
- アプリケーショントレースファイルを作成。

アプリケーションコンポーネントまたはタスクが「通知のみ」モードで実行されている場合、コンポーネントまたはタスクの GUI に *「通知のみ」モードが選択されていること*を示す警告が表示されます。

グラフィカルユーザーインターフェイス

通知領域の製品アイコン

Kaspersky Endpoint Security のグラフィカルユーザーインターフェイスをデバイスにインストールすると、タスクバー内の通知領域の右側に製品アイコンが表示されます。

製品アイコンは、コンテキストメニューとメインウィンドウへのショートカットとして機能します。

製品アイコンのコンテキストメニューには、次の項目が含まれています：

- **Kaspersky Endpoint Security 12.1 for Linux**。メインウィンドウが開きます。このウィンドウには、デバイスの保護ステータスが表示され、本製品の機能へアクセスするためのインターフェイス要素が含まれています。
- **終了**：製品のグラフィカルユーザーインターフェイスを終了します。

メインウィンドウ

メインウィンドウを開くには、次のいずれかの操作を実行します：

- タスクバーの通知領域にある本製品のアイコンを右クリックまたはダブルクリックします。
- オペレーティングシステムのウィンドウマネージャのアプリケーションメニューで、アプリケーション名を選択します。

メインウィンドウはいくつかのパートに分割されます：

- メインウィンドウの中央部には、デバイスの保護ステータスが表示されます。ウィンドウのこの部分をクリックすると、［**プロテクションセンター**］ウィンドウが表示されます。このウィンドウには、デバイスの保護ステータスに関する情報と、保護の問題を修正するために実行する処理に関する推奨事項（ある場合）が表示されます。
- ［**スキャン**］は、マルウェアのスキャンタスクのステータスと、検知した脅威の数を表示します。このボタンをクリックすると、［**スキャン**］ウィンドウが表示されます。このウィンドウでは、*マルウェアのスキャンタスク*、*簡易スキャン*、*コンテナースキャンタスク*の開始と停止ができます。また、これらのタスクのレポートを表示することもできます。
- **アップデート**は、*アップデート*タスクのステータスを表示します。このボタンをクリックすると、［**アップデート**］ウィンドウが表示されます。このウィンドウでは、*アップデート*タスクや*ロールバック*タスクを開始できます。また、これらのタスクのレポートを表示することもできます。
- メインウィンドウの下部には、次の要素が含まれています：
  - ［**レポート**］：このボタンをクリックすると**レポート**ウィンドウが表示されます。このウィンドウでは、コンポーネントとタスクの統計情報など様々なレポートを確認できます。
  - **バックアップ**ボタン。このボタンをクリックすると［**バックアップ**］ウィンドウが表示されます。このウィンドウでは、バックアップ内のオブジェクトに関する情報を確認できます。

- ［**設定**］ボタン：このボタンをクリックすると、**設定**ウィンドウが表示されます。このウィンドウでは、アプリケーションコンポーネントを有効または無効にし、Kaspersky Security Network を設定できます。

- ［**サポート**］：このボタンをクリックすると**サポート**ウィンドウが開き、本製品の現在のバージョンと次の情報が表示されます：

  - **ライセンス** – 本製品に追加された現在のライセンス、またはライセンスが追加されていないことを示すメッセージです。このフィールドのリンクをクリックすると、**ライセンス**ウィンドウが開き、詳細なライセンスの情報が表示されます。

  - **ライセンスのステータス** – 現在のライセンスのステータスに関する情報、またはライセンスが追加されていないことを示すメッセージです。

  - **データベースのリリース日** – 定義データベースのステータスとリリース日。

  - **オペレーティングシステム** – デバイスのオペレーティングシステムに関する情報です。

  サポートウィンドウの下部には、カスペルスキー の情報リソースへのリンクと、**トレース**ウィンドウを開くリンクが表示されます。このウィンドウでは、製品のトレースファイルを作成し、トレースファイルの詳細レベルを設定できます。

- メインウィンドウの下部には、ライセンスに関する情報、およびライセンスの問題（ある場合）に関する情報が表示されます。ウィンドウのこの領域をクリックすると、**ライセンス**ウィンドウが開き、詳細なライセンスの情報が表示されます。

  このウィンドウの［**ライセンスを購入**］ボタンをクリックすると、カスペルスキーオンラインストアが開き、ライセンスを購入できます。ライセンスを購入すると、製品を有効化するために使用する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が送信されます。

製品コンポーネントの有効化または無効化

グラフィカルユーザーインターフェースを使用して、アプリケーションコンポーネントを有効または無効にできます。コンポーネントを有効にすると、［**無効**］が使用可能になります。既定では、次のコンポーネントが有効になっています：ファイル脅威対策、デバイスコントロール、ふるまい検知。デバイス上で Web 脅威対策設定のローカル管理が許可されており（ポリシーが適用されていないか、ポリシーのプロパティで「ロック」に設定されていない）、対応ブラウザの 1 つがシステム上で検知された場合、Web 脅威対策コンポーネントが自動的に有効になることがあります。

コンポーネントを無効にすると、［**有効**］ボタンが使用可能になります。

アプリケーションコンポーネントを有効または無効にするには：

1. メインウィンドウを開きます。
2. メインウィンドウの下部で［**設定**］をクリックします。
   ［**設定**］ウィンドウが開きます。
3. コンポーネントの**有効化**または**無効化**をクリックします。

スキャンタスクの開始と停止

スキャンタスクを開始または停止するには：

1. メインウィンドウを開きます。
2. メインアプリケーションウィンドウで、［**スキャン**］をクリックします。
   ［**スキャン**］ウィンドウが表示されます。
3. 次のいずれかの操作を実行します：
   - スキャンタスクを開始するには、開始するスキャンタスクの下にある［**開始**］をクリックします。
     実行中のスキャンタスクの進捗が表示されます。
   - スキャンタスクを停止するには、停止するタスクの下にある［**停止**］をクリックします。
     スキャンタスクが停止し、スキャンしたオブジェクトおよび検知された脅威に関する情報が表示されます。
4. スキャンタスクのレポートを表示するには、［**レポートの表示**］をクリックします。

スキャンタスクの完了時に感染したオブジェクトが検知されると、タスクバーの右側にある本製品のアイコン近くの通知領域に、ポップアップウィンドウが表示されます。

スキャンウィンドウには、一時的なブートセクタスキャンタスク（*Scan_Boot_Sectors_{ID}*）と一時的なファイルのオブジェクトスキャンタスク（*Scan_File_{ID}*）の進行状況と結果も表示されます。［閉じる］（×）をクリックするか、［**スキャン**］ウィンドウを閉じる（メインウィンドウへの切り替え時や、本製品の終了時）と、既に完了した一時タスクに関する情報を非表示にできます。

アップデートタスクの開始と停止

アップデートタスクを開始または停止するには：

1. メインウィンドウを開きます。
2. メインアプリケーションウィンドウで、［**アップデート**］をクリックします。
   ［**アップデート**］ウィンドウが表示されます。
3. 次のいずれかの操作を実行します：
   - タスクを開始するには、開始するタスクの下にある［**開始**］をクリックします。
     実行中のアップデートタスクの進捗が表示されます。
     アップデートタスクが正常に完了したら、［**アップデートのロールバック**］が使用可能になり、最後に成功した定義データベースのアップデートをロールバックできます。
   - タスクを停止するには、停止するタスクの下にある［**停止**］をクリックします。
     アップデートタスクが停止します。
4. タスクのレポートを表示するには、［**レポートの表示**］をクリックします。

ロールバックタスクを開始するには：

1. メインウィンドウを開きます。
2. メインウィンドウで、［**アップデート**］セクションを選択します。

［**アップデート**］ウィンドウが表示されます。

3. ［**アップデートのロールバック**］をクリックして、ロールバックタスクを実行します。

Kaspersky Security Network の設定

グラフィカルユーザーインターフェイスを使用して、Kaspersky Security Network の使用を有効または無効にできます。

Kaspersky Security Network の使用を有効にするには：

1. メインウィンドウを開きます。
2. メインウィンドウの下部で［**設定**］をクリックします。
   ［**設定**］ウィンドウが開きます。
3. ［**設定**］ウィンドウで、次のいずれかのオプションを選択します：
   - ［**拡張 KSN モード**］：Kaspersky Security Network を使用する場合、ナレッジベースから情報を取得し、脅威の種別や発生源に関する統計や情報を匿名で送信します。
   - ［**基本 KSN モード**］：Kaspersky Security Network を使用する場合、ナレッジベースから情報を取得しますが、脅威の種別や発生源に関する統計や情報を匿名で送信することはできません。
4. ［**有効**］をクリックします。
   ［**Kaspersky Security Network の使用**］ウィンドウが開きます。
5. ［**Kaspersky Security Network の使用**］ウィンドウで、Kaspersky Security Network に関する声明をよく読み、［**私は、Kaspersky Security Network に関する声明の利用規約のすべてを確認し、理解した上で同意します**］を選択します。
6. ［**OK**］をクリックします。
   ［**Kaspersky Security Network の使用**］ウィンドウでオプションを選択していないと、［**OK**］は使用できません。

Kaspersky Security Network の使用を無効にするには：

1. メインウィンドウを開きます。
2. メインウィンドウの下部で［**設定**］をクリックします。
   ［**設定**］ウィンドウが開きます。
3. ［**有効**］をクリックします。
4. 開いたウィンドウで、［**はい**］をクリックして、Kaspersky Security Network の使用を拒否します。

レポートの表示

グラフィカルユーザーインターフェイスを使用して、アプリケーションレポートを表示できます。レポートには、アプリケーションコンポーネントとタスクの操作に関する情報が含まれます。

レポートデータは、イベントの一覧が含まれた表形式で示されます。表の各行に異なるイベントに関する情報が含まれます。イベントの属性は表の各列に表示されます。さまざまなコンポーネントやタスクの実行中にログに記録されるイベントには、さまざまな属性セットがあります。

レポートでは、次のイベント重要度が使用されます：

- *緊急* – デバイスの保護において、製品の動作や脆弱性の問題を示しているために注意が必要な、緊急の重要度のイベント。
- *高*
- *中*
- *低*
- *情報*
- *エラー*

レポートは、アプリケーションのメインウィンドウの下部にある**レポート**をクリックすると開くウィンドウに表示されます。

本製品では次のレポートを利用できます：

- **統計情報**：このレポートには、ファイル脅威対策とスキャンタスクの統計が含まれます。［**再読み込み**］をクリックすると、表示されているレポートを更新できます。
- **システム監査**：このレポートには、本製品の動作中やユーザーと製品との対話で発生するイベントに関する情報が含まれます。
- **脅威対策**：このレポートには、次の製品コンポーネントの実行中に記録されたイベントに関する情報が含まれています：
  - ファイル脅威対策
  - リムーバブルドライブのスキャン
  - アンチクリプター
  - ウェブ脅威対策
  - ネットワーク脅威対策
  - ファイアウォール管理
  - アプリケーションコントロール
  - デバイスコントロール
  - ふるまい検知
  - システム変更監視
- **オンデマンドタスク**：このレポートには、スキャンタスク、アップデートタスク、およびシステム整合性チェックによって記録されたイベントに関する情報が含まれています。

レポートを表示します：

1. メインウィンドウを開きます。
2. メインウィンドウの下部にある［**レポート**］をクリックします。
   ［**レポート**］ウィンドウが表示されます。
3. ［**レポート**］ウィンドウの左側で、必要なレポートの種別を選択します。
   ウィンドウの右側に、イベントのリストを含むレポートが表示されます。
   既定ではイベントは［**日付**］列の値で昇順にソートされています。
4. イベントに関する詳細情報を表示するには、レポートでイベントを選択します。
   このイベントの属性を含むセクションが、ウィンドウの下部に表示されます。

レポートを効果的に処理するため、画面上のデータ表示を次のように変更できます：

- イベントのリストを発生時間でフィルタリングする。
- 特定のイベントを見つけるため検索機能を使用する。
- 選択したイベントを別のセクションで表示する。

Backup オブジェクトの表示

グラフィカルユーザーインターフェースを使用して、Backup オブジェクトに対して次の操作を行うことができます：

- デバイス上の Backup に配置されたオブジェクトの情報を表示します。
- Backup からオブジェクトを元のディレクトリに復元します。
- Backup からオブジェクトを削除します。削除されたオブジェクトをその後で復元することはできません。

オブジェクトの復元と削除に関する情報は、イベントログに保存されます。

Backup にあるオブジェクトを表示するには：

1. メインウィンドウを開きます。
2. メインウィンドウの下部にある［**バックアップ**］をクリックします。
   これにより、［**バックアップ**］ウィンドウが開きます。

このウィンドウには、Backup 保管領域内のオブジェクトに関する次の情報が表示されます：

- オブジェクト名。
- オブジェクトの絶対パス。
- オブジェクトが Backup に追加された日付。
- オブジェクトが Backup から削除された日付（このフィールドは、Backup の保持期間が設定されている場合に表示されます）。

- オブジェクトのサイズ。

ライセンスの管理

グラフィカルユーザー インターフェイスを使用すると、アプリケーションライセンスを追加および削除し、アプリケーションが使用されているライセンスや関連付けられているライセンス関する情報を表示できます。

現在のライセンスを追加することで、アプリケーションを有効化できます。

*アクティベーション*とは、ライセンスの有効期限が切れるまで、すべての機能を使用できる製品版のライセンスを有効化するプロセスです。

Kaspersky Endpoint Detection and Response Optimum 機能が含まれていないライセンスで本製品を使用している場合、この機能を有効にするには、追加の Kaspersky Endpoint Detection and Response Optimum アドオンライセンス（「EDR Optimum ライセンス」）を追加する必要があります。

本製品に予備のライセンスを追加することもできます。現在のライセンスが期限切れになるか削除されると、予備のライセンスがアクティブになります。予備のライセンスを追加しておくことで、ライセンスの有効期限が切れた時に本製品の機能が制限されるのを防ぐことができます。

予備のライセンスは、現在のライセンスを追加した後にのみ追加できます。

ライセンスの追加

アプリケーションに有効なライセンスを追加します：

1. メインウィンドウを開きます。
2. 次のいずれかの操作を実行します：
   - メインウィンドウの下部にある、ライセンスに関する情報が表示されている領域をクリックします。
   - メインウィンドウの下部にある［**サポート**］をクリックして表示される［**サポート**］ウィンドウで、［**ライセンス**］フィールドのリンクをクリックして［**ライセンス**］ウィンドウを開きます。

   ［**ライセンス**］ウィンドウが表示されます。このウィンドウの［**ライセンスを購入**］ボタンをクリックすると、カスペルスキーオンラインストアが開き、ライセンスを購入できます。
3. 本製品は、製品版ライセンスまたは試用版ライセンスで有効化化できます。

   製品版ライセンスでアプリケーションを有効化します：

   a. ［**製品版ライセンス**］セクションの［**追加**］ボタンをクリックし、ライセンスの追加方法に応じて次の処理を実行します：
      - アクティベーションコードを使用してライセンスを追加する場合は、アクティベーションコードを入力して［**次へ**］ボタンをクリックします。

- ライセンス情報ファイルを使用してライセンスを追加する場合は、［**ライセンスの追加**］ボタンをクリックし、開いたウィンドウで .key 拡張子のファイルを選択します。

ウィンドウには、ライセンスとそれに関連付けられたライセンスに関する情報が表示されます。

b. ［**有効化**］ボタンをクリックします。

試用版ライセンスで本製品を有効化するには、［**試用版ライセンス**］セクションの［**有効化化**］ボタンをクリックします。ウィンドウには、試用版ライセンスと関連付けられたライセンスに関する情報が表示されます。

トライアルライセンスでアプリケーションを使用できるのは、1回のトライアル期間のみです。

現在のアプリケーションライセンスを追加した後、予備のライセンスを追加し、必要に応じて EDR Optimum アドオンライセンスを追加できます。予備のライセンスまたはアドオンライセンスの追加を開始するには、［**ライセンス**］ウィンドウの上部にある［**追加**］ボタンを使用します。

ライセンスの削除

本製品に追加されたライセンスを削除します：

1. メインウィンドウを開きます。
2. 次のいずれかの操作を実行します：
   - メインウィンドウの下部にある、ライセンスに関する情報が表示されている領域をクリックします。
   - メインウィンドウの下部にある［**サポート**］をクリックして表示される［**サポート**］ウィンドウで、［**ライセンス**］フィールドのリンクをクリックして［**ライセンス**］ウィンドウを開きます。

   ［**ライセンス**］ウィンドウが表示されます。
3. 削除するライセンスに関する情報の右にある［**削除**］ボタンをクリックします。
4. 開いたウィンドウで削除を確認します。

ライセンスの情報の表示

ライセンスの情報を表示するには：

1. メインウィンドウを開きます。
2. 次のいずれかの操作を実行します：
   - メインウィンドウの下部にある、ライセンスに関する情報が表示されている領域をクリックします。
   - メインウィンドウの下部にある［**サポート**］をクリックして表示される［**サポート**］ウィンドウで、［**ライセンス**］フィールドのリンクをクリックして［**ライセンス**］ウィンドウを開きます。

   ［**ライセンス**］ウィンドウが表示されます。

ウィンドウには、アプリケーションが使用されているライセンスに関する情報と、予備のライセンスがアプリケーションに追加されている場合は予備のライセンスに関連付けられているライセンスに関する情報が表示されます。ライセンスに関する完全な情報を表示するには、［**詳細情報**］リンクをクリックします。

［**現在のライセンス**］セクションには、現在のライセンスと関連付けられているライセンスに関する情報が表示されます。

- 現在のアプリケーションライセンスの種別、ライセンス制限、およびライセンスの有効期間。
- **識別 ID**：一意の英数字文字列。
- **ライセンスのステータス** - ライセンスのステータスまたはライセンスに関連する問題についてのメッセージ（問題がある場合）。
- **有効期間の開始日** - このライセンスを追加して製品をアクティベートした日付。
- **有効期限日数** – ライセンスの有効期限が切れるまでの日数と終了日（UTC）。
- **アプリケーション名** – ライセンスが追加された製品の名前。
- **保護** – 保護機能の制限と定義データベースの更新機能に関する情報。

現在の EDR Optimum ライセンスをアプリケーションに追加した場合、このライセンスとそれに関連付けられているライセンスに関する情報も［**現在のライセンス**］セクションに表示されます。

［**予備のライセンス**］セクションには、予備のライセンスと関連するライセンスに関する情報が表示されます。

- ライセンスに関連付けられた予備のライセンスの種別、ライセンス制限、およびライセンスの有効期間。
- **識別 ID**：一意の英数字文字列。
- **ライセンスの種別** – 予備のライセンスに関連付けられたライセンスの種別。
- **アプリケーション名** – ライセンスが追加された製品の名前。
- **保護** – 保護機能の制限と定義データベースの更新機能に関する情報。

アプリケーションに予備の EDR Optimum ライセンスを追加した場合、このライセンスとそれに関連付けられているライセンスに関する情報も［**予備のライセンス**］セクションに表示されます。

トレースファイルの作成

グラフィカルユーザーインターフェースを使用して、アプリケーショントレースファイルを作成し、その詳細レベルを定義できます。

トレースファイルを作成するには：

1. メインウィンドウを開きます。
2. メインウィンドウの下部にある［**サポート**］をクリックします。
   ［**サポート**］ウィンドウが表示されます。
3. ［**トレース**］をクリックして、［**トレース**］ウィンドウを開きます。

4. ［**レベル**］ドロップダウンリストで、トレースファイルの詳細レベルを選択します。

   カスペルスキーのテクニカルサポートの担当者に指示された詳細レベルを指定することを推奨します。既定値は **診断（300）** です。

5. ［**有効**］をクリックし、トレースを開始します。

6. 問題の原因となった状況を再現します。

7. ［**無効**］をクリックし、トレースを停止します。

作成されたトレースファイルは /var/log/kaspersky/kesl/ ディレクトリに保存されます。

Kaspersky Endpoint Security コンテナアプリケーション（KESL コンテナ）

Kaspersky Endpoint Security の配布キットには、イメージリポジトリからコンテナイメージをスキャンするために外部システムに埋め込むコンテナアプリケーション（「KESL コンテナ」）を作成するファイルが含まれています。

仮想環境の保護に Kaspersky Endpoint Security を Light Agent モードで使用している場合、KESL コンテナ機能には対応していません。

KESL コンテナでは、次の操作が可能です：

- リポジトリにあるコンテナイメージをスキャンします。
- 感染したオブジェクトが含まれていない、スキャンしたイメージを信頼するリポジトリに転送します。

展開、有効化、設定された KESL コンテナは、次の Kaspersky Endpoint Security の機能コンポーネントとタスクを提供します。

- ファイル脅威対策
- スキャンタスク：
  - マルウェアのスキャン
  - 簡易スキャン
  - コンテナースキャン
- コンテナの監視

KESL コンテナでは、次の Kaspersky Endpoint Security 追加機能を使用できます。

- 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を使用して、本製品をアクティベートします。
- アプリケーションデータベースのアップデートとロールバック。
- ファイルのコピーをデバイスのバックアップに保存します。

REST API を介して KESL コンテナと通信できます。Kaspersky Security Center のポリシーを使用して KESL コンテナを設定することもできます。

