kaspersky

Kaspersky Endpoint Security for Linux

© 2026 AO Kaspersky Lab

目次

Kaspersky Endpoint Security 12.4 for Linux ヘルプ

Kaspersky Endpoint Security 12.4 for Linux

- Kaspersky Endpoint Security の使用モードについて
  - 本製品の Light Agent モードでの使用
  - 本製品のEndpoint Detection and Response Agent モードでの使用
- 製品の購入
- システム要件
  - ハードウェア要件
  - ソフトウェア要件
  - Light Agent モードの追加ソフトウェア要求
  - サポートされる Kaspersky Security Center のバージョン
  - KATA および OSMP プラットフォームに対応しているソリューションのバージョン

新機能

修正された問題

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

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

- 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 管理プラグインのインストール
  - Kaspersky Endpoint Security Web プラグインのインストール
  - Kaspersky Endpoint Security MMC プラグインのインストール
- Kaspersky Security Center を使用した本製品のインストールと初期設定
  - Web コンソールでのインストールパッケージの作成
  - Web コンソールでの初期設定
  - 管理コンソールでのインストールパッケージの作成
  - 管理コンソールでの初期設定
  - 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
  - Autoinstall.ini 設定情報ファイルでの設定
  - Kaspersky Security Center の使用の開始
- 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
  - 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
  - 対話モードでの製品のインストール後の設定
    - 標準モードまたは Light Agent モードの選択
    - 仮想マシンのロールの定義
    - VDI 保護モードの有効化
    - モードの選択：標準モードまたは Endpoint Detection and Response Agent
    - ロケールの選択
    - 使用許諾契約書とプライバシーポリシーの表示
    - 使用許諾契約書への同意
    - プライバシーポリシーへの同意
    - Kaspersky Security Network の使用
    - 特権グループからのユーザーの削除
    - ユーザーへの Administrator ロールの割り当て
    - システムイベントインターセプターメカニズムの設定

SELinux の自動設定の有効化
アップデート元の設定
プロキシサーバーの設定
本製品の定義データベースのアップデートの開始
定義データベースの自動アップデートの有効化
製品のアクティベーション
自動モードでの製品のインストール後の設定
インストール後の設定情報ファイルの設定
SELinux システムの許可ルールの設定
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
閉鎖ソフトウェア環境モードの ALT SP での本製品の実行
アプリケーションの動作のための OSnova オペレーティングシステムの設定
製品によるリソース消費の最適化
一般的なサーバーのロールに関する推奨事項
デバイス上のアプリケーションパフォーマンスの分析
ファイル脅威対策タスクの消費元の分析
最も頻繁にスキャンするオブジェクトの特定
ファイル脅威対策とスキャンするタスクに関する推奨事項
ウイルススキャンの除外設定
ファイル操作の読み取りの除外リストの設定
製品のメモリ使用制限の設定
ウェブ脅威対策タスクおよびネットワーク脅威対策タスクの推奨事項
旧バージョンからの本製品のアップデート
Kaspersky Endpoint Security 管理プラグインのアップデート
Kaspersky Security Center 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本製品のアップデート
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
本製品のアンインストール
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
コマンドラインを使用した本製品のアンインストール
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
Kaspersky Endpoint Security 管理プラグインのアンインストール
製品のライセンス
使用許諾契約書について
ライセンスの概要
ライセンス証明書について
ライセンスについて
アクティベーションコードの概要
ライセンス情報ファイルについて
月額制サービスについて
異なるライセンス間の製品機能の比較
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
Kaspersky Security Center を使用した本製品のアクティベーション
コマンドラインでのライセンス管理

使用済みのライセンスに関する情報の表示
Web コンソールを使用してデバイスのライセンスに関する情報を表示する
管理コンソールを使用してデバイスのライセンスに関する情報を表示する
コマンドラインでのライセンスに関する情報の表示
データ提供
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
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
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 Center に送信されるデータ
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 Security Network を使用する時に提供されるデータ
Kaspersky Endpoint Detection and Response Optimum と連携時に提供されるデータ
Kaspersky Endpoint Detection and Response (KATA) コンポーネントと連携時に提供されるデータ
Kaspersky Endpoint Detection and Response Expert（オンプレミス）コンポーネントと連携時に提供されるデータ
Kaspersky Network Detection and Response (KATA) コンポーネントと連携時に提供されるデータ
Kaspersky Unified Monitoring and Analysis Platform と連携時に提供されるデータ
アプリケーション管理概念
Kaspersky Security Center を使用した製品の管理
Kaspersky Endpoint Security 管理プラグイン
Kaspersky Security Center ポリシー
Kaspersky Security Center で作成された Kaspersky Endpoint Security のタスク
Web コンソール、Cloud コンソールへのログインとログアウト
Web コンソールでのポリシーの管理
Web コンソールでのポリシーの作成
Web コンソールでのポリシーの変更
Web コンソールでのポリシーの設定
管理コンソールでのポリシーの管理
管理コンソールでのポリシーの作成
Kaspersky Security Center 管理コンソールでのポリシー設定の変更
管理コンソールでのポリシーの設定
Web コンソールでのタスクの管理
Web コンソールでのタスクの作成
Web コンソールでのポリシー設定の変更
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
管理コンソールでのタスクの管理
管理コンソールでのタスクの作成
管理コンソールでのポリシー設定の変更
管理コンソールでのタスクの開始、停止、一時停止、および再開
コマンドラインを使用した本製品の管理
kesl-control コマンドの自動追加の有効化（bash completion）
コマンドラインでのタスク管理
コマンドラインでのタスクリストの表示
コマンドラインでのタスクステータスの表示
コマンドラインでのタスクの作成
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
コマンドラインでのタスクの削除
コマンドラインでのタスク設定の表示

- コマンドラインでのタスク設定の編集
  - 設定情報ファイルを使用したタスク設定の編集
  - コマンドラインのオプションを使用したタスク設定の編集
  - コマンドラインでのタスク設定の既定の復元
- コマンドラインでのタスクスケジュールの設定
- 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の表示
  - 製品の全般設定の編集
- クエリの結果を制限するフィルターの使用
- 製品設定のエクスポートとインポート
- コマンドラインを使用したユーザーロールの管理
  - ユーザーとロールのリストの表示
  - ユーザーへのロールの割り当て
  - ユーザーロールの取り消し

本製品の起動および停止
- 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
- 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
- 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

デバイスの保護ステータスとアプリケーションのパフォーマンス情報の表示
- Web コンソールでのデバイスの保護ステータスの表示
- 管理コンソールでのデバイスの保護ステータスの表示
- 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
- 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
- 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
- 製品統計の表示
  - Web コンソールでのアプリケーション統計の表示
  - 管理コンソールでのアプリケーション統計の表示
  - Web コンソールでのマウントポイントのリストの表示
  - 管理コンソールでのマウントポイントのリストの表示
  - コマンドラインでのアプリケーション統計とマウントポイントのリストの