Kaspersky Security Center で KESL コンテナが正常に動作するには、KESL コンテナに対応するデバイスを固有のポリシーを持つ別の管理グループに移動してください。ポリシーのプロパティでは、Kaspersky Endpoint Security のすべての機能と設定を編集できますが、KESL コンテナに対応していない設定を構成しても、KESL コンテナの動作には影響しません。

KESL コンテナは、コマンドラインを使用して管理することはできません。

KESL コンテナが展開中に有効化され、管理対象デバイスへの自動ライセンス配布が設定された状態で Kaspersky Security Center に接続されている場合、ライセンスは KESL コンテナに対応するデバイスに適用されません。

KESL コンテナの導入とアクティベーション

配布パッケージの説明

配布パッケージには、次のファイルが含まれています：

- docker-service-<バージョン>.tgz - イメージの作成に必要なファイルのアーカイブ。
- kesl-<version>.rpm - Kaspersky Endpoint Security のインストールパッケージ。
- klnagent.rpm - Kaspersky Security Center ネットワークエージェントのインストールパッケージ。

docker-service-<バージョン>.tgz アーカイブには、次のファイルが含まれています：

- kesl-service - コンテナアプリケーションファイルのディレクトリ。
- Dockerfile - 18.06 より前のバージョンの Docker イメージをビルドするためのファイル。
- Dockerfile.1809 - 18.05 以降のバージョンの Docker イメージをビルドするためのファイル。
- build.sh.example - イメージをビルドするためのスクリプトの例。
- run.sh.example - KESL コンテナを起動するためのスクリプトの例。
- kesl-service.config.example - コンテナアプリケーションの設定情報ファイルの例。
- klnagent.conf.example - Kaspersky Security Center に接続するための設定情報ファイルの例。
- readme.md - クイックリファレンス。

KESL コンテナの導入とアクティベーション

KESL コンテナを使用するための準備をするには：

1. tar -xvf docker-service-<version>.tgz アーカイブファイルを展開します。
2. Kaspersky Security Center を使用して KESL コンテナを設定する場合は、次の操作を行います：
    a. klnagent.conf.example ファイルで、ネットワークエージェントの変数の値を指定します。詳細については、Kaspersky Security Center のヘルプ（*「Network Agent for Linux のサイレントモードでのインストール（応答ファイルを使用）」* セクション）を参照してください。
    b. klnagent.conf.example を kesl-service/klnagent.conf にコピーします。
3. build.sh.example インストールスクリプトを使用して、KESL コンテナの Docker イメージをビルドします：

a. プロキシサーバーを使用する場合は、COMMON_AGRS 変数に必要な値を指定します。

b. 必要に応じて、対象の kesl-service イメージの名前を変更します。

c. build.sh.example を build.sh にコピーし、実行ファイルの属性を割り当てます。

d. build.sh を実行します。

4. `docker images -a` コマンドを実行して、ビルドが正常に完了したことを確認します。
   コマンドの実行結果が次のように表示されます：
   `REPOSITORY TAG IMAGE ID CREATED SIZE`
   `kesl-service latest <hex> <作成時間> <サイズ>`

5. 次のいずれかの方法で KESL コンテナをアクティベートします：

   - Kaspersky Security Center を使用する。KESL コンテナを有効にするには、Web コンソールまたは管理コンソールで KESL コンテナに対応するデバイスにライセンスを追加する必要があります。

     > Kaspersky Security Center で KESL コンテナが正常に動作するには、KESL コンテナに対応するデバイスを固有のポリシーを持つ別の管理グループに移動してください。KESL コンテナが停止すると、これらのデバイスは管理グループから自動的に削除され、これらのデバイスに使用されていたライセンスが解放されます。

   - 設定情報ファイルを使用する。
   - 環境変数を使用する（手順 7 を参照）。

6. KESL コンテナを設定します（KESL コンテナの設定、KESL コンテナの設定）。

7. 次のコマンドを使用して、KESL コンテナを開始します：`docker run --privileged --init -p <<KESL container_port>:<device_port> \`
   `-e <変数_1> -e <変数_2> ... -e <変数_n> \`
   `-v <マウント ポイント_1> -v <マウント ポイント_2> ... -v <マウント ポイント_n> \`
   `<イメージ名>`
   説明：

   - `<KESL コンテナのポート>` は KESL コンテナのポートであり、KESL コンテナの外部からネットワーク経由でアクセスできる必要があります。
   - `<device_port>`は、KESL コンテナがインストールされているデバイスのポートです。

   KESL コンテナを起動するときに、環境変数を使用して有効化できます。

   - アクティベーションコードを使用している場合は、`KRAS4D_ACTIVATION='<アクティベーションコード>'` オプションを追加します：
     `docker run ... -e KRAS4D_ACTIVATION='<アクティベーションコード>'`
   - ライセンス情報ファイルを使用している場合は、`KRAS4D_ACTIVATION='<ライセンス情報ファイル>'` および `KRAS4D_KEYPATH=/root/kesl-service/keys` オプションを追加します：
     `docker run... -e KRAS4D_ACTIVATION='<ライセンス情報ファイル>' -e KRAS4D_KEYPATH=/root/kesl-service/keys -v <ライセンスがあるディレクトリのパス>:/root/kesl-service/keys`

ファイル run.sh.example に実行コマンドの例を表示できます。

KESL コンテナの設定

KESL コンテナの設定を初期化するにはいくつかの方法があります：

- 既定（指定がない場合）。
- 設定情報ファイル：この場合、設定情報ファイルの値は既定値よりも優先されます。
- 値は、起動時に環境変数として KESL コンテナに渡すことができます。環境変数は、設定情報ファイルでの指定よりも優先されます。
- スキャンリクエストボディ：リクエストボディの設定は最も高い優先度ですが、それらは1つのリクエスト内でのみ有効です。

KESL コンテナの設定

KESL コンテナの設定とその既定値を、次の表で説明します。

KESL コンテナの設定

設定の説明	取りうる値	既定値
REST API のリスニングポート		8085

イベントの緊急度	`debug`
	`info`
	`warning`
	`error`
	`critical`
	`noset`
		noset

認証鍵	`KRAS4D_XAPIKEY` が設定されている場合、各リクエストの検証は x-api-key ヘッダーの存在について、およびその内容が `KRAS4D_XAPIKEY` 設定の値と一致するかどうかについて行われます。これらの条件が満たされない場合、リクエストは拒否されます。この設定がない場合、検証は実行されません。	
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	アクティベーションコードを使用して KESL コンテナをアクティベートするには、KESL コンテナの実行時に、設定情報ファイルでアクティベーションコードを指定するか、環境変数でアクティベーションコードを指定します： `docker run ... -e KRAS4D_ACTIVATION='<アクティベーションコード>'` ライセンス情報ファイルを使用して KESL コンテナをアクティベートするには、KESL コンテナの実行時に、設定情報ファイルでライセンス情報ファイルを指定するか、環境変数でライセンス情報ファイルを指定します：	

	`docker run... -e KRAS4D_ACTIVATION='<` ライセンス情報ファイル `>' -e KRAS4D_KEYPATH=/root/kesl-service/keys -v <` ライセンスがあるディレクトリのパス `>:/root/kesl-service/keys` ライセンス情報ファイルを使用して KESL コンテナをアクティベートするには、マウントポイント「/root/kesl-service/keys」が必要です。	
スキャンの詳細設定	オプションの `KRAS4D_SCANOPTIONS` 設定を使用すると、コンテナースキャンタスクを設定できます： `docker run ... -e KRAS4D_SCANOPTIONS='<` 設定 `>'` `<` 設定 `>` は、コンテナースキャンタスクの設定です。	
アップデートの詳細設定	オプションの `KRAS4D_UPDATEOPTIONS` 設定を使用すると、アップデートタスクを設定 できます。 `docker run ... -e KRAS4D_UPDATEOPTIONS='<` 設定 `>'` `<` 設定 `>` は、アップデートタスクの設定（`SourceType` 設定、`ApplicationUpdateMode` 設定、および `CustomSources.item_#` セクションの設定）です。	
KESL コンテナの開始時に定義データベースをアップデートする	既定では、定義データベースは KESL コンテナの開始時にディレクトリ /vvar/opt/kaspersky/kesl/private/updates にダウンロードされます。 定義データベースの 1 つのインスタンスを使用して複数の KESL コンテナの連動操作を導入し、KESL コンテナの起動を高速化するには、KESL コンテナがインストールされているデバイスにマウントしてこのディレクトリを移動してください： `docker run ... -v <` 定義データベースのディレクトリへのパス `>:/var/opt/kaspersky/kesl/private/updates`	True
対象のリポジトリに既に存在する場合は、イメージを処理しないでください。		False
アプリケーションのコマンドの実行を待機する最長時間（秒単位）		600
定義データベースのアップデートを待機する最長時間（秒単位）		600
KESL コンテナ設定情報ファイルの名前		kesl-service.config

環境変数

KESL コンテナの設定で、以下の環境変数が使用できます：

- KRAS4D_PORT – REST API のリスニングポート。

- KRAS4D_LOGLEVEL – イベントの緊急度。
- KRAS4D_XAPIKEY – 認証鍵のリクエスト。
- KRAS4D_ACTIVATION – 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名。
- KRAS4D_SCANOPTIONS – スキャンの詳細設定。
- KRAS4D_UPDATEOPTIONS – アップデートの詳細設定。
- KRAS4D_FORCEUPDATE – KESL コンテナの開始時に定義データベースをアップデートする。
- KRAS4D_SKIPIMAGEIFEXISTS – 対象のリポジトリに既に存在する場合は、イメージを処理しない。
- KRAS4D_GENERALTIMEOUT – アプリケーションのコマンドの実行を待機する最長時間。
- KRAS4D_UPDTASKTIMEOUT – 定義データベースのアップデートを待機する最長時間。
- KRAS4D_CFGNAME：KESL コンテナ設定情報ファイルの名前。

設定情報ファイル

KESL コンテナ設定情報ファイルの形式は yaml です。ファイルから設定を読み取るには、KESL コンテナがインストールされているデバイスで「/root/kesl-service/config/」パスをマウントし、さらに設定情報ファイルの名前が既定と異なる場合はファイル名を指定します。このように、KESL コンテナのセットごとに個別の設定情報ファイルを指定できます。

```
例：KESL コンテナの開始
docker run ... \
-e KRAS4D_CFGNAME='unique_file_name' \
-v <HOST_PATH>:/root/kesl-service/config \
kesl-service
```

設定情報ファイルの設定項目に対応する環境変数を、次の表に記します。

設定項目と環境変数の対応

設定情報ファイルの設定項目	環境変数
共通セクション	
port: <リスニングポート>	# KRAS4D_PORT=8085
sqlpath: <スキャン結果を含むデータベースファイルへの完全パス>	# KRAS4D_SQLPATH
certdir: <レジストリ証明書のあるディレクトリのパス>	# KRAS4D_CERTDIR
keypath: <ライセンス情報ファイルのあるディレクトリのパス>	# KRAS4D_KEYPATH
tmppath: <一時ディレクトリへの完全パス>	# KRAS4D_TMPPATH
logpath: <イベントログへの完全パス>	# KRAS4D_LOGPATH
loglevel: [noset|debug|info|warning|error|critical]	# KRAS4D_LOGLEVEL
管理セクション	
xapikey: <認証鍵のリクエスト>	# KRAS4D_XAPIKEY=None

forceupdate: <コンテナの開始時に定義データベースを強制的にアップデート [True|False]>	# KRAS4D_FORCEUPDATE
activation: <アクティベーションコードまたは /root/kesl-service/config/ にあるライセンス情報ファイル名>	# KRAS4D_ACTIVATION
detectaction: [delete|skip]	# KRAS4D_DETECTACTION
scanoptions: <スキャン設定 [ScanArchived=yes ScanSfxArchived=yes ...]>	# KRAS4D_SCANOPTIONS
skipimageifexist: <スキャンしたイメージのコピー先のサーバーに既にイメージが存在する場合は、イメージをスキャンしない>	# KRAS4D_SKIPIMAGEIFEXIST
generaltimeout: <アプリケーションのコマンドの実行を待機する最長時間>	# KRAS4D_GENERALTIMEOUT
updtasktimeout: <定義データベースのアップデートを待機する最長時間>	# KRAS4D_UPDTASKTIMEOUT
リポジトリセクション	
<サーバー>:<ポート>: 検証のリクエスト時に認証を必要とするイメージレジストリのアドレスとポート。	
認証情報サブセクション	
user: イメージレジストリでの認証用のユーザー名	
pass: イメージレジストリでの認証用のパスワード	

設定情報ファイルの例

```
common:
    port: 8085
    sqlpath: './data/scans.sqlite'
    tmppath: './tmp/'
    keypath: './keys/'
    certdir: './certificates/'
    logpath: '/var/log/kaspersky/kesl-service/'
    loglevel: 'debug'
control:
    xapikey: 0000
    activation: XXXX-XXXX-XXXX-XXXX or XXXX.key
    scanoptions: 'ScanArchives=yes'
    updateoptions: ''
    forceupdate: True
    skipimageifexists: False
    generaltimeout: 600
    updtasktimeout: 1000
repositories:
    repository.any.com:
        certificate: repository_any_comcert.pem
        credentials:
            user: user
            pass: password
```

使用可能なマウントポイント

KESL コンテナの操作で、次のマウントポイントを使用できます：

- /root/kesl-service/data/scans.sqlite – スキャン結果を含むデータベースファイルへのパス。
- /var/opt/kaspersky/kesl/private/updates – 定義データベースへのパス。
- /root/kesl-service/certificates – リポジトリ証明書があるディレクトリのパス。
- /root/kesl-service/keys – ライセンス情報ファイルがあるディレクトリのパス。
- /var/log/kaspersky/ – イベントログがあるディレクトリのパス。

- /root/kesl-service/config/ – 設定情報ファイルへのパス。
- /var/lib/containers/vfs-storage – Podman ユーティリティが正しく機能するために必要なマウントポイント。

REST API を使用した KESL コンテナの管理

KESL コンテナとの対話は REST API を使用して実装されます。REST API を使用して次の操作を行うことができます：

- 1つのファイルまたは複数のファイルをスキャンします。これを行うには、スキャンリクエスト（POST）を送信します。

  例：
  POST http://<サーバー>:<ポート>/scans

  1つまたは複数のファイル。

- 1つの Docker イメージ または複数の Docker イメージをスキャンします。これを行うには、スキャンリクエスト（POST）を送信します。

  例：
  POST http://<サーバー>:<ポート>/scans

  スキャンする Docker イメージへのリンク。

- 詳細設定で、1つの Docker イメージ または複数の Docker イメージをスキャンします。これを行うには、スキャンリクエスト（POST）を送信します。

  例：
  POST http://<サーバー>:<ポート>/scans

  特定の種別の JSON。

- スキャンセッションのリストを取得します。これを行うには、スキャンセッション（GET）に関する情報のリクエストを送信します。

  例：
  GET http://<サーバー>:<ポート>/scans

- スキャンセッションに関する情報を取得します。これを行うには、スキャンセッション（GET）に関する情報のリクエストを送信します。

  例：
  GET http://<サーバー>:<ポート>/scans/<スキャンセッションの一意の識別子>

- KESL コンテナを再読み込みせずにレジストリ証明書を追加します。これを行うには、レジストリ証明書（POST）を追加するためのリクエストを送信します。

  例：
  POST http://<サーバー>:<ポート>/addcert

- KESL コンテナの状態に関する情報を取得します。そのためには、KESL コンテナの状態に関する情報を受け取るリクエストを送信します（GET）。

  例：
  GET http://<サーバー>:<ポート>/status

スキャンリクエスト

目的

リクエストボディで指定されたオブジェクトのスキャン。

次のオブジェクトをスキャンできます：

- 1つのファイル
- 複数のファイル
- 特定のリポジトリにある1つまたは複数のDockerイメージ
- 詳細設定の特定のリポジトリにある1つまたは複数のDockerイメージ

パス

http://<サーバー>:<ポート>/scans[?wait=1]

設定

オプションの `wait` 設定では、スキャンセッションの種別を指定します。

設定値が `1` の場合、同期スキャンが実行され、スキャンが終了するとレポートが送信されます。

設定値が `0` の場合、非同期スキャンが実行され、次のような応答が返されます：

```
{
  "id"="7d27e9b4-a4d7-469b-bdcf-ebfe953498e4",
  "location"="/scans/7d27e9b4-a4d7-469b-bdcf-ebfe953498e4"
}
```

説明：

- id – スキャンセッションの一意の識別子。
- location – このセクションに関する情報をリクエストするパス：http://<サーバー>:<ポート>/scans/<場所>。

リクエストヘッダー

リクエストには、次のヘッダーを含めることができます：

- Content-Type

スキャンに対して送信されるオブジェクトの種別を定義します。
サポートされる値：

- application/octet-stream – 1つのファイル
- multipart/form-data – 複数のファイル
- text/plain – 特定のリポジトリにある1つまたは複数の Docker イメージ
- application/json – 詳細設定の特定のリポジトリにある1つまたは複数の Docker イメージ

- x-api-key（オプション）
  KRAS4D_XAPIKEY 環境変数または設定情報ファイルの xapikey 変数で指定された API キー。

考えられるエラー

サポートされていない値が Content-Type ヘッダーに指定されている場合、次のエラーが返されます：

```
{
  "error"={

"code"="NOT_SUPPORTED_CONTENT_TYPE",
"details"="<content type>",
"message"="Not supported Content-Type"
  },

  "status"="error"

}
```

ファイルのスキャンリクエスト

Content-Type

application/octet-stream

リクエストボディ

1つのファイル。

応答例：

```
{

  "completed": "Mon, 01 Mar 2021 06:54:39 GMT",
```

```
  "created": "Mon, 01 Mar 2021 06:54:38 GMT",

  "progress": 100,

  "scan_result": {

"noname": {
"started": "2021-03-01 06:54:39",
"stopped": "2021-03-01 06:54:39",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/b8eb4128-8cb4-4964-87cf-b9853e6544ec"
}
],
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"infected"
  ]

}
```


複数ファイルのスキャンリクエスト

Content-Type

multipart/form-data

リクエストボディ

複数ファイル。

応答例：


```
{

  "completed": "Mon, 01 Mar 2021 06:55:44 GMT",
```

```
  "created": "Mon, 01 Mar 2021 06:55:43 GMT",

  "progress": 100,

  "scan_result": {

"clean": {
"started": "2021-03-01 06:55:43",
"stopped": "2021-03-01 06:55:43",
"verdict": "clean"
},
"corrupted.com": {
"errors": [
{
"error": "Corrupted object",
"object": "/root/kesl-service/tmp/75d28fe6-8154-4361-9382-90a76861518a"
}
],
"started": "2021-03-01 06:55:43",
"stopped": "2021-03-01 06:55:43",
"verdict": "non scanned"
},
"error.com": {
"errors": [
{
"error": "read error",
"object": "/root/kesl-service/tmp/37f6e0dd-13f9-4d11-899c-5fe0f23e407d"
}
],
"started": "2021-03-01 06:55:44",
"stopped": "2021-03-01 06:55:44",
"verdict": "non scanned"
},
"infected.com": {
"started": "2021-03-01 06:55:44",
"stopped": "2021-03-01 06:55:44",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/7d664646-bf56-4060-b958-5ce9e746c929"
}
],
```

```
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"clean",
"non scanned",
"infected"
  ]

}
```

Docker イメージのスキャンリクエスト

Content-Type

text/plain

リクエストボディ

スキャンする Docker イメージへのリンク。

次の値を使用できます：

- リポジトリ内のイメージのパス（例：https://index.docker.io/jerbi/eicar:latest）。
- 複数のイメージへのパスマスク（例：https://index.docker.io/<名前マスク>:<タグマスク>）。? や * の記号でマスクを指定できます。

応答例：

```
{

  "completed": "Sun, 31 Jan 2021 10:29:26 GMT",

  "created": "Sun, 31 Jan 2021 10:29:20 GMT",

  "progress": 100,

  "scan_result": {

"jerbi/eicar:latest": {
```

```
"started": "2021-01-31 10:29:25",
"stopped": "2021-01-31 10:29:26",
"threats": [
{
"name": "EICAR-Test-File",
"object": "[image:docker.io/jerbi/eicar:latest] /eicar.com.txt"
}
],
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"infected"

  ]

}
```


考えられるエラー

Docker REST API を使用するリクエストは、マスクによるイメージのリストの取得に使用されます。

ただし、多くの公開サーバーでは、セキュリティ上の理由から無効になっています。このようなサーバーでマスクを使用してイメージをスキャンしようとすると、エラーが発生します。

エラーの例：


```
{

  "completed": "Mon, 01 Mar 2021 07:02:24 GMT",

  "created": "Mon, 01 Mar 2021 07:02:22 GMT",

  "scan_errors": [

{
"code": 401,
"details": {
"context": {
"image_mask": "/jerbi/eic*:latest",
"repository": "index.docker.io",
"repository_base": "index.docker.io"
```

```
},
"errors": [
"Unauthorized"
]
},
"message": "Invalid source"
},
[
"Unauthorized"
]
  ],

  "status": "completed"

}
```

詳細設定での Docker イメージのスキャンリクエスト

Content-Type

application/json

リクエストボディ

次の種別の JSON：

```
{

  "source": "https://index.docker.io/jerbi/eicar:latest",

  "params": {

"destination": "https://fake",
"skipimageifexists": true,
"custom_callbacks": {
"on_detect": {
"uri": "http://10.16.42.75:5050",
"content-type": "application/json",
"body": {
"session_id": "100",
"session_init": "20201105T072403+0300",
"infected_items": "$infected"
```

```
}
},
"on_complete": {
"body": {
"session_id": "100",
},
"uri": "http://10.16.42.75:5050/on_complete",
}
}
  }

}
```

リクエストの詳細設定

`params` セクションには、次の設定が含まれています：

- `destination`（オプション）- スキャンしたイメージのコピー先のサーバー。
- `skipimageifexists`（オプション） – コピー先のサーバーに名前と SHA256 ハッシュが同じイメージが既にある場合は、イメージをスキャンまたはコピーしません。この設定は、コピー先の設定が指定されている場合にのみ指定できます。
- `custom_callbacks`（オプション） – スキャンの終了時に送信する必要があるリクエストについて説明します：
  - on_detect – 脅威が検知された場合、リクエストが送信されます。
  - on_complete – スキャンが終了すると、リクエストは常に送信されます。

リクエストボディの説明では、`$infected` 置換変数を指定できます。この変数の代わりに、感染したオブジェクトのリストが置き換えられます。

応答例：

```
{
  "completed": "Mon, 01 Mar 2021 07:13:49 GMT",
  "created": "Mon, 01 Mar 2021 07:13:42 GMT",
  "progress": 100,
  "scan_errors": [
{
"code": 500,
"message": "Unable to get images hash from destination registry"
```

```
}
  ],

  "scan_params": {

"destination": "https://fake",
"skipimageifexists": true
  },

  "scan_result": {

"jerbi/eicar:latest": {
"started": "2021-03-01 07:13:48",
"stopped": "2021-03-01 07:13:49",
"threats": [
{
"name": "EICAR-Test-File",
"object": "[image:docker.io/jerbi/eicar:latest] /eicar.com.txt"
}
],
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"infected"
  ]

}
```


スキャンセッションに関する情報のリクエスト（GET）

目的

スキャンセッションに関する情報を取得します。

パス

http://<サーバー>:<ポート>/scans[?force] – セッションのリストのリクエスト。

http://<サーバー>:<ポート>/scans/<スキャンセッションの一意の識別子>[?force] – 特定のセッションに関する情報のリクエスト。

設定

KESL コンテナは、スキャンセッションに関するデータをメモリに保存し、スキャン結果データベースに書き込みます。

複数の KESL コンテナのインスタンスが同じデータベースで動作している場合、オプションの `?force` 設定はデータベースからの情報の読み取りを開始します。この設定がない場合、特定の KESL コンテナのインスタンスによって開始されたセッションに関する情報のみが表示されます。

スキャンセッションのリストのリクエスト

パス

http://<サーバー>:<ポート>/scans[?force]

応答例：

```
{
  "629ae0a9-28de-4e2f-b130-67e87ba4d61d": {
"progress": 100,
"status": "completed"
  },
  "655b96fc-34ca-4915-9c41-d52724a277de": {
"progress": 100,
"status": "completed"
  },
  "7d27e9b4-a4d7-469b-bdcf-ebfe953498e4": {
"progress": 100,
"status": "completed"
  },
  "c32ca88f-2d24-47ec-b040-0540366bea4b": {
"progress": 100,
```

```
"status": "completed"
  },
  "df11ad81-26aa-42f9-94bb-39dee4304807": {
"progress": 0,
"status": "completed"
  },
  "fa25340f-4898-497f-ab59-8df494f4ea47": {
"progress": 100,
"status": "completed"
  }
}
```

特定のセッションに関する情報のリクエスト

パス

http://<サーバー>:<ポート>/scans/<スキャンセッションの一意の識別子>[?force]

応答例：

```
{
  "completed": "Mon, 01 Mar 2021 06:45:19 GMT",
  "created": "Mon, 01 Mar 2021 06:45:19 GMT",
  "progress": 100,
  "scan_result": {
"noname": {
"started": "2021-03-01 06:45:19",
"stopped": "2021-03-01 06:45:19",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/65b55d89-b758-4609-a2f3-f63ef839815d"
}
```

```
],
"verdict": "infected"
}
  },
  "status": "completed",
  "verdicts": [
"infected"
  ]
}
```

レジストリ証明書の追加のリクエスト（POST）

目的

KESL コンテナを再読み込みせずにレジストリ証明書を追加します。

パス

http://<サーバー>:<ポート>/addcert

リクエストヘッダー

リクエストには Content-Type ヘッダーが含まれています。

サポートされる値：

- application/octet-stream – 1つの証明書ファイル
- multipart/form-data – 複数の証明書ファイル

KESL コンテナの状態に関する情報のリクエスト（GET）

目的

KESL コンテナの現在の状態と、KESL コンテナの状態を決定するアプリケーションステータスパラメータ（アプリケーション、ライセンス、およびデータベースのステータス）に関する情報を取得します。

Path

http://<サーバー>:<ポート>/status

応答例：

```
{'product info': {'databases_date': '<データベース公開日>', 'databases_loaded': True,
'license_expiration': '<ライセンス有効期限>', 'license_info': 'ライセンス有効',
'policy': '適用外', 'version': '<アプリケーションバージョン>'}, 'status': 'サービス使用可
能'}
```

考えられるエラー

エラーの例（アプリケーションが KESL コンテナ内で実行されていない）：

```
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'サービスは使用不可', 'status_reason': ['KESL は応答なし']}{'product
info': {'databases_date': 'N/A', 'databases_loaded': False, 'license_expiration':
'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version': 'N/A'}, 'status': 'サービス
は使用不可', 'status_reason': ['KESL は応答なし']}{'product info': {'databases_date':
'N/A', 'databases_loaded': False, 'license_expiration': 'N/A', 'license_info': 'N/A',
'policy': 'N/A', 'version': 'N/A'}, 'status': 'サービスは使用不可', 'status_reason':
['KESL は応答なし']}
```

エラーの例（定義データベースがダウンロードされていません）：

```
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': '<ライセンス有効期限>', 'license_info': '一貫性のないアップデート',
'policy': '適用外', 'version': '<アプリケーションバージョン>'}, 'status': 'サービスは使用
不可', 'status_reason': ['データベースが読み込まれない', 'ライセンスエラー: 一貫性のないア
ップデート']}
```

エラーの例（ライセンスの有効期限切れ）：

```
{'product info': {'databases_date': '<データベース公開日>', 'databases_loaded': True,
'license_expiration': '<ライセンス有効期限>', 'license_info': '期限切れ', 'policy': '適
用外', 'version': '<KESL バージョン>'}, 'status': 'サービスは使用不可', 'status_reason':
['ライセンスエラー： 期限切れ']}
```

テクニカルサポートへの問い合わせ

製品のヘルプや製品に関する情報源で問題の解決策が見つからなかった場合は、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。テクニカルサポートの担当者が、Kaspersky Endpoint Security のインストール方法または使用方法についての質問にお答えします。

カスペルスキーは、Kaspersky Endpoint Security のライフサイクル全体にわたってサポートを提供します（アプリケーションのライフサイクルを参照）。テクニカルサポートに問い合わせる前に、サポートのルールをお読みください。

テクニカルサポートに問い合わせるには、次のいずれかの方法があります：

- テクニカルサポートサイトを参照する。
- カスペルスキーカンパニーアカウントのポータルからカスペルスキーのテクニカルサポートにリクエストを送信する。

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企業のためのポータルです。カスペルスキーカンパニーアカウントのポータルは、オンラインリクエストを経由して容易にユーザーとカスペルスキーが対話できるよう設計されています。カスペルスキーカンパニーアカウントのポータルでは、カスペルスキーの担当者によるリクエスト処理の進捗を確認したり、リクエストの履歴を保存したりできます。

組織内のすべての従業員をカスペルスキーカンパニーアカウントの1つのアカウントに登録することができます。1つのカンパニーアカウントで、登録済みユーザーからカスペルスキーへのオンラインリクエストを一元的に管理することに加えて、カスペルスキーカンパニーアカウント経由でこのようなユーザー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、次の言語で使用できます：

- 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の詳細は、テクニカルサポートサイトを参照してください。

テクニカルサポートに関する情報の入手

カスペルスキーのテクニカルサポートの担当者に問題について通知すると、*トレースファイル*または*ダンプファイル*の送信を依頼されることがあります。

テクニカルサポートの担当者は、デバイスのオペレーティングシステムや実行中のプロセス、アプリケーションコンポーネントの操作に関する詳細レポートを必要とする場合もあります。

問題の診断中、テクニカルサポートの担当者は以下のアプリケーション設定の変更を依頼することがあります：

- 高度な診断情報を受信するための機能のアクティベート。
- 標準的なユーザーインターフェイスでは実行不可能な個々のアプリケーションコンポーネントの詳細設定の実行。
- 受信した診断情報の保存設定の変更。
- ファイル内のネットワークトラフィックのキャプチャおよび保管領域の設定。

テクニカルサポートの担当者は、これらの処理（ステップの順序、変更用の設定、設定情報ファイル、スクリプト、高度なコマンドライン機能、モジュールのデバッグ、特別ユーティリティなど）を実行するための情報に加え、診断目的で受信された情報の本文などを提供します。受信された詳細な診断情報はユーザーのデバイスに保管されます。この情報はカスペルスキーに自動送信されません。

上記のステップはテクニカルサポートの担当者の指導のもと、担当者が提供する指示に従って実行される必要があります。アプリケーションドキュメントに記載されていない、またはテクニカルサポートスペシャリストが推奨していない方法を使用してアプリケーションファイルを単独で変更すると、アプリケーションやオペレーティングシステムのパフォーマンスの低下や障害、保護の低下、データへのアクセス不能や破損につながる可能性があります。

アプリケーショントレースファイル

*トレースファイル*は、アプリケーションコマンドの実行をステップごとに追跡し、アプリケーション操作のどの段階でエラーが発生したかを検知することができます。

アプリケーショントレースファイルは既定では生成されません。アプリケーションの全般設定およびグラフィカルユーザーインターフェイスを介してコマンド ラインで、アプリケーショントレースファイルの生成を有効または無効にし、トレースファイルの詳細レベルを定義できます。

アプリケーショントレースファイルを有効にしている場合、ファイルは /var/log/kaspersky/kesl/ に保存されます。このディレクトリへのアクセスには root 権限が必要です。

トレースファイルは、製品が使用されている限りデバイスに保存されます。製品が削除されると完全に削除されます。トレース ファイルはカスペルスキーに自動的に送信されません。

トレース ファイルは、人間が判読できる形式で保存されます。カスペルスキーに送信する前に、不正アクセスから情報を保護するようにしてください。

アプリケーショントレースファイルのコンテンツ

トレースファイルには、次の一般的なデータが含まれています：

- イベントの時刻。
- 実行されているスレッドの数。
- イベントを発生させた製品コンポーネント。
- イベントの重要度（情報イベント、警告、緊急イベント、エラー）。
- 製品のコンポーネントによるコマンド実行に関係するイベントの説明と、このコマンドの実行結果。

トレースファイルには、一般的なデータに加えて以下の情報が保存される場合があります：

- 本製品のコンポーネントとその動作データのステータス。
- 製品におけるユーザーの操作に関するデータ。
- デバイスに装備されているハードウェアのデータ。
- ユーザーの操作に関する情報を含む、オペレーティングシステムのオブジェクトおよびイベントに関するすべてのデータ。
- オペレーティングシステムのオブジェクトに含まれるデータ（ユーザーの個人データを含むファイルの内容など）。
- ネットワークトラフィックデータ（たとえば、銀行カード情報やその他の機密データを含む可能性のあるWebサイトの入力フィールドの内容など）。
- カスペルスキーのサーバーから受信したデータ（定義データベースのバージョンなど）。
- KATAサーバーから受信したデータ。
- 消費されたCPUリソースに関するデータ。
- 消費されたRAMリソースに関するデータ。
- 本製品によるファイルの読み取りおよび書き込み操作に関するデータ。
- 本製品の動作に必要なキャッシュ情報の量に関するデータ。

アプリケーショントレースの設定

Kaspersky Security Centerを通じてKaspersky Endpoint Securityアプリケーションを管理している場合は、Webコンソールまたは管理コンソールを使用して、Kaspersky Endpoint Securityのポリシー設定でアプリケーションのトレース設定を構成できます。

コマンドラインでアプリケーションを管理している場合は、アプリケーションの全般設定でアプリケーションのトレース設定を構成できます。

Web コンソールでのトレース設定の編集

Web コンソールでは、ポリシーのプロパティ（［**製品設定**］→［**全般設定**］→［**製品設定**］の［**トレースとダンプの設定**］）で本製品のトレース設定を構成できます（次の表を参照）。

アプリケーショントレースの設定

設定	説明
トレースファイルのディレクトリへのパス	トレースファイルが保存されているディレクトリへのパスの入力フィールド。 既定値：/var/log/kaspersky/kesl 別のディレクトリを指定する場合は、Kaspersky Endpoint Security を実行しているアカウントが、このディレクトリに対して読み取り / 書き込み権限を持っていることを確認します。既定のトレースファイルのディレクトリにアクセスするには、root 権限が必要です。
トレースファイルの最大数	本製品のトレースファイルの最大数の入力フィールドです。 既定値：10
トレースファイルの最大サイズ（MB）	本製品のトレースの最大サイズ（メガバイト単位）の入力フィールドです。 既定値：500

トレース設定を適用するには、アプリケーションを再起動する必要があります。

管理コンソールでのトレース設定の編集

管理コンソールでは、ポリシーのプロパティ内で本製品のトレース設定を行うことができます（**全般設定 → 製品設定**）。

［**トレースとダンプの設定**］で、［**構成**］をクリックすると、トレース設定を編集できるウィンドウが開きます（次の表を参照）。

アプリケーショントレースの設定

設定	説明
トレースファイルのディレクトリへのパス	トレースファイルが保存されているディレクトリへのパスの入力フィールド。 既定値：/var/log/kaspersky/kesl 別のディレクトリを指定する場合は、Kaspersky Endpoint Security を実行しているアカウントが、このディレクトリに対して読み取り / 書き込み権限を持っていることを確認します。既定のトレースファイルのディレクトリにアクセスするには、root 権限が必要です。
トレースファイルの最大サイズ（MB）	本製品のトレースの最大サイズ（メガバイト単位）の入力フィールドです。 既定値：500
トレースファイルの最大数	本製品のトレースファイルの最大数の入力フィールドです。 既定値：10

トレース設定を適用するには、アプリケーションを再起動する必要があります。

コマンドラインでのトレース設定の編集

コマンドラインでは、製品の全般設定の `TraceLevel`、`TraceFolder`、`TraceMaxFileCount`、および TraceMaxFileSize 設定を使用して、本製品のトレース設定を構成できます。

`TraceLevel` 設定を使用すると、本製品のトレースを有効または無効にし、トレースファイルの詳細レベルを指定できます。この設定は次の値を使用できます：

- `Detailed` - 詳細なトレースファイルを生成します。
- `MediumDetailed` - 情報メッセージとエラーメッセージを含むトレースファイルを生成します。
- `NotDetailed` - エラーメッセージを含むトレースファイルを生成します。
- `None`（既定値） - トレースファイルを生成しません。

`TraceFolder` 設定では、本製品のトレースファイルが保存されるディレクトリを指定できます。既定値：/var/log/kaspersky/kesl別のディレクトリを指定する場合は、Kaspersky Endpoint Security を実行しているアカウントが、このディレクトリに対して読み取り / 書き込み権限を持っていることを確認します。既定のトレースファイルのディレクトリにアクセスするには、root 権限が必要です。

`TraceMaxFileCount` では、本製品のトレースファイルの最大数を指定できます。設定できる値は 1 ～ 10000 です。既定値：10

`TraceMaxFileSize` では、レースファイルの最大サイズ（メガバイト単位）を指定できます。設定できる値は 1 ～ 1000 です。既定値：500

コマンドラインオプションまたは本製品の全般設定のすべてを含む設定情報ファイルを使用して設定を編集できます。

> `TraceFolder`、`TraceMaxFileCount`、または `TraceMaxFileSize` 設定の値を変更した後は、本製品を再起動する必要があります。

アプリケーション管理プラグインのトレースファイル

管理プラグイントレースファイルはカスペルスキーに自動的に送信されません。

> トレース ファイルは、人間が判読できる形式で保存されます。カスペルスキーに送信する前に、不正アクセスから情報を保護するようにしてください。

MMC管理プラグインのトレースファイル

管理コンソールを使用して Kaspersky Endpoint Security を管理する場合、MMC 管理プラグインの実行中に発生したイベントに関する情報を、管理サーバーがインストールされているデバイス上の Kaspersky Endpoint Security MMC プラグイントレースファイルに保存できます。ファイル名には、アプリケーションのバージョン番号、ファイルの作成日時、プロセス識別子 (PID) が含まれます。このファイルには、MMC プラグインの操作中に発生するイベント、特にポリシーとタスクの操作に関する情報が含まれています。

MMC プラグイントレースファイルは既定では生成されません。レジストリキーを使用して、MMC プラグイントレースファイルを作成できます。トレースファイルの作成方法の詳細については、テクニカルサポート担当者にお問い合わせください。

MMC プラグインの作成されたすべてのトレースファイルは、レジストリキーの設定時にユーザーが指定したフォルダーにあります。

Web 管理プラグインのトレースファイル

Web コンソールを使用して Kaspersky Endpoint Security を管理する場合、Web 管理プラグインの実行中に発生するイベントに関する情報を Web プラグイントレースファイルに書き込むことができます。

Web コンソールインストールウィザードで Web コンソールアクティビティのログが有効になっている場合、Web プラグインのトレースファイルは自動的に作成されます（詳細については、Kaspersky Security Center のヘルプを参照してください）。

Web プラグインのトレースファイルは、Web コンソールのインストールフォルダーの［logs］サブフォルダーに保存されます。

管理プラグインのトレースファイルのコンテンツ

トレースファイルには、次の一般的なデータが含まれています：

- イベントの時刻。
- 実行されているスレッドの数。
- イベントを発生させた製品コンポーネント。
- イベントの重要度（情報イベント、警告、緊急イベント、エラー）。
- 製品のコンポーネントによるコマンド実行に関係するイベントの説明と、このコマンドの実行結果。

トレースファイルには、一般的なデータに加えて、次の情報が含まれる場合があります：

- 姓、名、ミドルネームを含む個人データ （そのようなデータがファイルへのパスの一部である場合）。
- ユーザーアカウント名がファイル名の一部である場合、オペレーティングシステムへのログインに使用されるアカウントの名前。

ダンプファイルについて

*ダンプファイル*には、ダンプ作成時の Kaspersky Endpoint Security プロセスの作業メモリに関するすべての情報が含まれています。既定では、ダンプファイルは生成されません。アプリケーション障害が発生した場合のダンピングを有効または無効にできます。

ダンプを有効にすると、ダンプファイルは /var/opt/kaspersky/kesl/common/dumps および /var/opt/kaspersky/kesl/common/dumps-user に保存されます。

ダンプファイルにアクセスするには、root 権限が必要です。

ダンプファイルは、製品が使用されている限りコンピューターに保存されます。製品が削除されると完全に削除されます。ダンプ ファイルは カスペルスキーに自動的に送信されません。

ダンプファイルには、個人データが含まれる場合があります。カスペルスキーに送信する前に、不正アクセスから情報を保護するようにしてください。

ダンプのログ記録の有効化または無効化

Kaspersky Security Center を通じて Kaspersky Endpoint Security アプリケーションを管理している場合は、Web コンソールまたは管理コンソールを使用して、Kaspersky Endpoint Security のポリシー設定でダンプを有効または無効にできます。

コマンドラインを使用してアプリケーションを管理する場合は、kesl.ini 設定情報ファイルを介してダンプを有効または無効にすることができます。

ダンプファイルの最大数には制限があります。

オペレーティングシステムの設定によっては、ユーザーダンプファイルが作成されない場合があります。システムカーネルが `sysctl kernel.yama.ptrace_scope=0` を使用して設定されていることを確認してください。

Web コンソールでのダンピングの有効化または無効化

Web コンソールでは、ポリシーのプロパティ（［**アプリケーション設定**］→［**全般設定**］→［**アプリケーション設定**］の［**トレースとダンプの設定**］セクション）でダンプのログ記録を有効または無効にできます。

ダンプファイルの設定

設定	説明
アプリケーションがクラッシュした際にダンプファイルを作成する	このチェックボックスは、アプリケーションがクラッシュした時にダンプファイルの作成を有効または無効にします。 既定では、このチェックボックスはオフです。
ダンプファイルのディレクトリへのパス。	ダンプファイルが保存されているディレクトリへのパスの入力フィールド。入力フィールドは 128 文字に制限されています。 既定値：/var/opt/kaspersky/kesl/common/dumps。

ダンプファイルの設定を適用するには、アプリケーションを再起動する必要があります。

管理コンソールでのダンピングの有効化または無効化

管理コンソールでは、ポリシーのプロパティ（**全般設定 → 製品設定**）でダンプファイルのログ記録を有効または無効にすることができます。

［**トレースとダンプの設定**］で、［**構成**］をクリックすると、ダンプ設定を編集できるウィンドウが開きます。

設定	説明
アプリケーションがクラッシュした際にダンプファイルを作成する	このチェックボックスは、アプリケーションがクラッシュした時にダンプファイルの作成を有効または無効にします。 既定では、このチェックボックスはオフです。
ダンプファイルのディレクトリへのパス。	ダンプファイルが保存されているディレクトリへのパスの入力フィールド。入力フィールドは 128 文字に制限されています。 既定値：/var/opt/kaspersky/kesl/common/dumps。

ダンプファイルの設定を適用するには、アプリケーションを再起動する必要があります。

コマンドラインでのダンプの有効化または無効化

kesl.ini 設定情報ファイルを使用してダンプを有効または無効にするには、次の手順を実行します。

1. Kaspersky Endpoint Security を停止します。
2. ファイル /var/opt/kaspersky/kesl/common/kesl.ini を開いて編集します。
3. **[全般]** で、パラメータ値を設定します。
   - `CoreDumps = yes`：障害が発生した場合のダンプを有効にします。
   - `CoreDumps = no`：ダンピングを無効にします。
4. ダンプファイルが保存される既定のディレクトリを変更する場合は、`CoreDumpsPath` オプションでディレクトリへのパスを指定します。
5. Kaspersky Endpoint Security を起動します。

Kaspersky Security Center を使用したリモートデバイス診断

Kaspersky Security Center 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。リモート診断で、次の操作をリモートで実行できます：

- トレーシングの有効化または無効化。
- 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。
- リモートアプリケーションのインストールログのダウンロード。
- システムイベント (syslog) ログのダウンロード。
- アプリケーションの起動、停止および再起動。

Web コンソールでのリモート診断。

Web コンソールを使用して Kaspersky Endpoint Security を管理する場合、クライアントデバイスのリモート診断はリモート診断ウィンドウで実行されます。

デバイスのリモートデバイス診断ウィンドウを開きます：

1. Web コンソールのメインウィンドウで、**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. リモートで診断するデバイスを選択し、その名前をクリックします。
   デバイスのプロパティウィンドウが表示されます。
3. ［**詳細設定**］タブで、［**リモート診断**］セクションを選択します。

リモートデバイス診断ウィンドウでは、リモートアプリケーションのインストールログを表示できます。

デバイス上のリモートアプリケーションのインストールログを表示します：

1. リモートデバイス診断ウィンドウを開きます。
2. **イベントログ**タブの**トレースファイル**ブロックで、**リモートインストールログ**をクリックします。
   ［**デバイストレースイベントログ**］ウィンドウが開きます。

リモート診断の詳細については、Kaspersky Security Center のヘルプを参照してください。

管理コンソールを使用したリモート診断

管理コンソールを使用して Kaspersky Endpoint Security を管理する場合、リモート診断は、管理コンソールとともにデバイスに自動的にインストールされる特別な Kaspersky Security Center リモート診断ユーティリティを使用して実行されます。

リモート診断ユーティリティのメインウィンドウを開くには、次の手順を実行します。

1. 管理コンソールのツリーの**管理対象デバイス**フォルダで、必要なデバイスを含む管理グループを選択します。
2. 作業領域で、［**デバイス**］タブを選択します。
3. 管理対象デバイスのリストで、リモート診断ユーティリティを接続するデバイスを選択し、デバイスのコンテキストメニューから［**外部ツール**］→［**リモート診断**］を選択します。
   Kaspersky Security Center リモート診断ユーティリティのメインウィンドウが開きます。

リモートデバイス診断ユーティリティを使用して、リモートインストールログを表示できます。

デバイス上のリモートアプリケーションのインストールログを表示するには：

1. リモート診断ユーティリティのメインウィンドウが開きます。
2. 必要に応じて、ユーティリティをデバイスに接続するためのオプションを設定します。リモート診断ユーティリティのメインウィンドウで、［**ログイン**］をクリックします。
3. 開いたウィンドウのオブジェクトツリーで、**リモートインストールログ**フォルダーを選択します。

ネットワークエージェントの設定の詳細は、Kaspersky Security Center のヘルプを参照してください。

手動による管理サーバーへの接続の確認：Klnagchk ユーティリティ

ネットワークエージェント配布キットには、管理サーバーとの接続をチェックするための klnagchk ユーティリティが含まれています。

ネットワークエージェントのインストール後、ユーティリティがディレクトリ /opt/kaspersky/klnagent/bin（32 ビットオペレーティングシステムの場合）、またはディレクトリ /opt/kaspersky/klnagent64/bin（64 ビットオペレーティングシステムの場合）に配置されます。使用するキーに応じて、ネットワークエージェントは開始時に次の処理を実行します：

- 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を管理サーバーに接続するための設定値を表示するか、イベントログファイルに書き込みます。
- イベントログファイルに書き込みをするか、またはネットワークエージェントの統計情報（前回の起動時以降）とユーティリティの実行結果を表示します。
- ネットワークエージェントと管理サーバーとの間の接続の確立を試行します。
- 接続が確立できない場合、ユーティリティは ICMP パケットを送信して、管理サーバーがインストールされているデバイスのステータスを確認します。

ユーティリティの構文

```
klnagchk [-logfile <ファイル名>] [-sp] [-savecert <証明書ファイルのパス>] [-restart]
```

キーの説明

- `-logfile <ファイル名>`：ネットワークエージェントを管理サーバーに接続するための設定値と、ユーティリティの実行結果の両方をイベントログファイルに書き込みます。このキーが使用されない場合、設定、結果、およびエラーメッセージは画面に表示されます。
- `-sp`：プロキシサーバーのユーザー認証のパスワードを表示します。この設定は、プロキシサーバーを使用して管理サーバーへの接続が確立される場合に使用されます。
- `-savecert <ファイル名>`：管理サーバーへのアクセスを認証するために使用される証明書を指定したファイルに保存します。
- `-restart`：ネットワークエージェントを再起動します。

手動による管理サーバーへの接続：Klmover ユーティリティ

ネットワークエージェント配布キットには、管理サーバーとの接続を管理するための klmover ユーティリティが含まれています。

ネットワークエージェントのインストール後、ユーティリティがディレクトリ /opt/kaspersky/klnagent/bin（32 ビットオペレーティングシステムの場合）、またはディレクトリ /opt/kaspersky/klnagent64/bin（64 ビットオペレーティングシステムの場合）に配置されます。使用するキーに応じて、ネットワークエージェントは開始時に次の処理を実行します：

- 指定された設定を使用して、ネットワークエージェントを管理サーバーに接続します。
- イベントログファイルへの書き込みをするか、または動作結果を表示します。

ユーティリティの構文

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

キーの説明

- `-logfile <ファイル名>` – ユーティリティの実行結果を指定したファイルに書き込みます。このキーが使用されない場合、結果とエラーメッセージは stdout に表示されます。
- `-address <サーバーアドレス>` – 接続用の管理サーバーのアドレス。デバイスの IP アドレス、NetBIOS 名、または DNS 名を指定できます。
- `-pn <ポート番号>` – 管理サーバーへの暗号化されていない接続が確立されるポート番号。ポート 14000 が既定で使用されます。
- `-ps <SSL ポート番号>` – SSL プロトコルを使用して管理サーバーへの暗号化された接続が確立される SSL ポートの番号。ポート 13000 が既定で使用されます。
- `-nossl` – 管理サーバーに対して暗号化されていない接続を使用します。このキーが指定されていない場合、エージェントは暗号化された SSL プロトコルを使用して管理サーバーに接続します。
- `-cert <証明書ファイルへのパス>` – 新しい管理サーバーへのアクセス認証に、指定した証明書ファイルを使用します。このキーが使用されていない場合、ネットワークエージェントは管理サーバーへの最初の接続時に証明書を取得します。
- `-silent` – ユーティリティを非対話モードで起動します。このキーを使用すると、たとえばユーザー登録中に起動スクリプトからユーティリティが起動された場合などに役立ちます。
- `-dupfix` – ネットワークエージェントのインストール方法が配布キット内のインストールと異なる場合に、このキーを使用します。たとえば、ネットワークエージェントがディスクイメージから復元された場合などです。
- `-cloningmode 1` – クローニングモードへ切り替えます。
- `-cloningmode 0` – クローニングモードから切り替えます。

付録

このセクションでは、ヘルプの主要部分の補足情報を説明します。

付録1：リソース消費の最適化

オブジェクトのスキャン時に、Kaspersky Endpoint Security はプロセッサリソース、ディスクサブシステムの入出力、およびオペレーティングシステムを使用します。

製品によるリソース消費を表示するには、次のコマンドを実行します：

```
top -bn1|grep kesl
```

このコマンドは、システムのロード時に実行する必要があります。

コマンドの出力結果には、使用されているメモリの量とプロセッサの稼働時間が示されます：

```
651 root 20 0 3014172 2.302g 154360 S 120.0 30.0 0:32.80 kesl
```

列 6 には常駐メモリの量、`2.302g` が示されます。

列 9 にはプロセッサコアの使用率、120.0 が示されます。各コアは 100% で表されます。したがって、120% は、一方のコアがすべて使用され、もう一方が 20% 使用されていることを意味します。

オブジェクトのスキャン中に Kaspersky Endpoint Security を操作するとシステムの速度が大幅に低下する場合、システムリソースの消費を最適化するように製品を設定する必要があります。

リソースを消費するタスクの判定

どの製品タスクがシステムリソースを消費しているかを判断するには、ファイル脅威対策タスクのリソース消費（種別：OAS）とオンデマンドスキャンタスクのリソース消費（種別：ODS および ContainerScan）を区別する必要があります。

製品が Kaspersky Security Center ポリシーによって管理されている場合、調査期間中にローカルタスクの管理をできるようにする必要があります。

ファイル脅威対策タスクの動作分析

ファイル脅威対策タスクの動作を分析するには：

1. すべてのスキャンタスクと監視タスクを停止します。
2. オンデマンドスキャンタスクがスキャン中に実行されないこと、または実行スケジュールが設定されていないことを確認してください。Kaspersky Security Center を使用するか、次の手順を実行してローカルで実行できます：

a. すべてのアプリケーションタスクの一覧を取得します。次のコマンドを実行します：

```
kesl-control --get-task-list
```

b. マルウェアのスキャンタスクのスケジュール設定を取得します。次のコマンドを実行します：

```
kesl-control --get-schedule <タスク ID>
```

コマンドの出力が `RuleType=Manual` の場合、タスクは手動でのみ開始できます。

c. すべてのマルウェアのスキャンタスクのスケジュール設定を取得し、手動での開始に設定します。次のコマンドを実行します：

```
kesl-control --set-schedule <タスク ID> RuleType=Manual
```

3. 次のコマンドを実行して、高レベルの詳細を含むアプリケーション トレース ファイルの生成を有効にします：

```
kesl-control --set-app-settings TraceLevel=Detailed
```

4. ファイル脅威対策タスクが開始されていない場合は開始します。次のコマンドを実行します：

```
kesl-control --start-task 1
```

5. パフォーマンスの問題を引き起こしたモードでシステムをロードします。数時間で十分です。

ロード中、製品はトレースファイルに多くの情報を書き込みます。ただし、既定では 500MB のファイルが 5 つしか保存されないため、古い情報は上書きされます。パフォーマンスとリソース消費の問題が発生しなくなった場合は、オンデマンドスキャンタスクが原因である可能性が高く、ContainerScan および ODS スキャンタスクの動作の分析に進むことができます。

6. 製品トレースファイルの作成を無効にします。次のコマンドを実行します：

```
kesl-control --set-app-settings TraceLevel=None
```

7. 最も頻繁にスキャンされたオブジェクトのリストを確認します。次のコマンドを実行します：

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | sort | uniq -c | sort -k1 -n -r|less
```

結果は、テキスト ビューアー ユーティリティである less に読み込まれ、最も多くスキャンされたオブジェクトが最初に表示されます。

8. 最も多くスキャンされたオブジェクトが危険かどうかを判断します。問題がある場合は、テクニカルサポートにお問い合わせください。

たとえば、信頼するプロセスがディレクトリとログファイルに書き込む場合、それらのディレクトリとログファイルは安全であると判断することができ、データベースファイルも安全であると考えられます。

9. 安全と思われるオブジェクトのパスを控えておいてください。スキャン範囲からの除外を設定するには、パスが必要になります。

10. 様々なサービスがシステム内のファイルにデータを頻繁に書き込む場合、そのようなファイルは保留中のキューで再度スキャンされます。保留中のキューで最も頻繁にスキャンされたパスのリストを確認します。次のコマンドを実行します：

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $9}' | sort | uniq -c | sort -k1 -n -r
```

最も頻繁にスキャンされたファイルがリストの最初に表示されます。

11. ファイルのカウンターが数時間で数千を超える場合は、スキャンから除外するために、このファイルが信頼できるかどうかを確認する必要があります。

それを決定するロジックは、前の調査（ステップ 8 を参照）と同じです。ログファイルは起動できないため、安全であると判断することができます。

12. 一部のファイルがリアルタイム保護タスクのスキャンから除外されたとしても、それらのファイルは本製品によってインターセプトされる可能性があります。特定のファイルをリアルタイム保護から除外してもパフォーマンスが大幅に向上しない場合は、これらのファイルが配置されているマウントポイントを本製品のインターセプトの範囲から完全に除外できます。除外するには、次の手順を実行します：

    a. 次のコマンドを実行し、本製品がインターセプトしたファイルのリストを取得します：

    ```
    grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | sort | uniq -c | sort -k1 -n -r
    ```

    b. このリストを使用して、ほとんどのファイル操作のインターセプトに使用されるパスを特定し、インターセプトの例外を設定します。

オンデマンドスキャンタスクの動作分析

種別が ODS および ContainerScan のタスクは、大量のリソース消費を引き起こす可能性もあります。種別が ODS のタスクについては、次の推奨事項に従ってください：

- 複数のオンデマンドスキャンタスクが同時に実行されていないことを確認してください。製品はこのモードでの操作を許可しますが、リソース消費は大幅に増加する可能性があります。種別が ODS および ContainerScan のすべてのタスクのスケジュールをローカルで（ファイル脅威対策タスクでの説明を参照）、または Kaspersky Security Center を使用して確認します。
- サーバー負荷が最小である時間にスキャンを実行します。
- 指定されたスキャンのパスにマウントされたリモートリソース（SMB / NFS）がないことを確認してください。リソースを提供するサーバーでリモートリソースのスキャンタスクを直接実行できない場合は、重要なサービスを備えたサーバーでリソーススキャンを実行しないでください。このタスクの実行には時間がかかる可能性があります（接続速度とファイル数によって異なります）。
- 開始する前に、オンデマンドスキャンタスクの設定を最適化します。

ファイル脅威対策タスクの設定

ファイル脅威対策タスクの動作の分析後に、スキャン範囲から除外できるディレクトリとファイルのリストを作成した場合は、それらを除外に追加する必要があります。

スキャンの除外

/tmp/logs ディレクトリとすべてのサブディレクトリおよびファイルを再帰的に除外するには、次のコマンドを実行します：

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

/tmp/logs ディレクトリ内の特定のファイルをマスクで除外するには、次のコマンドを実行します：

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

再帰マスクを使用して、/tmp/ ディレクトリおよびサブディレクトリ内の拡張子が .log のすべてのファイルを除外するには、次のコマンドを実行します：

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

インターセプターの除外

特定のディレクトリ内のファイルをスキャンだけでなくインターセプターからも除外する場合は、マウントポイント全体を除外できます。

マウントポイント全体を除外するには：

1. ディレクトリがマウントポイントでない場合は、そこからマウントポイントを作成します。たとえば、/tmp ディレクトリからマウントポイントを作成するには、次のコマンドを実行します：

   ```
   mount --bind /tmp/ /tmp
   ```

2. サーバーの再起動後もマウントポイントを維持するには、/etc/fstab ファイルに次の行を追加します：

   ```
   /tmp /tmp none defaults,bind 0 0
   ```

3. /tmp ディレクトリをグローバル除外リストに追加します。次のコマンドを実行します：

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
   ```

4. 複数のディレクトリを追加する場合は、item_0000 カウンターを 1 つ増やします（item_0001、item_0002 など）。

接続が不安定または速度が遅いリモートリソースにマウントされているマウントポイントも除外することを推奨します。

スキャン種別の変更

既定では、ファイル脅威対策タスクは、ファイルを開いたり閉じたりする時にそのファイルをスキャンできます。ファイル脅威保護タスクのパフォーマンス分析で、書き込まれているファイルが多すぎることが判明した場合は、次のコマンドを実行して、ファイルが開かれているときにのみタスクが実行されるようにできます。

```
kesl-control --set-set 1 ScanByAccessType=Open
```

この動作モードでは、ファイルを開いた後に加えられた変更は、次にファイルを開くまでスキャンされません。

オンデマンドスキャンタスクの設定

スキャンの除外

オンデマンド ODS および ContainerScan タスクのスキャン除外を定義できます。これは、ファイル脅威対策タスクのスキャン除外と同じ方法で設定できます。

1 つのスキャンタスクのスキャン除外設定は、他のスキャンタスクには影響しません。除外はスキャンタスクごとに個別に設定する必要があります。

アーカイブの展開時における、メモリ使用の制限設定

オンデマンドスキャンタスクでは、アーカイブを再帰的にスキャンする時に、メモリを使用してアーカイブを展開します。既定では、制限は使用可能なすべてのメモリの 40% ですが、2GB 以上です。そのため、システムに 5GB を超えるメモリがある場合は、メモリ使用量の制限を手動で設定できます。これは、数百ギガバイトのメモリを搭載したサーバーなどで特に役立ちます。

製品のメモリ使用制限の設定

Kaspersky Endpoint Security が OAS、ODS、および ContainerScan のスキャンタスクを実行する際に使用する RAM の容量を制限できます。

本製品は、既定で利用可能な RAM 全体の40%以下を使用します。メモリ使用量制限は、大量の RAM (5 GB 以上) を搭載したシステムに役立つ場合があります。

kesl.ini 設定情報ファイルの `ScanMemoryLimit` オプションを使用すると、ファイルのスキャン時に本製品が使用する RAM のサイズを調整できます。既定値は 8192 MB です。

この設定は、ファイルのスキャン時に使用されるメモリの量のみを制限します。これは、本製品に必要なメモリの総量が、この設定の値を超える可能性があることを意味します。

ファイルスキャン時のメモリ使用の制限を指定するには：

1. Kaspersky Endpoint Security を停止します。
2. ファイル /var/opt/kaspersky/kesl/common/kesl.ini を開いて編集します。
3. **[General]** で、必要な RAM の量を `ScanMemoryLimit` に指定します。

   `ScanMemoryLimit=<` メガバイト単位のメモリ量 `>`

   最小値は 2048 MB です。値が 2048 MB 未満の場合、本製品は最小値を使用します。

   システム RAM サイズを超える値を指定した場合、本製品は使用可能なすべての RAM の最大 40% を使用します。
4. Kaspersky Endpoint Security を起動します。

ファイルスキャン用の新しいメモリ使用制限は、製品の再起動後に有効になります。

付録 2：Kaspersky Endpoint Security を管理するコマンド

コマンドラインでは、Kaspersky Endpoint Security 管理コマンドを使用して、Kaspersky Endpoint Security を管理します。

次のコマンドを実行すれば、管理コマンドのヘルプが表示されます：

`kesl-control --help <` コマンドグループの接頭辞 `>`

< コマンドグループ接頭辞 > では次の値を利用できます：

- -A：アプリケーションコントロールを管理するコマンド

- -B：バックアップを管理するコマンド
- -C：コンテナースキャンの全般設定を管理するコマンド
- -D：デバイスコントロールを管理するコマンド
- -E：製品イベントを管理するコマンド
- -F：ファイアウォールを管理するコマンド
- -H：ブロックされたデバイスを管理するコマンド
- -L：ライセンスを管理するコマンド
- -N：暗号化された接続のスキャン設定を管理するコマンド
- -R: Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response (KATA) および Kaspersky Endpoint Detection and Response Optimum の連携の設定を管理するためのコマンド
- -S：統計コマンド
- -T：製品のタスクと設定を管理するコマンド
- -U：ユーザーとユーザーロールを管理するコマンド
- -V：仮想環境を保護する Light Agent モードでの本製品のコマンド
- -W：イベントを表示するコマンド

製品のタスクと設定を管理するためのコマンド

「-T」は、製品設定とタスクを管理するためのコマンドのグループに、そのコマンドが属することを示す接頭辞です。

「-C」は、コンテナースキャン設定を管理するためのコマンドのグループに、そのコマンドが属することを示す接頭辞です。

「-N」は、安全な接続のスキャン設定を管理するためのコマンドのグループに、そのコマンドが属することを示す接頭辞です。

kesl-control --export-settings

このコマンドは、すべてのアプリケーション設定をコンソールに出力するか、設定情報ファイルにエクスポートします。これらには、コンテナースキャンの全般設定、暗号化された接続スキャン設定、アプリケーションの全般設定、およびタスク設定が含まれます。

コマンド構文

```
kesl-control [-T] --export-settings [--file <設定情報ファイルのパス>] [--json]
```

引数とキー

`--file <設定情報ファイルのパス>` - アプリケーション設定を保存する設定情報ファイルの絶対パス。

`--json` を指定すると、設定はJSON形式で出力されます。もし `--json` キーが指定されなければ、設定は INI 形式でインポートされます。

kesl-control --import-settings

このコマンドは、コンテナースキャンの全般設定、暗号化された接続スキャン設定、アプリケーションの全般設定、およびタスク設定を含むすべてのアプリケーション設定を設定情報ファイルからインポートします。

コマンド構文

`kesl-control [-T] --import-settings --file <設定情報ファイルのパス> [--json]`

引数とキー

`--file <設定情報ファイルのパス>` - 本製品へ設定をインポートする設定情報ファイルの絶対パス。

`--json` を指定すると、設定情報ファイルの設定を JSON 形式でインポートします。`--jason` のライセンスが指定されていない場合、設定は INI ファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

kesl-control --update-application

このコマンドは、ダウンロードされたアプリケーションモジュールのアップデートをインストールします。

> アプリケーションが標準モードで使用されている場合にのみ実行できます。

コマンド構文

`kesl-control [-T] --update-application`

本製品の全般設定を管理するコマンド

kesl-control --get-app-settings コマンド

このコマンドは、本製品の全般設定の現在の値をコンソールまたは設定ファイルに出力します。

コマンド構文

`kesl-control [-T] --get-app-settings [--file <設定情報ファイルのパス>] [--json]`

引数とキー

`--file <設定情報ファイルのパス>` - 本製品の全般設定が表示される設定情報ファイルのパス。`--file` オプションを指定しない場合、設定がコンソールに出力されます。

パスなしでファイルの名前を指定した場合、そのファイルは現在のディレクトリに作成されます。ファイルが指定されたパスに既に存在する場合は、上書きされます。指定されたディレクトリが存在しない場合、設定情報ファイルは生成されません。

--json を指定すると、設定はJSON形式で出力されます。もし --json キーが指定されなければ、設定は INI 形式でインポートされます。

kesl-control --set-app-settings コマンド

このコマンドは、コマンドオプションまたは設定情報ファイルから設定をインポートすることによって、本製品の全般設定を構成します。

コマンド構文

コマンドオプションで設定を定義します：

```
kesl-control [-T] --set-app-settings <オプション名>=<オプション値> [<オプション名>=<オプション値>]
```

設定情報ファイルを介して設定を定義します：

```
kesl-control [-T] --set-app-settings --file <設定情報ファイルのパス> [--json]
```

引数とキー

オプション名>=オプション値>: アプリケーションの全般設定の名前と値。

--file <設定情報ファイルのパス> - 本製品へインポートしたい設定情報ファイル元への絶対パス。

--json を指定すると、設定情報ファイルの設定を JSON 形式で本製品にインポートします。--jason のライセンスが指定されていない場合、設定は INI ファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

タスク設定を管理するコマンド

kesl-control --get-settings

このコマンドは、指定されたタスクの現在の設定をコンソールまたは設定情報ファイルに出力します。

コマンド構文

```
kesl-control [-T] --get-settings <タスク ID / 名> [--file <設定情報ファイルのパス>] [--json]
```

引数とキー

<タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

--file <設定情報ファイルのパス> - タスク設定を書き込む設定情報ファイルへのパス。--file オプションを指定しない場合、設定がコンソールに出力されます。

パスなしでファイルの名前を指定した場合、そのファイルは現在のディレクトリに作成されます。ファイルが指定されたパスに既に存在する場合は、上書きされます。指定されたディレクトリが存在しない場合、設定情報ファイルは生成されません。

--json を指定すると、設定はJSON形式で出力されます。もし --json キーが指定されなければ、設定は INI 形式でインポートされます。

kesl-control --set-settings

このコマンドは、コマンドオプションを使用するか、設定情報ファイルから設定をインポートすることによって、指定されたタスクの設定を定義します。

コマンド構文

コマンドオプションで設定を定義します：

```
kesl-control [-T] --set-settings <タスク 名 / ID> <オプション名>=<オプション値> [<オプション名>=<オプション値>] [--add-path <パス>] [--del-path <パス>] [--add-exclusion <パス>] [--del-exclusion <パス>]
```

設定情報ファイルを介して設定を定義します：

```
kesl-control [-T] --set-settings <タスク 名 / ID> --file <設定情報ファイルのパス> [--json]
```

引数とキー

<タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

<設定名>=<設定値> はタスク設定の名前と値です。

--add-path <path> は、スキャンするオブジェクトのあるディレクトリへのパスを追加します。

--del-path <path> は、スキャンするオブジェクトのあるディレクトリへのパスを削除します。

--add-exclusion <path>：スキャンから除外するオブジェクトが含まれるディレクトリへのパスを追加します。

--del-exclusion <path> は、スキャンするオブジェクトのあるディレクトリへのパスを除外します。

--file <設定情報ファイルのパス> – タスク設定をインポートする設定情報ファイルの絶対パス。

--json を指定すると、設定情報ファイルの設定を JSON 形式でインポートします。--jason のライセンスが指定されていない場合、設定は INI ファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

kesl-control --set-to-default

このコマンドは、指定されたタスクの既定を復元します。

コマンド構文

```
kesl-control [-T] --set-settings <タスク ID / 名> --set-to-default
```

引数とキー

<タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

kesl-control --get-schedule コマンド

このコマンドは、指定されたタスクの現在のスケジュールをコンソールまたは設定情報ファイルに出力します。

コマンド構文

```
kesl-control [-T] --get-schedule <タスク ID / 名> [--file <設定情報ファイルのパス>] [--json]
```

引数とキー

<タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

--file <設定情報ファイルへのパス> は、タスク実行スケジュールの設定が出力される設定情報ファイルへのパスです。--file オプションを指定しない場合、設定がコンソールに出力されます。

パスなしでファイルの名前を指定した場合、そのファイルは現在のディレクトリに作成されます。ファイルが指定されたパスに既に存在する場合は、上書きされます。指定されたディレクトリが存在しない場合、設定情報ファイルは生成されません。

--json を指定すると、設定はJSON形式で出力されます。もし --json キーが指定されなければ、設定は INI 形式でインポートされます。

kesl-control --set-schedule コマンド

このコマンドは、コマンドオプションを使用するか、設定情報ファイルから設定をインポートすることによって、指定されたタスクのスケジュールを定義します。

コマンド構文

コマンドオプションで設定を定義します：

```
kesl-control [-T] --set-schedule <タスク ID / 名> <オプション名>=<オプション値> [<オプション名>=<オプション値>]
```

設定情報ファイルを介して設定を定義します：

```
kesl-control [-T] --set-schedule <タスク ID / 名> --file <設定情報ファイルのパス> [--json]
```

引数とキー

<タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

<設定名>=<設定値> は、タスクスケジュールの設定の1つの名前と値です。

--file <設定情報ファイルのパス> - タスクスケジュール設定をインポートする設定情報ファイルの絶対パス。

--json を指定すると、設定情報ファイルの設定を JSON 形式でインポートします。--jason のライセンスが指定されていない場合、設定は INI ファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

タスクを管理するコマンド

kesl-control --get-task-list

このコマンドは、既存タスクのリストを出力します。

コマンド構文

```
kesl-control [-T] --get-task-list [--json]
```

引数とキー

--json を指定すると、設定はJSON形式で出力されます。

kesl-control --get-task-state

このコマンドは、指定されたタスクのステータスを出力します。

コマンド構文

```
kesl-control [-T] --get-task-state <タスク ID / 名> [--json]
```

引数とキー

<タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

--json を指定すると、設定はJSON形式で出力されます。

kesl-control --create-task

このコマンドは、既定または設定情報ファイルで指定された設定で、指定されたタイプのタスクを作成します。

コマンド構文

既定でタスクを作成します：

```
kesl-control [-T] --create-task <タスク名> --type <タスクの種別>
```

設定情報ファイルの設定でタスクを作成します：

```
kesl-control [-T] --create-task <タスク名> --type <タスクの種別> --file <設定情報ファイルへのパス> [--json]
```

引数とキー

< タスク名 > は、新しいタスクに指定する名前です。

< task type > は、作成されたタスクタイプの識別子です。

--file < 設定情報ファイルのパス > : 設定をインポートする設定情報ファイルからの絶対パスです。

--json を指定すると、設定情報ファイルの設定を JSON 形式でインポートします。--jason のライセンスが指定されていない場合、設定は INI ファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

kesl-control --delete-task

このコマンドはタスクを削除します。

コマンド構文

kesl-control [-T] --delete-task < タスク ID / 名 >

引数とキー

< タスク ID / 名 > は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

kesl-control --start-task

このコマンドはタスクを開始します。

コマンド構文

kesl-control [-T] --start-task < タスク ID / 名 > [-W] [--progress]

引数とキー

< タスク ID / 名 > は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

[-W] : 現在のイベントの出力を有効にします。

[--progress] : タスクの進行状況を表示します。

kesl-control --stop-task

このコマンドはタスクを停止します。

コマンド構文

kesl-control [-T] --stop-task < タスク ID / 名 > [-W]

引数とキー

< タスク ID / 名 > は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

[-W] : 現在のイベントの出力を有効にします。

kesl-control --suspend-task

このコマンドはタスクを一時停止します。

コマンド構文

```
kesl-control [-T] --suspend-task <タスク ID / 名>
```

引数とキー

<タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

kesl-control --resume-task

このコマンドはタスクを再開します。

コマンド構文

```
kesl-control [-T] --resume-task <タスク ID / 名>
```

引数とキー

<タスク ID / 名> は、タスク作成時に割り当てられたID、またはコマンドラインでのタスク名です。

kesl-control --scan-file

このコマンドは、オブジェクトスキャンタスクを作成して実行します。

コマンド構文

```
kesl-control [-T] --scan-file <パス> [--action <処理>]
```

引数とキー

<path>：スキャンしたいファイルやディレクトリへのパスです。スペースで区切って複数のパスを指定することもできる。

--action <action> は、感染したオブジェクトに対してアプリケーションが実行する処理です。--action キーを指定しないと、アプリケーションは推奨される処理を実行します。

kesl-control --scan-container

このコマンドは、コンテナまたはイメージのカスタムスキャンタスクを作成して実行します。

コマンド構文

```
kesl-control [-T] --scan-container <コンテナ / イメージ[:タグ]>
```

引数とキー

<コンテナ / イメージ [:タグ]>：コンテナ / イメージ ID / 名。マスクを使用して複数のオブジェクトをスキャンできます。

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を1つ指定することができます。例：「/dir/*/file」または「/dir/*/*/file」

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：「/dir/**/file*/」または「/dir/file**/」

アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。

ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。

コンテナースキャンの全般設定を管理するコマンド

kesl-control --get-container-settings コマンド

このコマンドは、コンテナースキャンの全般設定の現在の値をコンソールまたは設定情報ファイルに出力します。

コマンド構文

kesl-control [-C] --get-container-settings [--file <設定情報ファイルのパス>] [--json]

引数とキー

--file <設定情報ファイルのパス>：コンテナースキャンの全般設定が保存される設定情報ファイルへのパスです。--file オプションを指定しない場合、設定はコンソールに出力されます。

パスなしでファイルの名前を指定した場合、そのファイルは現在のディレクトリに作成されます。ファイルが指定されたパスに既に存在する場合は、上書きされます。指定されたディレクトリが存在しない場合、設定情報ファイルは生成されません。

--json を指定すると、設定はJSON形式で出力されます。もし --json キーが指定されなければ、設定は INI 形式でインポートされます。

kesl-control --set-container-settings コマンド

このコマンドは、コマンドオプションまたは設定情報ファイルから設定をインポートすることによって、コンテナースキャンの全般設定を構成します。

コマンド構文

コマンドオプションで設定を定義します：

kesl-control [-C] --set-container-settings <設定名>=<設定値> [<設定名>=<設定値>]

設定情報ファイルを介して設定を定義します：

kesl-control [-C] --set-container-settings --file <設定情報ファイルのパス> [--json]

引数とキー

<オプション名> = <オプション値>: コンテナースキャンの全般設定の名前と値。

`--file` <構成ファイルのパス>：構成ファイルへの絶対パスです。このファイルのコンテナースキャンの全般設定がアプリケーションにインポートされます。

`--json` を指定すると、設定情報ファイルの設定を JSON 形式で本製品にインポートします。`--jason` のライセンスが指定されていない場合、設定は INI ファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

暗号化された接続のスキャン設定を管理するコマンド

「-N」は、安全な接続のスキャン設定を管理するためのコマンドのグループに、そのコマンドが属することを示す接頭辞です。

kesl-control -N --query

このコマンドは、暗号化された接続のスキャンからの除外リストを出力します。

- ユーザーが追加した除外項目のリスト
- 本製品によって追加された除外項目のリスト
- 本製品のデータベースから受信した除外項目のリスト

コマンド構文

```
kesl-control -N --query user

kesl-control -N --query auto

kesl-control -N --query kl
```

kesl-control --clear-web-auto-excluded

このコマンドは、アプリケーションがスキャンから自動的に除外したドメインのリストを消去します。

コマンド構文

```
kesl-control -N --clear-web-auto-excluded
```

kesl-control --get-net-settings

このコマンドは、現在の暗号化された接続スキャンをコンソールまたは設定情報ファイルに出力します。

コマンド構文

```
kesl-control [-N] --get-net-settings [--file <設定情報ファイルのパス>] [--json]
```

引数とキー

`--file <設定情報ファイルのパス>`：暗号化された接続のスキャン設定を出力する設定情報ファイルへのパスです。`--file` オプションを指定しない場合、設定がコンソールに出力されます。

パスなしでファイルの名前を指定した場合、そのファイルは現在のディレクトリに作成されます。ファイルが指定されたパスに既に存在する場合は、上書きされます。指定されたディレクトリが存在しない場合、設定情報ファイルは生成されません。

`--json` を指定すると、設定はJSON形式で出力されます。もし `--json` キーが指定されなければ、設定は INI 形式でインポートされます。

kesl-control --set-net-settings

このコマンドは、コマンドオプションまたは設定情報ファイルから設定をインポートすることによって、暗号化された接続スキャンの全般設定を構成します。

コマンド構文

コマンドオプションで設定を定義します：

`kesl-control [-N] --set-net-settings <オプション名>=<オプション値> [<オプション名>=<オプション値>]`

設定情報ファイルを介して設定を定義します：

`kesl-control [-N] --set-net-settings --file <設定情報ファイルのパス> [--json]`

引数とキー

`<オプション名> = <オプション値>`: 暗号化された接続のスキャンオプションの名前と値。

`--file <設定情報ファイルのパス>`：暗号化された接続のスキャン設定をインポートする設定情報ファイルからの絶対パスです。

`--json` を指定すると、設定情報ファイルの設定を JSON 形式で本製品にインポートします。`--jason` のライセンスが指定されていない場合、設定は INI ファイルからインポートされます。インポートが失敗すると、エラーが表示されます。

kesl-control --add-certificate

このコマンドは、信頼できる証明書のリストに証明書を追加します。

コマンド構文

`kesl-control [-N] -add-certificate <証明書のパス>`

引数とキー

`<証明書のパス>` は、追加する証明書ファイルへのパスです（PEM または DER 形式）。

kesl-control --remove-certificate

このコマンドは、信頼できる証明書のリストから証明書を削除します。

コマンド構文

`kesl-control [-N] --remove-certificate <証明書のサブジェクト>`

kesl-control --list-certificates

このコマンドは、信頼できる証明書のリストを出力します。

コマンド構文

`kesl-control [-N] --list-certificates`

統計コマンド

「-S」は、統計コマンドグループにそのコマンドが属することを示す接頭辞です。

kesl-control --app-info

このコマンドは、アプリケーションに関する情報を出力します。

コマンド構文

`kesl-control [-S] --app-info [--json]`

引数とキー

`--json` を指定すると、設定はJSON形式で出力されます。

kesl-control --omsinfo

このコマンドは、Microsoft Operations Management Suite と連携するための JSON ファイルを作成します。

コマンド構文

`kesl-control [-S] --omsinfo --file <ファイル名とパス>`

イベントを表示するコマンド

kesl-control -W

このコマンドは、現在の製品イベントの表示を有効にします。このコマンドにより、イベント名、およびイベントに関する追加情報が表示されます。このコマンドを使用すると、現在の製品イベントをすべて表示することも、現在実行中のタスクに関連付けられているイベントのみを表示することもできます。

コマンド構文

```
kesl-control -W [--query "<フィルター条件>"]
```

引数とキー

<フィルタ条件>：<フィールド> <比較演算子> '<値>' 形式の1つまたは複数の論理式。論理演算子と組み合わせて、特定の現在のイベントを出力します。

製品イベントを管理するコマンド

-E：アプリケーションイベントの管理に使用されるコマンドのグループに、そのコマンドが属することを示す接頭辞です。

kesl-control -E

このコマンドは、アプリケーションイベントログ内のすべてのイベントに関する情報を出力します。`less` コマンドを使用して、表示されたイベントのリストを操作できます。

コマンド構文

```
kesl-control -E
```

kesl-control -E --query

このコマンドは、アプリケーションイベントログからのイベントに関する情報を出力します。`less` コマンドを使用して、表示されたイベントのリストを操作できます。フィルターを使用して、特定のイベントを出力したり、イベントのリストをファイルに出力したりできます。

コマンド構文

```
kesl-control -E --query "<フィルター条件>" [--db <データベースファイル>] [-n <数値>] --file <ファイル名とパス> [--json] [--reverse]
```

引数とキー

<データベースファイル> は、イベントの出力元となるイベントログデータベースファイルへの絶対パスです。既定では、イベントに関する情報は、データベース /var/opt/kaspersky/kesl/private/storage/events.db に保存されます。データベースの場所は、EventsStoragePath のアプリケーショングローバル設定によって決まります。

<フィルター条件>：<フィールド> <比較演算子> '<値>' 形式の1つまたは複数の論理式。論理演算子と組み合わせて、結果を限定します。

<数値> - 表示される選択の最新のイベントの数（選択の最後からのレコードの数）。

`--file` <ファイル名とパス>：イベントを出力するファイルへの絶対パスです。パスを指定しないでファイルの名前を指定した場合、そのファイルは現在のディレクトリに作成されます。指定された名前のファイルが指定されたパスに既に存在する場合は、上書きされます。指定されたディレクトリがディスクに見つからない場合、ファイルは作成されません。

`--file` オプションを指定しない場合、イベントのリストがコンソールに出力されます。

`--json`：イベントを JSON 形式で出力します。

`--reverse`：イベントを逆の順序で表示します（最新のイベントが上に表示され、最も古いイベントが下に表示されます）。

ライセンスを管理するコマンド

「-L」は、ライセンスの管理に使用されるコマンドのグループに、そのコマンドが属することを示す接頭辞です。

ライセンスの追加と削除のコマンドは、アプリケーションが標準モードで使用されている場合にのみ実行できます。Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護すると、ライセンスを管理するコマンドがエラーで終了します。このアプリケーションは、Kaspersky Security for Virtualization Light Agent の一部として有効化されるため、アプリケーションを個別に有効化する必要はありません。

kesl-control --add-active-key

このコマンドを使用すると、ライセンスファイルまたはアクティベーションコードを使用して、現在のライセンスを本製品に追加できます。

このコマンドを使用すると、現在の製品ライセンスと現在の EDR Optimum ライセンスを追加できます。コマンドでライセンスの種別を指定する必要はありません。

コマンド構文

`kesl-control [-L] --add-active-key` <ライセンス情報ファイルパス>

`kesl-control [-L] --add-active-key` <アクティベーションコード>

引数とキー

<ライセンス情報ファイルへのパス> - ライセンス情報ファイルへのパス。ライセンス情報ファイルが現在のディレクトリにある場合は、ファイル名だけを指定します。

<アクティベーションコード> - アクティベーションコード。

例：
/home/test/00000001.key ファイルから、現在のライセンスとして追加します：

```
kesl-control --add-active-key /home/test/00000001.key
```

kesl-control --add-reserve-key

このコマンドを使用すると、ライセンスファイルまたはアクティベーションコードを使用して、予備のライセンスを本製品に追加できます。

このコマンドを使用すると、予備の製品ライセンス と予備の EDR Optimum ライセンスを追加できます。コマンドでライセンスの種別を指定する必要はありません。

デバイス上の製品に現在のライセンスがまだ追加されていない場合、コマンドは失敗します。

コマンド構文

```
kesl-control [-L] --add-reserve-key <ライセンス情報ファイルパス>

kesl-control [-L] --add-reserve-key <アクティベーションコード>
```

引数とキー

<ライセンス情報ファイルへのパス> - ライセンス情報ファイルへのパス。ライセンス情報ファイルが現在のディレクトリにある場合は、ファイル名だけを指定します。

<アクティベーションコード> - アクティベーションコード。

例：
/home/test/00000002.key ファイルを使用して、予備のライセンスを追加します：

```
kesl-control --add-reserve-key /home/test/00000002.key
```

kesl-control --remove-active-key

このコマンドを使用すると、現在のライセンスを削除できます。

コマンド構文

```
kesl-control [-L] --remove-active-key [--edr-optimum]
```

引数とキー

`--edr-optimum` – 現在の EDR Optimum ライセンスを削除します。`--edr-optimum` オプションを指定しないと、Kaspersky Endpoint Security の現在のライセンスが削除されます。

kesl-control --remove-reserve-key

このコマンドを使用すると、予備のライセンスを削除できます。

コマンド構文

```
kesl-control [-L] --remove-reserve-key [--edr-optimum]
```

引数とキー

`--edr-optimum` – 予備の EDR Optimum ライセンスを削除します。`--edr-optimum` オプションを指定しないと、Kaspersky Endpoint Security の予備のライセンスが削除されます。

kesl-control -L --query

`-L --query` コマンドは、アプリケーションの有効化に使用されたライセンスと、現在使用されているライセンスに関する情報を出力します。

コマンド構文

```
kesl-control -L --query [--json]
```

引数とキー

`--json`：データを JSON 形式で出力します。

kesl-control --load-mdr-blob

`--load-mdr-blob` コマンドは、Kaspersky Managed Detection and Response との連携に必要な BLOB 設定ファイルをダウンロードします。

コマンド構文

```
kesl-control [-L] --load-mdr-blob <MDR BLOB 設定情報ファイルのパス>
```

kesl-control --remove-mdr-blob

`--remove-mdr-blob` コマンドは、Kaspersky Managed Detection and Response との連携に必要な BLOB 設定ファイルを削除します。

コマンド構文

```
kesl-control [-L] --remove-mdr-blob
```

ファイアウォールを管理するコマンド

-F：コマンドがファイアウォール管理コマンドに属することを示す接頭辞。

kesl-control --add-rule

このコマンドは、新しいネットワークパケットルールを追加します。

コマンド構文

```
kesl-control [-F] --add-rule [--name <ルールの名前>] [--action <処理>] [--protocol <プロトコル>] [--direction <通信方向>] [--remote <アドレスの削除>[:<ポートの範囲>]] [--local <ローカルアドレス>[:<ポートの範囲>]] [--at <インデックス>]
```

引数とキー

`--name <ルールの名前>` は、ネットワークパケットルールの名前です。

`--action <処理>` は、ネットワークパケットルールで指定された接続に対して実行される処理です。

`--protocol <プロトコル>` は、ネットワークアクティビティを監視したいデータ転送プロトコルの種別です。

`--direction <通信方向>` は、監視するネットワークアクティビティの通信方向です。

`--remote <リモートアドレス>[:<ポートの範囲>]`：リモートデバイスのネットワークアドレス。

--local <ローカルアドレス>[:<ポートの範囲>]：Kaspersky Endpoint Securityがインストールされているデバイスのネットワークアドレス。

--at <インデックス>：ネットワークパケットルールのリスト中のルールの番号。--at ライセンスが指定されていない場合、または値がリストのルールの数より大きい場合、新しいルールがリストの最後に追加されます。

コマンドで値を指定しなかったパラメータは、既定値に設定されます。

kesl-control --del-rule

このコマンドは、ルールのリスト内の指定された名前またはインデックスを持つネットワークパケットルールを削除します。

コマンド構文

```
kesl-control -F --del-rule --name <ルール名>

kesl-control [-F] --del-rule --index <インデックス>
```

引数とキー

--name <ルールの名前> は、ネットワークパケットルールの名前です。

--index <インデックス>：ネットワークパケットルールのリスト中のルールの番号。

kesl-control --move-rule

このコマンドは、ネットワークパケットルールの実行の優先度を変更します。

コマンド構文

```
kesl-control [-F] --move-rule --name <ルール名> --at <インデックス>

kesl-control [-F] --move-rule --index <インデックス> --at <インデックス>
```

引数とキー

--name <ルールの名前> は、ネットワークパケットルールの名前です。

--index <インデックス>：ネットワークパケットルールのリスト中のルールの現在の番号。

--at <インデックス>：ネットワークパケットルールのリスト中のルールの新しい番号。

kesl-control --add-zone

このコマンドは、ネットワークゾーンにアドレスを追加します。

コマンド構文

```
kesl-control [-F] --add-zone --zone <ゾーン> --address <アドレス>
```

引数とキー

`--zone <zone>` は、ネットワークゾーンの事前定義済みの名前です。

`--address <address>` はネットワークアドレスまたはサブネットです。

kesl-control --del-zone

このコマンドは、ネットワークゾーンからアドレスを削除します。

コマンド構文

```
kesl-control [-F] --del-zone --zone <ゾーン> --address <アドレス>
```

```
kesl-control [-F] --del-zone --zone <ゾーン> --index <アドレスインデックス>
```

引数とキー

`--zone <zone>` は、ネットワークゾーンの事前定義済みの名前です。

`--address <address>` はネットワークアドレスまたはサブネットです。

`--index <アドレスインデックス>`：ネットワークゾーン内のアドレスの番号。

kesl-control -F --query

このコマンドは、Kaspersky Endpoint Security で作成されたファイアウォールルールを表示します。

コマンド構文

```
kesl-control -F --query
```

ブロックされたデバイスの管理に使用されるコマンド

「-H」は、アンチクリプターおよびネットワーク脅威対策によってブロックされたデバイスを管理するためのコマンドのグループに属することを示す接頭辞です。

The kesl-control --get-blocked-hosts コマンド

このコマンドを使用すると、ブロックされるデバイスのリストをコンソールに出力できます。

コマンド構文

```
kesl-control [-H] --get-blocked-hosts
```

kesl-control --allow-hosts コマンド

このコマンドを使用すると、ブロックされるデバイスのブロックを解除できます。

コマンド構文

```
kesl-control [-H] --allow-hosts <アドレス>
```

引数とキー

< address > は、デバイスまたはサブネットの IP アドレス（IPv4 / IPv6、短縮形式のアドレスを含む）です。デバイスまたはサブネットの IP アドレスをスペースで区切って複数指定できます。

デバイスコントロールを管理するコマンド

-D は、デバイスコントロールを管理するコマンドのグループに、そのコマンドが属することを示す接頭辞です。

kesl-control --get-device-list

このコマンドは、クライアントデバイスにインストールされているデバイス、またはクライアントデバイスに接続されているデバイスのリストをコンソールに出力します。

コマンド構文

```
kesl-control [-D] --get-device-list [--json]
```

引数とキー

--json：データを JSON 形式で出力します。

アプリケーションコントロールを管理するコマンド

-A は、アプリケーションコントロールを管理するコマンドのグループに、そのコマンドが属することを示す接頭辞です。

kesl-control --get-app-list

このコマンドは、インベントリタスクによってクライアントデバイス上で見つかったアプリケーションのリストを出力します。

コマンド構文

```
kesl-control [-A] --get-app-list [--json]
```

引数とキー

--json：データを JSON 形式で出力します。

kesl-control --get-categories

このコマンドは、作成されたアプリケーションコントロールのカテゴリリストを出力します。

コマンド構文

`kesl-control [-A] --get-categories [--names <カテゴリ 1 の名前> <カテゴリ 2 の名前> ... <カテゴリ N の名前>] --file <設定情報ファイルへのパス> [--json]`

引数とキー

`<カテゴリ 1 の名前> <カテゴリ 2 の名前> ... <カテゴリ N の名前>` – 情報を表示するカテゴリの名前。複数のカテゴリに関する情報を表示する場合は、カテゴリ名をスペースで区切って指定します。

`--file <設定情報ファイルのパス>` – 設定が出力される JSON 構成ファイルへの絶対パス。

`--json`：データを JSON 形式で出力します。

kesl-control --set-categories

このコマンドを使用すると、作成されたアプリケーションコントロールカテゴリのリストを作成または編集できます。

コマンド構文

`kesl-control [-A] --set-categories [--names <カテゴリ 1 の名前> <カテゴリ 2 の名前> ... <カテゴリ N の名前>] --file <設定情報ファイルへのパス>`

引数とキー

`<カテゴリ 1 の名前> <カテゴリ 2 の名前> ... <カテゴリ N の名前>` – 情報を変更するカテゴリの名前複数のカテゴリに関する情報を変更する場合は、カテゴリ名をスペースで区切って指定します。カテゴリ名を指定しないと、カテゴリはリストから削除されます。

`--file <設定情報ファイルへのパス>` – カテゴリ設定が含まれる設定情報ファイルへの絶対パスです。

kesl-control --get-settings 21

このコマンドは、作成されたアプリケーションコントロールのルールリストを出力します。

コマンド構文

`kesl-control --get-settings 21 --file <設定情報ファイルのパス> [--json]`

引数とキー

`--file <設定情報ファイルのパス>` – 設定がエクスポートされる設定情報ファイルへの絶対パス。

`--json`：データを JSON 形式で出力します。

kesl-control --set-settings 21

このコマンドを使用すると、作成されたアプリケーションカテゴリとアプリケーションコントロールのルールリストを編集できます。

コマンド構文

```
kesl-control --set-settings 21 [--file <設定情報ファイルのパス>] [--json]
```

引数とキー

`--file <設定情報ファイルのパス>` – 設定がインポートされる設定情報ファイルへの絶対パス。

`--json` – JSON ファイルからデータをインポートします。

kesl-control --set-to-default 21

このコマンドを使用すると、アプリケーションカテゴリとアプリケーションコントロールルールのリストを削除できます。

コマンド構文

```
kesl-control --set-settings 21 --set-to-default
```

ウェブコントロール管理コマンド

kesl-control --get-settings 26

このコマンドを使用すると、指定されたウェブコントロール設定のリストを表示できます。

コマンド構文

```
kesl-control --get-settings 26 --file <設定情報ファイルのパス> [--json]
```

引数とキー

`--file <設定情報ファイルのパス>` – 設定がエクスポートされる設定情報ファイルへの絶対パス。

`--json`：データを JSON 形式で出力します。

kesl-control --set-settings 26

このコマンドを使用すると、指定されたウェブコントロール設定のリストを編集できます。

コマンド構文

```
kesl-control --set-settings 26 [--file <設定情報ファイルのパス>] [--json]
```

引数とキー

`--file <設定情報ファイルのパス>` – 設定がインポートされる設定情報ファイルへの絶対パス。

`--json` – JSON ファイルからデータをインポートします。

kesl-control --set-to-default 26

このコマンドを使用すると、指定された設定を削除し、ウェブコントロール設定を既定のルールにリセットできます。

コマンド構文

```
kesl-control --set-settings 26 --set-to-default
```

バックアップを管理するコマンド

「-B」は、バックアップ保管領域の管理に使用されるコマンドのグループに、そのコマンドが属することを示す接頭辞です。

kesl-control --mass-remove

このコマンドは、バックアップから一部または全部のオブジェクトを削除します。

コマンド構文

すべてのオブジェクトを削除します：

```
kesl-control [-B] --mass-remove
```

フィルター条件に一致するオブジェクトを削除します：

```
kesl-control [-B] --mass-remove --query "<フィルター条件>"
```

引数とキー

<フィルター条件>：<フィールド> <比較演算子> '<値>' 形式の1つまたは複数の論理式。論理演算子と組み合わせて、結果を限定します。

kesl-control -B --query

このコマンドは、バックアップオブジェクトに関する情報を出力します。

コマンド構文

バックアップ内のすべてのオブジェクトに関する情報を出力します：

```
kesl-control -B --query [-n <数値>] [--json] [--reverse]
```

フィルター条件に一致するバックアップオブジェクトに関する情報を出力します。

```
kesl-control -B --query ["<フィルター条件>"] [-n <数値>] [--json] [--reverse]
```

引数とキー

<フィルター条件>：<フィールド> <比較演算子> '<値>' 形式の1つまたは複数の論理式。論理演算子と組み合わせて、結果を限定します。 フィルター条件を指定しない場合、バックアップ内のすべてのオブジェクトの詳細を表示します。

<数値>：表示する最新のオブジェクトの数。 -n スイッチを指定しない場合は、最後の 30 個のオブジェクトが表示されます。0 を指定してすべてのオブジェクトを表示します。

--json：データを JSON 形式で出力します。

kesl-control --restore

このコマンドは、バックアップからオブジェクトを復元します。

コマンド構文

```
kesl-control [-B] --restore <オブジェクト ID> [--file <ファイル名とパス>]
```

引数とキー

<オブジェクト ID>：バックアップ オブジェクトの ID。

--file <ファイル名とパス>：ファイルの新しい名前と、ファイルを保存するディレクトリへのパスです。 --file オプションを指定しない場合、オブジェクトは元の名前と元の場所に復元されます。

ユーザーとロールを管理するためのコマンド

「-U」は、ユーザーとロールを管理するためのコマンドのグループに、そのコマンドが属することを示す接頭辞です。

kesl-control --get-user-list

このコマンドは、ユーザートロールのリストを出力します。

コマンド構文

```
kesl-control [-U] --get-user-list
```

kesl-control --grant-role

このコマンドは、特定のユーザーにロールを割り当てます。

コマンド構文

```
kesl-control [-U] --grant-role <ロール> <ユーザー>
```

kesl-control --revoke-role

このコマンドは、特定のユーザーのロールを取り消します。

コマンド構文

```
kesl-control [-U] --revoke-role <ロール> <ユーザー>
```

Kaspersky Managed Detection and Response（KATA）との連携の設定を管理するためのコマンド

-R は、コマンドが Kaspersky Endpoint Detection and Response (KATA) および Kaspersky Endpoint Detection and Response Optimum との連携の設定を管理するためのコマンドグループに属していることを示す接頭辞です。

kesl-control --add-kataedr-server-certificate

このコマンドは、以前に追加された KATA サーバー証明書を追加または置換します。

コマンド構文

```
kesl-control [-R] --add-kataedr-server-certificate <ファイル名とパス>
```

引数とキー

<ファイル名とパス>は、サーバー証明書を含むファイルの名前とパスです。

kesl-control --remove-kataedr-server-certificate

このコマンドは、KATA サーバー証明書を削除します。

コマンド構文

```
kesl-control [-R] --remove-kataedr-server-certificate
```

kesl-control --query-kataedr-server-certificate

このコマンドは、KATA サーバー証明書に関する情報を出力します。

コマンド構文

```
kesl-control [-R] --query-kataedr-server-certificate
```

kesl-control --add-kataedr-client-certificate

このコマンドは、KATA サーバーへの接続を保護するために使用される、以前に追加されたクライアント証明書を追加または置換します。

コマンド構文

```
kesl-control [-R] --add-kataedr-client-certificate <ファイル名とパス>
```

引数とキー

<ファイル名とパス>は、クライアント証明書と秘密鍵を含む暗号コンテナ（PFX アーカイブ）の名前とパスです。

kesl-control --remove-kataedr-client-certificate

このコマンドは、KATA サーバーへの接続を保護するために使用されるクライアント証明書を削除します。

コマンド構文

```
kesl-control [-R] --remove-kataedr-client-certificate
```

kesl-control --query-kataedr-client-certificate

このコマンドは、クライアント証明書に関する情報を出力します。

コマンド構文

```
kesl-control [-R] --query-kataedr-client-certificate
```

kesl-control --isolation-stat

このコマンドは、ネットワーク分離の現在の状態をコンソールに出力します。

コマンド構文

```
kesl-control [-R] --isolation-stat
```

kesl-control --isolation-off

このコマンドを使用すると、デバイスのネットワーク分離を無効にすることができます。

コマンド構文

```
kesl-control [-R] --isolation-off
```

Kaspersky Managed Detection and Response Optimum との連携の設定を管理するためのコマンド

-R は、コマンドが Kaspersky Endpoint Detection and Response (KATA) および Kaspersky Endpoint Detection and Response Optimum との連携の設定を管理するためのコマンドグループに属していることを示す接頭辞です。

製品の全般設定の `UseEdrOptimum` 設定を使用して、Kaspersky Endpoint Detection and Response Optimum との連携を有効または無効にできます。

kesl-control --isolation-stat

このコマンドは、ネットワーク分離の現在の状態をコンソールに出力します。

コマンド構文

```
kesl-control [-R] --isolation-stat
```

kesl-control --isolation-off

このコマンドを使用すると、デバイスのネットワーク分離を無効にすることができます。

コマンド構文

```
kesl-control [-R] --isolation-off
```

仮想環境を保護する Light Agent モードでのアプリケーションコマンド

-V：仮想環境を保護するために Light Agent モードで使用される Kaspersky Endpoint Security のコマンドグループに属することを示す接頭辞（Kaspersky Security for Virtualization Light Agent の一部）。

これらのコマンドは、Kaspersky Endpoint Security を Light Agent モードで使用して仮想環境を保護する場合にのみ実行できます。

kesl-control --ksvla-info

このコマンドは、仮想環境を保護する Light Agent モードでの本製品の使用に関する情報を出力します：

コマンド構文

```
kesl-control --ksvla-info
```

kesl-control --viis-info

このコマンドは、Light Agent（Kaspersky Security for Virtualization Light Agent の一部として Light Agent として使用される Kaspersky Endpoint Security アプリケーション）と Integration Server の接続に関する情報を出力します：

コマンド構文

```
kesl-control --viis-info
```

kesl-control --svm-info

このコマンドは、Light Agent（Kaspersky Security for Virtualization Light Agent の一部として Light Agent として使用される Kaspersky Endpoint Security アプリケーション）と SVM の接続に関する情報を出力します：

コマンド構文

```
kesl-control --svm-info
```

付録 3：設定情報ファイルと既定のアプリケーション設定

Kaspersky Endpoint Security の管理には、次の設定ファイルが使用されます：

- 本製品の初期設定を含む設定情報ファイル：
  - autoinstall.ini 設定情報ファイルは、Kaspersky Security Center 経由で本製品をインストールするときに使用されます。
  - コマンドライン経由でアプリケーションをインストールするときに使用される設定情報ファイル。
- 本製品の初期設定中に自動的に生成され、初期設定中に設定されたオプションを含むプリセット設定情報ファイル。これらの設定は実行時に適用されます。
- Kaspersky Endpoint Security 管理コマンドを使用して作成できる設定情報ファイル。これらの設定情報ファイルには、タスク設定などのアプリケーション設定が含まれることがあります。これらのファイルを変更し、本製品にインポートして、対応するオプションを変更できます。

製品タスクの設定情報ファイルの編集ルール

設定情報ファイルを編集する場合は、次のルールを順守してください：

- 設定情報ファイル内の設定必須の項目はすべて指定します。コマンドラインを使用して、個別のタスクの設定をファイルなしで指定できます。
- 設定が特定のセクションに属している場合は、そのセクションのみに指定されます。1つのセクション内で任意の順序で設定を指定できます。
- セクションの名前は角括弧（[ ]）で囲みます。
- < 設定名 >=< 設定値 > の形式で設定値を入力します（設定名とその値の間のスペースは処理されません）。

  例：
  ```
  [ScanScope.item_0000]
  AreaDesc=Home
  AreaMask.item_0000=*doc
  Path=/home
  ```

  空白文字とタブ文字は、文字列値の最初の引用符の前と最後の引用符の後、および引用符で囲まれていない文字列値の最初と最後は無視されます。
- 設定に対していくつかの値を指定する必要がある場合は、指定する値の数と同じ数だけ設定を繰り返します。

  例：
  ```
  AreaMask.item_0000=*xml
  AreaMask.item_0001=*doc
  ```
- 次の種別の設定の値を入力する時は、大文字と小文字を区別します：
  - スキャン済みのオブジェクトと除外されるオブジェクトの名前（マスク）。

- 脅威の名前（マスク）。

残りの設定値は大文字と小文字が区別されません。

- ブール型の設定値は、`Yes / No` のように指定します。
- 空白文字を含む文字列値は引用符で囲みます（例：ファイル名、ディレクトリ名、パス名、YYYY-MM-DD HH:MM:SS 形式の日時を含む表現など）。
  それ以外の値は、引用符の有無に関係なく入力できます。

```
例：
AreaDesc="Scanning of email databases"
```

文字列の最初または最後の一重引用符は、エラーと認識されます。

プレセットの設定情報ファイル

初期設定の後、次の設定情報ファイルが作成されます：

- /var/opt/kaspersky/kesl/common/agreements.ini
  設定情報ファイル agreements.ini には、使用許諾契約書、プライバシーポリシー、および Kaspersky Security Network に関する声明に関連する設定が含まれています。
- /var/opt/kaspersky/kesl/common/kesl.ini
  設定情報ファイル kesl.ini で設定可能な項目について、以下の表で説明します。

必要に応じて、これらのファイルの設定値を編集できます。

これらのファイルの既定値を変更する場合は、テクニカルサポートの指示に従って行ってください。

設定情報ファイル kesl.ini の設定項目

設定	説明	値
[General] セクションには、次の設定が含まれています：		
`Locale`	Kaspersky Endpoint Security から Kaspersky Security Center に送信されるテキスト（イベント、通知、タスク結果など）のローカライズに使用されるロケールです。 グラフィカルインターフェイスとコマンドラインのロケールは、`LANG` 環境変数の値によって異なります。Kaspersky Endpoint Security でサポートされていないロケールが `LANG` 環境変数の値として指定されている場合、グラフィカルインターフェイスとコマンドラインは英語で表示されます。	RFC 3066 で指定されてい `Locale` 設定が指定されてィングシステムのローカリされます。製品がオペレーカリゼーション言語を判またはオペレーティングシションがサポートされてい`en_US.utf8` が使用されま
`PackageType`	インストールされた製品パッケージの	`rpm` – RPM パッケージがイ

	形式。 この設定はアプリケーションの動作には影響しません。設定の値は、アプリケーションの初期設定中に自動的に入力されます。	deb – DEB パッケージがイ
UseFanotify	fanotify 通知の使用を指定します。 この設定はアプリケーションの動作には影響しません。設定の値は、アプリケーションの初期設定中に自動的に入力されます。	true/yes – オペレーティ通知をサポートします。 false/no – オペレーティ通知をサポートしません。
KsvlaMode	Kaspersky Endpoint Security の使用モード。 この設定はアプリケーションの動作には影響しません。設定の値は、アプリケーションの初期設定中に自動的に入力されます。	true/yes – アプリケーシ Light Agent モードで使用さ false/no – アプリケーシされます。
StartupTraces	製品起動時の、トレースファイルの生成を指定します。	true/yes – アプリケーシファイルを生成します。 false/no（既定値）– 本製ファイルを生成しません。
RevealSensitiveInfoInTraces	個人情報が含まれる可能性のあるトレースファイルの情報（パスワードなど）を表示します。	true/yes（既定値）– アファイル内の、個人情報が情報を表示します。 false/no（既定値）– ト人情報が含まれる可能性のん。
AsyncTraces	非同期トレースを有効にします。非同期トレースでは、情報がトレースファイルに非同期的に記録されます。	true/yes – 非同期トレー false/no（デフォルト値）効にしません。
CoreDumps	本製品の障害発生時の、ダンプファイルの作成を指定します。	true/yes（既定値）– アプ生時に、ダンプファイルを false/no（既定値）– アプ生時に、ダンプファイルを
CoreDumpsPath	ダンプファイルが保存されているディレクトリへのパス。	既定値：/var/opt/kaspersky/ke 既定のダンプファイルのデするには、root 権限が必要
MinFreeDiskSpace	ダンプファイルの書き込み後に残るディスクメモリの最小量（メガバイト単位）。	既定値：300
ScanMemoryLimit	製品のメモリ使用量を制限します（メガバイト単位）。	既定値：8192
MachineId	ユーザーの一意のデバイス ID。	設定の値は、アプリケーシに自動的に入力されます。
SocketPath	たとえば、グラフィカルインターフェイスや kesl-control ユーティリティへのリモート接続用のソケットへのパス。	既定値：/var/run/bl4contr

`MaxInotifyWatches`	/proc/sys/fs/inotify/max_user_watches でファイルやディレクトリの変更に対するサブスクリプション数（ユーザーウォッチ）を制限します。	既定値：300000
`MaxInotifyInstances`	1人のユーザーのファイルやディレクトリの変更に対するサブスクリプション数を制限します。	既定値：2048
`ExecEnvMax`	command call から取得する環境変数の数。	既定値：50
`ExecArgMax`	exec call から取得する引数の数。	既定値：50
`DisableFileAvActions`	インストール後のアプリケーションコンポーネントの駆除およびファイル削除機能を無効にします。 駆除およびファイル削除機能が無効で、脅威が検出された場合、アプリケーションは、脅威が検出されたファイルの駆除または削除を試みず、脅威の検出についてユーザに通知するだけです。	`true / yes`：インストー 起動時に、駆除機能とファ します。 `false / no`（既定値）： ケーション起動時に、駆除 能を無効にしません。
`AdditionalDNSLookup`	パブリック DNS の使用を指定します。 システム DNS を使用してサーバーにアクセスする際にエラーが発生した場合は、パブリック DNS が使用されます。これは、定義データベースをアップデートし、デバイスのセキュリティを維持するために必要です。本製品では、以下のパブリック DNS がこの順番で使用されます： • Google Public DNS™（8.8.8.8） • Cloudflare® DNS（1.1.1.1） • Alibaba Cloud® DNS（223.6.6.6） • Quad9® DNS（9.9.9.9） • CleanBrowsing（185.228.168.168）	`true/yes` – カスペルスキ スに、パブリック DNS を使 `false/no`（既定値）– カス へのアクセスに、パブリッ ん。 本製品は DNS サーバーと 確立するため、要求には ユーザーの外部 IP アドレ あります。たとえば、HT Web リソースの証明書を の情報が必要になります ーバーが使用されている ールは、対応するサービ リシーによって管理され DNS サーバーの使用をブ る場合は、テクニカルサ ライベートパッチを取得
[Network] セクションには、次の設定が含まれています：		
`WtpFwMark`	ウェブ脅威対策コンポーネントによる処理のために本製品に転送されるトラフィックの iptables ルール内のマーク。本製品がインストールされたデバイスで、TCP パケットマスクの 9 番目のビットを使用する他のソフトウェアが実行され、競合が発生した場合は、このマークを変更する必要があります。	10 進数の値または先頭に 0 既定値：0x100。
`NtpFwMark`	ネットワーク脅威対策コンポーネントによる処理のためにアプリケーションに転送されるトラフィックの iptables ルール内のマーク。	10 進数の値または先頭に 0 既定値：0x200。

	本製品がインストールされたデバイスで、TCP パケットマスクの 9 番目のビットを使用する他のソフトウェアが実行され、競合が発生した場合は、このマークを変更する必要があります。	
`BypassFwMark`	パケットが再度スキャンされないように、本製品によって作成またはスキャンされたパケットを指定するために使用されるマーク。	10 進数の値または先頭に 0 既定値：0x400。
`BypassNFlogMark`	Iptable ユーティリティによってログに記録されないように、アプリケーションによって作成またはスキャンされたパッケージを示すために使用されるマークです。	10 進数の値または先頭に 0 既定値：0x800。
`ProxyRouteTable`	ルーティングテーブルの番号。	既定値：101
［**Virtualization**］セクションには、次の設定が含まれています：		
`ServerMode`	Kaspersky Endpoint Security が仮想環境を保護するために Light Agent モードで使用される場合の、保護対象仮想マシンのロール：server または workstation。 この設定はアプリケーションの動作には影響しません。設定の値は、アプリケーションの初期設定中に自動的に入力されます。	`true/yes` – 保護対象仮想 使用されます。 `false/no` – 保護対象仮想 ョンとして使用されます。
`VdiMode`	アプリケーションを仮想環境保護用 Light Agent モードで使用して場合、VDI 保護モードを有効にします。 この設定はアプリケーションの動作には影響しません。設定の値は、アプリケーションの初期設定中に自動的に入力されます。	`true/yes` – VDI 保護モー す。 `false/no` – VDI 保護モー
[Watchdog] セクションには、次の設定が含まれています：		
`TimeoutAfterHeadshot`	Watchdog サーバーが kesl プロセスに HEADSHOT シグナルを送信してから、kesl プロセスが完了するまでに待機する最大時間。	既定値：2 分。
`StartupTimeout`	本製品の起動を待機する最大時間（分単位）。この時間が経過すると、kesl プロセスが再起動されます。	既定値：3 分。
`TimeoutAfterKill`	Watchdog サーバーが kesl プロセスに SIGKILL シグナルを送信してから、制御対象 kesl プロセスが完了するまでに待機する最大時間。 この時間が経過する前に kesl プロセスが終了しない場合、--failed-kill 設定で指定された処理が実行されます。	既定値：2 日。
`PingInterval`	受信した PING メッセージに応答して、PONG メッセージのサーバーへの送信を試行する時間。	既定値：2000 ミリ秒
`MaxRestartCount`	本製品の起動を連続して失敗する最大	既定値：5

	回数。	
ActivityTimeout	Watchdog サーバーにメッセージを送信する最大時間。 この時間内に本製品からメッセージが受信されない場合、Watchdog サーバーは kesl プロセスを終了する手順を開始します。	既定値：2 分。
ConnectTimeout	kesl プロセスの開始から、Watchdog サーバーとの接続が確立されるまでの最大時間。 この時間内に本製品が接続を確立しない場合、Watchdog サーバーは kesl プロセスを終了する手順を開始します。	既定値：3 分。
RegisterTimeout	本製品が Watchdog サーバーに接続してから、サーバーが REGISTER メッセージを受信するまでの最大時間。	既定値：500 ミリ秒
TimeoutAfterShutdown	Watchdog サーバーが kesl プロセスに SHUTDOWN シグナルを送信してから、kesl プロセスが完了するまでに待機する最大時間。	既定値：2 分。
MaxMemory	kesl プロセスによる常駐メモリの使用を制限します。 kesl プロセスがこの制限を超える常駐メモリを使用する場合、Watchdog サーバーは kesl プロセスを終了する手順を開始します。	off – 常駐設定のサイズは < value >% – メモリのパー 100）。 < value >MB – メガバイト単 lowest/< value >%/< valu で表した値とメガバイトで の値。l highest/< 値 >%/< 値 >MB た値とメガバイトで表した auto – 仕様可能なメモリの GB 以上 16 GB 以下。 既定値：auto
MaxVirtualMemory	kesl プロセスによる仮想メモリの使用を制限します。 kesl プロセスがこの制限を超える仮想メモリを使用する場合、Watchdog サーバーは kesl プロセスを終了する手順を開始します。	off（既定値） – 仮想メモ せん。 < value >MB – メガバイト単
MaxSwapMemory	kesl プロセスのスワップファイルのサイズを制限します。 kesl プロセスのスワップファイルがこの制限を超えると、Watchdog サーバーは kesl プロセスを終了する手順を開始します。	off（既定値） – スワップ 限されません。 < value >% – メモリのパー 100）。 < value >MB – メガバイト単 lowest/< value >%/< valu で表した値とメガバイトで の値。l highest/< 値 >%/< 値 >MB た値とメガバイトで表した
TrackProductCrashes	本製品の安定性監視の有効化。	true/yes – アプリケーシ

	本製品の安定性監視が有効になっている場合、Watchdog サーバーは本製品の異常停止の数を追跡します。	にします。 `false/no`（デフォルト値）を無効にします。
`ProductHealthLogFile`	本製品の安定性の監視に使用されるファイルへのパス。	既定値：/var/opt/kaspersky/ke
`WarnThreshold`	不安定な動作に関する通知を表示する前に、本製品が指定された回数の異常停止を経験する必要がある時間間隔（秒単位）。	既定値：3600 秒
`WarnAfter_#_crash`	不安定な製品動作に関する通知を表示する前に必要な本製品の異常停止回数。	既定値：10 値が 0 の場合、不安定な製せん。
`WarnRemovingThreshold`	本製品の不安定な状態がクリアされるまでの時間間隔（秒単位）。	既定値：86400 秒。
既定では、［**環境**］セクションは設定情報ファイルに存在しません。		
`ExperimentalContainerdSupport`	コンテナ監視コンポーネントを実行するときに、containerd 環境のサポートを有効にします。 既定では、このセクションは設定情報ファイルに存在しません。コンテナ監視コンポーネントの実行中に containerd 環境を使用する場合は、設定情報ファイルとその中に［環境］セクションと `ExperimentalContainerdSupport` 設定を手動で追加する必要があります。	`true/yes` – コンテナ監視 containerd 環境への対応を `false/no` – コンテナ監視 containerd 環境への対応を

既定のコマンドラインタスク設定

このセクションには、コマンドライン経由で Kaspersky Endpoint Security を管理するために提供されるすべての事前定義済みタスクの既定オプションが含まれています。

*ロールバック*と *ライセンス*のタスクには設定がありません。

File_Threat_Protection タスク（ID:1）の既定

```
ScanArchived=No

ScanSfxArchived=No

ScanMailBases=No

ScanPlainMail=No

SkipPlainTextFiles=No
```

```
TimeLimit=60

SizeLimit=0

FirstAction=Recommended

SecondAction=Block

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanByAccessType=SmartCheck

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Scan_My_Computer タスク（ID:2）の既定

```
ScanFiles=Yes

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No
```

```
TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Scan_File タスク（ID:3）の既定

```
ScanFiles=Yes

ScanBootSectors=No

ScanComputerMemory=No

ScanStartupObjects=No

ScanArchived=Yes

ScanSfxArchived=Yes
```

```
ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Critical_Areas_Scan タスク（ID:4）の既定

```
ScanFiles=No

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes
```

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Update タスク（ID:6）の既定

```
SourceType="KLServers"

UseKLServersWhenUnavailable=Yes
```

```
ApplicationUpdateMode=DownloadOnly

ConnectionTimeout=10
```

Backup タスク（ID:10）の既定

```
DaysToLive=90

BackupSizeLimit=0

BackupFolder=/var/opt/kaspersky/kesl/common/objects-backup/
```

System_Integrity_Monitoring タスク（ID:11）の既定

```
UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=Kaspersky internal objects

UseScanArea=Yes

Path=/opt/kaspersky/kesl/

AreaMask.item_0000=*
```

Firewall_Management タスク（ID:12）の既定

```
DefaultIncomingAction=Allow

DefaultIncomingPacketAction=Allow

OpenNagentPorts=Yes

[NetworkZonesTrusted]

[NetworkZonesLocal]

[NetworkZonesPublic]
```

Anti_Cryptor タスク（ID:13）の既定

```
ActionOnDetect=Block

BlockTime=30

UseExcludeMasks=No

[ScanScope.item_0000]
```

```
AreaDesc=All shared directories

UseScanArea=Yes

Path=AllShared

AreaMask.item_0000=*
```

Web_Threat_Protection タスク（ID:14）の既定

```
UseTrustedAddresses=Yes

ActionOnDetect=Block

CheckMalicious=Yes

CheckPhishing=Yes

UseHeuristicForPhishing=Yes

CheckAdware=No

CheckOther=No
```

Device_Control タスク（ID:15）の既定

```
OperationMode=Block

[DeviceClass]

HardDrive=DependsOnBus

RemovableDrive=DependsOnBus

Printer=DependsOnBus

FloppyDrive=DependsOnBus

OpticalDrive=DependsOnBus

Modem=DependsOnBus

TapeDrive=DependsOnBus

MultifuncDevice=DependsOnBus

SmartCardReader=DependsOnBus

PortableDevice=DependsOnBus

WiFiAdapter=DependsOnBus
```

```
NetworkAdapter=DependsOnBus

BluetoothDevice=DependsOnBus

ImagingDevice=DependsOnBus

SerialPortDevice=DependsOnBus

ParallelPortDevice=DependsOnBus

InputDevice=DependsOnBus

SoundAdapter=DependsOnBus

[DeviceBus]

USB=Allow

FireWire=Allow

[Schedules.item_0000]

ScheduleName=Default

DaysHours=All

[HardDrivePrincipals.item_0000]

Principal=\Everyone

[HardDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[RemovableDrivePrincipals.item_0000]

Principal=\Everyone

[RemovableDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[FloppyDrivePrincipals.item_0000]

Principal=\Everyone

[FloppyDrivePrincipals.item_0000.AccessRules.item_0000]
```

```
UseRule=Yes

ScheduleName=Default

Access=Allow

[OpticalDrivePrincipals.item_0000]

Principal=\Everyone

[OpticalDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow
```

Removable_Drives_Scan タスク（ID:16）の既定

```
ScanRemovableDrives=NoScan

ScanOpticalDrives=NoScan

BlockDuringScan=No
```

Network_Threat_Protection タスク（ID:17）の既定

```
ActionOnDetect=Block

BlockAttackingHosts=Yes

BlockDurationMinutes=60

UseExcludeIPs=No
```

Container_Scan（ID:18）と Custom_Container_Scan（ID:19）タスクの既定

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0
```

```
FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanContainers=Yes

ContainerNameMask=*

ScanImages=Yes

ImageNameMask=*

DeepScan=No

ContainerScanAction=StopContainerIfFailed

ImageAction=Skip

UseGlobalExclusions=Yes
```

この設定情報ファイルのオプションは、カスタムコンテナースキャンタスクにも使用できます。

Behavior_Detection タスク（ID:20）の既定

```
UseTrustedPrograms=No

TaskMode=Block
```

Application_Control タスク（ID:21）の既定

```
AppControlMode=DenyList

AppControlRulesAction=ApplyRules
```

Inventory_Scan タスク（ID:22）の既定

```
ScanScripts=Yes

ScanBinaries=Yes

ScanAllExecutable=Yes

CreateGoldenImage=No

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/usr/bin

AreaMask.item_0000=*
```

KATAEDR タスク（ID:24）の既定

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=

Port=443

[EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

Web_Control タスク（ID:26）の既定

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

全般的な製品設定

アプリケーションの全般設定で、アプリケーション全体の動作や個々の機能の動作を定義します。

全般的な製品設定

設定	説明	
SambaConfigPath	Samba 設定情報ファイルを格納するディレクトリ。AllShared または Shared:SMB の値を Path オプションに使用できるようにするには、Samba 設定情報ファイルが必要です。	既定では、コンピュータイルの標準ディレクトリ 既定値：/etc/samba/smb この設定の変更後は、製す。
NfsExportPath	NFS 設定情報ファイルが格納されているディレクトリ。AllShared または Shared:NFS の値を Path 設定に使用できるようにするには、NFS 設定情報ファイルが必要です。	既定では、コンピュータルの標準ディレクトリが 既定値：/etc/exports この設定の変更後は、製す。
TraceLevel	本製品のトレースとトレースファイルの詳細レベルを有効にします。	Detailed - 詳細なトレー MediumDetailed - 情報ジを含むトレースファイ NotDetailed - エラーメイルを生成します。 None（既定値） - トレーん。
TraceFolder	本製品のトレースファイルを格納するディレクトリ。	既定値：/var/log/kaspers 別のディレクトリを指定Endpoint Security を実行ディレクトリに対して読ていることを確認します。ディレクトリにアクセスす。 この設定の変更後は、製す。
TraceMaxFileCount	本製品のトレースファイルの最大数。	1 - 10000 既定値：10 この設定の変更後は、製す。
TraceMaxFileSize	トレースファイルの最大サイズを指定します（メガバイト単位）。	1 - 1000 既定値：500 この設定の変更後は、製す。
BlockFilesGreaterMaxFileNamePath	絶対パスの長さがバイト単位で指定された設定の定義値を超えているファイルへのアクセスをブロッ	4096 - 33554432 既定値：16384

	クします。スキャン対象のファイルの完全パスの長さがこの設定の値を超えると、スキャンタスクのスキャン中にそのファイルはスキップされます。 この設定は、fanotify テクノロジーを使用しているオペレーティングシステムでは使用できません。	この設定の値を変更した を再起動する必要があり
DetectOtherObjects	侵入者がデバイスやデータを侵害するために使用できる正規のアプリケーションの検出を有効にします。	Yes：侵入者がデバイス 用できる正規のアプリケ す。 No（既定）：侵入者がデ ために使用できる正規の 効にします。
NamespaceMonitoring	名前空間とコンテナースキャンを有効にします。 コンテナと名前空間を操作するためのコンポーネントがオペレーティングシステムにインストールされていない限り、アプリケーションは名前空間とコンテナーをスキャンしません。	Yes（既定値）- 名前空間 効にします。 No - 名前空間とコンテナ す。
FileBlockDuringScan	スキャン中はファイルへのアクセスをブロックするファイル操作遮断モードを有効にします。ファイル操作遮断モードは、ファイル脅威対策およびデバイスコントロールコンポーネントに影響します。	はい（既定値）を選択す ルへのアクセスがブロッ スキャン中にファイルに を選択します。すべての 可し、スキャンは非同期 操作遮断モードはシステ 響は少ないですが、本製 る前に、たとえばスキャ された場合、ファイル内 ないリスクがあります。
UseKSN	Kaspersky Security Network の使用を有効にするには：	標準 - 標準モードで Kasp 用を有効にします。 拡張 - 拡張モードで Kasp 用を有効にします。 No（既定値）- Kaspersky 無効にします。
CloudMode	クラウドモードを有効にします。KSN の使用が有効になっている場合、クラウドモードを使用できます。 クラウドモードを使用する予定がある場合は、デバイスで KSN が使用可能であることを確認してください。	Yes — Kaspersky Endpoin タベースの軽量バージョ 効にします。 No（既定値）– マルウェ ョンを使用します。 KSN の使用が無効にな ードは自動的に無効に

	この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。	
UseMDR	Kaspersky Managed Detection and Responseとの連携のために Managed Detection and Response コンポーネントを有効にします。	Managed Detection and R 効にするには、 はいを選 No（既定値）- Managed 効にします。
UseProxy	Kaspersky Endpoint Security コンポーネントによるプロキシサーバーの使用を有効にします。Kaspersky Security Network および Kaspersky Endpoint Detection and Response（KATA）との通信、本製品のアクティベーション、および定義データベースとモジュールのアップデート時に、プロキシサーバーを使用できます。 Kaspersky Endpoint Security を仮想環境保護用 Light Agent モードで使用する場合、Kaspersky Security Network、SVM、および Integration Server との接続にプロキシサーバーを使用することはサポートされません。	Yes – プロキシサーバー No（既定値） - プロキシ ます。 Yes を選択すると、Kasp Response（KATA）との通 で行われます。
ProxyServer	プロキシサーバーオプションの形式：[<ユーザー>[:<パスワード>]@]<プロキシサーバーアドレス>[:<ポート>]。 HTTP プロキシ経由で接続する場合は、他のシステムへのログインに使用しない別のアカウントを使用することを推奨します。HTTP プロキシがセキュアでない接続を使用しているため、アカウントが危険にさらされている可能性があります。	-
MaxEventsNumber	製品によって保存されるイベントの最大数。指定されたイベントの数を超えると、最も古いイベントから削除されます。	既定値：500000 0 を指定すると、イベン
LimitNumberOfScanFileTasks	権限のないユーザーがデバイスで同時に開始できるオブジェクトスキャンタスクの最大数。この設定	0 - 4294967295 既定値：0

	は、root 権限を持つユーザーが開始できるタスクの数を制限しません。	0 を指定すると、権限のスキャンタスクを開始で 製品のインストール時にルした場合、LimitNumb 既定値は 5 になります。
UseSyslog	イベントに関する情報の syslog への記録を指定します。 syslog にアクセスするには、root 権限が必要です。	Yes - イベントに関する情にします。 No（既定値） - イベント記録を無効にします。
EventsStoragePath	イベントに関する情報を保存するデータベースディレクトリ。 既定のイベントデータベースにアクセスするには、root 権限が必要です。	既定 値：/var/opt/kaspersky/k
ExcludedMountPoint.item_#	スキャン範囲から除外するマウントポイント。除外は、ファイル脅威対策、アンチクリプター、およびコンテナ監視コンポーネントの操作とリムーバブルドライブスキャンタスクに適用され、ODS および ContainerScan スキャンタスクの操作でも設定されます。 複数のマウントポイントを選択して、スキャンから除外することも可能です。 マウントポイントは、mount コマンドを実行して出力されるのと同じものを指定する必要があります。 既定では、ExcludedMountPoint.item_# 設定は指定されていません。	AllRemoteMounted — SM コルを使用してデバイスモートディレクトリをフから除外します。 Mounted:NFS — NFS プロにマウントされるすべてファイル操作のインターセ Mounted:SMB — SMB プロにマウントされるすべてファイル操作のインターセ Mounted:< ファイルシスイルシステム種別でマウトリをファイル操作のイす。 /mnt — /mnt マウントポを含む）内のオブジェク外します。このディレクブの一時的なマウントポ <「/mnt/user*」またはを含むパス>- 指定したマポイントのオブジェクトプトから除外します。

		アスタリスク記号「*」 またはディレクトリ名 ファイル名またはディ 前にある任意の文字数 含む）を表す「*」記号 きます。例：「/dir/* 「/dir/*/*/file」 2 つの連続する「*」記 ディレクトリ名におけ 文字数の文字列（0 文字 す。例：「/dir/**/f 「/dir/file**/」 アスタリスク記号を 2 つ いうマスク表現は、デ 用できます。たとえば、 は不適切なマスク表現 マウントポイント /dir （アスタリスク記号（* があります。 マスク /dir/* では、 すべてのマウントポイ が、/dir 自身は除外さ は、/dir よりも下の全 トポイントが除外され されません。 ファイル名またはディ 任意の文字（/ を含む）
MemScanExcludedProgramPath.item_#	プロセスメモリをスキャンから除外します。 指定されたプロセスのメモリはスキャンされません。	< プロセスへの絶対パス レクトリ内のプロセスは 指定にマスクを使用でき

		アスタリスク記号「*」 またはディレクトリ名 ファイル名またはディ 前にある任意の文字数 含む）を表す「*」記号 きます。例：「/dir/* 「/dir/*/*/file」 2 つの連続する「*」記 ディレクトリ名におけ 文字数の文字列（0 文字 す。例：「/dir/**/f 「/dir/file**/」 アスタリスク記号を 2 つ いうマスク表現は、デ 用できます。たとえば、 は不適切なマスク表現 ファイル名またはディ 使用して任意の文字を
UseOnDemandCPULimit	*ODS*、*ContainerScan*、および *InventoryScan* タイプのタスクの CPU 使用量制限を有効にします。	Yes：*ODS*、*ContainerSc* スクの CPU 使用量制限を No（既定）：タスクの C す。
OnDemandCPULimit	*ODS*、*ContainerScan*、および *InventoryScan* タイプのタスクを実行する時の、すべてのプロセッサコアにおける最大使用率（パーセンテージ）。	10～100 既定値：100
UseEdrOptimum	Kaspersky Endpoint Detection and Response Optimum との連携のために EDR Optimum コンポーネントを有効にします。	Yes – EDR Optimum コン す。 No（既定）– EDR Optimu します。

コンテナースキャンの全般設定

コンテナースキャンの全般設定は、ネームスペースとコンテナをリアルタイムでスキャンするときに使用されます。

コンテナと名前空間のスキャンの全般設定

設定	説明	値
OnAccessContainerScanAction	感染したオブジェクトの検知時に、コンテナに対して実行する処理。	StopContainerIfFailed（既定値） - 感染したオブジェクトの駆除や削除ができなかった場合、コンテナを停止します。

	この設定は、この機能をサポートするライセンスでアプリケーションを使用する場合に使用できます。 ファイル脅威対策タスクの設定は、コンテナ内のオブジェクトをスキャンするときに使用されます。感染したオブジェクトの検知時にコンテナで実行される処理は、ファイル脅威対策タスクの設定にも依存します（以下の表を参照）。	`StopContainer` - 感染したオブジェクトが検知された場合、コンテナを停止します。 `Skip` - 感染したオブジェクトが検知されても、コンテナに対して何の処理も実行しません。
`UseDocker`	Docker 環境の使用。	`Yes`（既定値） - Docker 環境を使用します。 `No` - Docker 環境を使用しません。
`DockerSocket`	Docker ソケットパスまたは URI（ユニバーサルリソース識別子）。	既定値：/var/run/docker.sock
`UseCrio`	CRI-O 環境の使用。	`Yes`（既定値） - CRI-O 環境を使用します。 `No` - CRI-O 環境を使用しません。
`CrioConfigFilePath`	CRI-O 設定情報ファイルへのパス。	既定値：/etc/crio/crio.conf
`UsePodman`	Podman ユーティリティの使用。	`Yes`（既定値） - Podman ユーティリティを使用します。 `No` - Podman ユーティリティを使用しません。
`PodmanBinaryPath`	Podman ユーティリティの実行ファイルへのパス。	既定値：/usr/bin/podman
`PodmanRootFolder`	コンテナの保管領域のルートディレクトリへのパス。	既定値：/var/lib/containers/storage
`UseRunc`	runc ユーティリティの使用。	`Yes`（既定値） - runc ユーティリティを使用します。 `No`：runc ユーティリティを使用しません。
`RuncBinaryPath`	runc ユーティリティの実行ファイルへのパス。	既定値：/usr/bin/runc
`RuncRootFolder`	コンテナ状態の保管領域のルートディレクトリへのパス。	既定値：/run/runc

感染したオブジェクトが検知されたときにコンテナに対して実行される処理は、ファイル脅威対策タスクの `FirstAction` および `SecondAction` パラメータの指定された値によって異なる場合があります。

コンテナで実行する処理と、感染したオブジェクトに実行する指定された処理との関係

FirstAction / SecondAction の値の設定	StopContainerIfFailed 処理の選択時に、コンテナに対して実行される処理

Disinfect	感染したオブジェクトの駆除に失敗した場合、コンテナは停止されます。
Remove	感染したオブジェクトの削除に失敗した場合、コンテナは停止されます。

暗号化された接続のスキャン設定

暗号化された接続のスキャン設定

設定	説明	値
EncryptedConnectionsScan	暗号化されたトラフィックのスキャンを有効または無効にします。 FTP プロトコルの場合、安全な接続のスキャンが既定で無効になっています。	Yes（既定値） - 安全な接続スキャンを有効にします。 No - 暗号化された接続のスキャンを無効にします。暗号化されたトラフィックを復号化しません。
EncryptedConnectionsScanErrorAction	安全な接続のスキャンエラーが Web サイトで発生した場合に実行する処理を指定します。	AddToAutoExclusions（既定値） - エラーが発生したドメインを、スキャンエラーが発生したドメインのリストに追加します。このドメインへのアクセス時には、暗号化されたネットワークトラフィックは監視されません。 Disconnect - ネットワーク接続をブロックします。
CertificateVerificationPolicy	Kaspersky Endpoint Security が証明書を確認する方法を指定します。 証明書が自己署名である場合、追加の検証は実行されません。	FullCheck（既定値） - 証明書の検証にインターネットを使用し、証明書の検証に必要だが存在しないチェーンをダウンロードします。 LocalCheck - 証明書の検証にインターネットを使用しません。
UntrustedCertificateAction	未確認の証明書が検出されたときに行うべき処理です。	Allow（既定値） - 信頼されない証明書のドメインへのアクセス時に確立されたネットワーク接続を許可します。 Block - 信頼されない証明書のドメインへのアクセス時に確立されたネットワーク接続をブロックします。
ManageExclusions	暗号化されたトラフィックをスキャンする際に除外リストを使用します。	Yes：[Exclusions.item_#]（下記参照）で指定された Web サイトをスキャンしません。 No（既定値） - すべての Web サイトをスキャンします。
MonitorNetworkPorts	本製品がネット	Selected（既定値） -

	ワークポートを監視する方法を指定します。	`[NetworkPorts.item_#]` セクション（下を参照）で指定されたネットワークポートのみを監視します。 `All` - すべてのネットワークポートを監視します。 この値を指定すると、オペレーティングシステムへの負荷が大幅に増大する場合があります。
[Exclusions.item_#] セクションには、スキャンから除外するドメインが含まれます。指定したドメインへのアクセス時に確立された、安全な接続をスキャンしません。		
`DomainName`	ドメイン名を指定します。ドメインの指定にマスクを使用できます。	既定値は定義されていません。
[NetworkPorts.item_#] セクションには、本製品が監視するネットワークポートが含まれます。		
`PortName`	ネットワークポートの説明。	既定値は定義されていません。
`Port`	本製品が監視するネットワークポートの番号。	`1～65535` 既定値は定義されていません。

タスクのスケジュール設定

タスクの開始スケジュール設定

設定	説明	値
`RuleType`	タスクの開始スケジュール。	`Once`：タスクを一度だけ実行します。 毎月：毎月指定した日時にタスクを実行します。 毎週：毎週指定した日時にタスクを実行します。 `Daily`：指定した日数間隔で定期的にタスクを実行します。 `Hourly`：指定された日時に、指定された時間間隔で定期的にタスクを実行します。 `Minutely`：指定した時刻から、指定した時間間隔（分）で定期的にタスクを実行する。 `Manual` - タスクを手動で開始します。

		PS - 製品の起動後にタスクを開始します。 BR - 定義データベースのアップデート後にタスクを開始します。
StartTime	タスクの開始日時。 StartTime オプションは、RuleType オプションが次のいずれかに設定されている場合に必要です： Once、Monthly、Weekly、Daily、Hourly、またはMinutely。	[< 年 >/< 月 >/< 月の日付 >] [hh]:[mm]:[ss]; [< 月の日付 >|< 週の日付 >]; [< 定期的に開始 >]。
RandomInterval	0 から指定値（分）までの時間間隔。これは、同時にタスクが開始されないようにタスク開始時刻に加算されます。	
RunMissedStartRules	本製品を起動後にミスタスクを実行します。	Yes：本製品を起動後にミスタスクを実行します。 No は、本製品を起動後のミスタスクの実行を有効にしません。

付録 4：コマンドラインの戻りコード

Kaspersky Endpoint Security のコマンドラインの戻りコードは次の通りです：

0 - コマンド / タスクが正常に完了しました。

1 - コマンド引数の一般的なエラー。

2 - 渡された製品設定のエラー。

64 - Kaspersky Endpoint Security が動作していません。

66 - 定義データベースがダウンロードされません（kesl-control --app-info コマンドでのみ使用）。

67 - ネットワークの問題のため、アクティベーション 2.0 がエラーで終了しました。

68 - 製品がポリシーに従って動作しているため、コマンドを実行できません。

69 - 本製品は、Amazon Paid Ami のインフラに設置されています。

70 - 次の操作が試行されました：実行中のタスクの開始、実行中のタスクの削除、実行中のタスクの設定の変更、停止中のタスクの停止、中断中のタスクの一時停止、実行中のタスクの再開。

71 - Kaspersky Security Network に関する声明に同意しませんでした。

72 - オブジェクトスキャンタスクまたはコンテナのカスタムスキャンタスクの実行中に脅威が検知されました。

73 - 設定内容を確認せずに、--accept フラグを使用してアプリケーションの処理に影響を与えるアプリケーションコントロールタスク設定の指定が試行されました。

74 - Kaspersky Endpoint Security は、アップデート後に再起動する必要があります。

75 - デバイスを再起動する必要があります。

76 - Root 権限を持つユーザーのみが指定されたパスへの書き込み権限を持つべきであるため、接続は禁止されています。

77 - 指定されたライセンスは、既にデバイスで使用されています。

128 - 不明なエラー。

65 - その他のすべてのエラー。

付録 5：Kaspersky Anti-Virus for Linux Mail Server との対話の設定

Kaspersky Endpoint Security と Kaspersky Anti-Virus for Linux Mail Server の連係動作を設定するには：

1. 次のコマンドを使用して、ファイル脅威対策タスクの設定を設定情報ファイルに保存します：

   `kesl-control --get-settings 1 --file <` ファイルの絶対パス `>`

2. 作成した設定情報ファイルを編集のために開きます。

3. 作成したファイルに、次のセクションを追加します：

   `[ExcludedFromScanScope.item_<` 項目番号 `>]`

   `Path=/var/opt/kaspersky/klms`

4. Kaspersky Anti-Virus for Linux Mail Server と連携されているすべてのメールエージェントについて、前述の手順で指定したセクションを繰り返します。

5. Kaspersky Anti-Virus for Linux Mail Server のフィルターおよびサービスの一時ディレクトリをスキャンから除外するには、作成したファイルに次のセクションを追加します：

   `[ExcludedFromScanScope.item_<` 項目番号 `>]`

   `Path=/tmp/klmstmp`

6. 変更内容を設定情報ファイルに保存します。

7. 次のコマンドを使用して、設定情報ファイルからファイル保護対策タスクへ設定をインポートします：

   `kesl-control --set-settings 1 --file <` ファイルの絶対パス `>`

Kaspersky Endpoint Security に関する情報源

ナレッジベースの Kaspersky Endpoint Security のページ

*ナレッジベース*は、カスペルスキーのテクニカルサポートサイトの一部です。

ナレッジベースの Kaspersky Endpoint Security のページに、製品の購入、インストール、使用方法について、役立つ情報、推奨事項、およびよくある質問への回答が掲載されています。

ナレッジベースの記事により、Kaspersky Endpoint Security およびその他のカスペルスキー製品に関連する質問への回答が得られる場合があります。ナレッジベースには、テクニカルサポートのニュースが含まれる場合もあります。

カスペルスキー製品のフォーラムの利用

特に緊急の対応が必要ではない場合は、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。

用語解説

Integration Server

Kaspersky Endpoint Security for Virtualization Light Agent コンポーネント。Kaspersky Endpoint Security コンポーネントと仮想インフラストラクチャの間で対話します。

Light Agent

Kaspersky Endpoint Security for Virtualization Light Agent コンポーネント。保護が必要な各仮想マシンにインストールします。

SIEM システム

*SIEM（セキュリティ情報およびイベント管理）*システムは、組織のセキュリティシステム内の情報とイベントを管理するためのソリューションです。

SVM

セキュア仮想マシン - スキャンサーバーサービス（Protection Server、Kaspersky Endpoint Security for Virtualization Light Agent のコンポーネント）がインストールされた特別な仮想マシン。

悪意のある URL のデータベース

危険と見なされるコンテンツを含む Web リソースのリスト。このリストは、カスペルスキーが作成しています。定期的にアップデートされ、カスペルスキー製品の配布キットに含まれています。

アプリケーション設定

あらゆる種別のタスクに共通し、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（アプリケーションの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）。

オブジェクトの駆除

感染したオブジェクトの処理方法。実行すると、データを全部または一部復元します。感染したすべてのオブジェクトを駆除できるわけではありません。

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 サーバーおよび FTP 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。

感染したオブジェクト

既知の悪意のあるコードの一部と完全に一致するコードを含むオブジェクト。そのようなオブジェクトにはアクセスしないでください。

管理グループ

デバイスの用途やインストールされたカスペルスキー製品に応じて、Kaspersky Security Center でグループ化された一連のデバイス。デバイスのグループは単一のユニットとして管理できるため、デバイスは管理を簡素化するためにグループ化されています。1 つの管理グループに他の複数のグループを含めることができます。管理グループにインストールされている製品ごとに、グループポリシーとグループタスクを作成できます。

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 のコンポーネント。また、これらの製品を管理するために使用することもできます。

グループタスク

管理グループに割り当てられ、その管理グループに属するすべての管理対象デバイスで実行されるタスク。

グループポリシー

「ポリシー」を参照してください。

現在のポリシー

データの漏洩を制御するために現在製品で使用されているポリシー。同時に複数のポリシーを使用できます。

現在のライセンス

製品が現在使用しているライセンス。

誤検知

感染していないオブジェクトがウイルスのコードに似たコードを持っているために、誤って感染したオブジェクトとして分類されること。

除外

除外：カスペルスキーのアプリケーションスキャンから除外されたオブジェクト。ファイル形式、ファイルマスク、領域（フォルダーやアプリケーションなど）、アプリケーションプロセス、ウイルス百科事典の分類に基づくオブジェクトの名前などによって特定されたファイルを、スキャンから除外することができます。それぞれのタスクに除外のセットを割り当てることができます。

信頼するデバイス

信頼するデバイスの設定の下にリストされているユーザーがいつでも完全にアクセスできるデバイス。

スタートアップオブジェクト

コンピューターにインストールされているオペレーティングシステムとソフトウェアが、正しく起動して動作するために必要なアプリケーションのセット。これらのオブジェクトは、オペレーティングシステムが起動するたびに実行されます。そのようなオブジェクトに感染することに特化したウイルスが存在し、オペレーティングシステムの起動をブロックしたりすることがあります。

定額制サービス

選択した設定（有効期限と端末の数）内での製品の使用を可能にします。定額制サービスは停止、再開、自動更新、およびキャンセルすることができます。

定義データベース

定義データベースの公開日時の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の脅威に関する情報が格納されているデータベース。定義データベースはカスペルスキーが作成し、1時間ごとにアップデートされます。

ファイルマスク

ワイルドカードを使用したファイル名の表示。ファイル名マスクで使用される標準的なワイルドカードは「*」と「?」です。「*」は任意の文字数の文字列を表し、「?」は任意の1文字を表します。

フィッシングサイトの URL のデータベース

カスペルスキーがフィッシングサイトとして識別した Web リソースの URL のリスト。データベースは定期的にアップデートされ、カスペルスキー製品の配布キットに含まれています。

プロキシサーバー

ユーザーが他のネットワークサービスへ間接的なリクエストを行えるようにするコンピューターネットワークのサービス。ユーザーは最初にプロキシサーバーへ接続し、他のサーバー上にある特定のリソース（ファイルなど）をリクエストします。次に、プロキシサーバーは指定されたサーバーに接続しリソースを取得するか、自身のキャッシュからリソースを返します（プロキシサーバーが自身のキャッシュを持っている場合）。場合によっては、プロキシサーバーがユーザーのリクエストやサーバーの応答を修正する場合があります。

ポリシー

ポリシーは、製品の設定を決定するとともに、管理グループ内のデバイスにインストールされた製品の設定へのアクセスを管理します。各アプリケーションに対して個別のポリシーを作成する必要があります。各管理グループのデバイスにインストールされた製品に対して作成できるポリシーの数に制限はありませんが、管理グループ内の各製品に対して一度に適用できるポリシーは1つだけです。

本製品のアクティベーション

製品をすべての機能が使用できる状態に切り替えます。アクティベーションは、製品のインストール中またはインストール後に実行します。製品をアクティベートするには、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が必要です。

予備のライセンス

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。

ライセンス

使用許諾契約書に基づいて提供される、製品を使用する期限付きの権利。

ライセンス証明書

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とともに、カスペルスキーから受け取る文書。ユーザーに提供されたライセンスに関する情報が記載されています。

サードパーティ製のコードに関する情報

サードパーティ製コードに関する情報は、製品のインストールフォルダーにある legal_notices.txt ファイルに記載されています。

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。

Amazon は Amazon.com, Inc. またはその関連会社の商標です。

FireWire は Apple Inc. の商標です。

Arm は、米国およびその他の地域における Arm Limited（またはその子会社）の登録商標です。

Bluetooth のワードマーク、およびロゴは Bluetooth SIG, Inc. の所有財産です。

Ubuntu および LTS は Canonical Ltd. の登録商標です。

Citrix、XenServer は、Citrix Systems, Inc. または 1 つ以上の子会社の商標であり、米国特許商標庁およびその他の国で登録されています。

Cloudflare、Cloudflare 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. の商標および登録商標です。

Docker および Docker ロゴは、米国およびその他の国における Docker, Inc. の商標または登録商標です。また、Docker, Inc. およびその他の当事者は、この文書で使用されているその他の用語の商標権を有している場合があります。

Chrome、Google Public DNS は、Google LLC の商標です。

HUAWEI、EulerOS、および FusionSphere は、Huawei Technologies Co., Ltd. の商標です。

Intel、Core は、米国およびその他の国における Intel Corporation の商標です。

Linux は、米国およびその他の国における Linus Torvalds の商標です。

Microsoft、Active Directory、Hyper-V、Outlook、Visual C++、Windows は、Microsoft グループ企業の商標です。

OpenStack は、米国およびその他の国における OpenStack Foundation の登録商標です。

Oracle および JavaScript は、Oracle およびその関連会社の登録商標です。

Red Hat、Red Hat Enterprise Linux、および CentOS は、米国およびその他の国における Red Hat Inc. またはその子会社の商標または登録商標です。

Debian は、Software in the Public Interest, Inc. の登録商標です。

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。

VMware、VMware NSX、VMware NSX Manager、VMware Tools、VMware vCenter、VMware vSphere は、米国およびその他の管轄区域における VMware, Inc. の登録商標または商標です。

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 により独占的に認可されています。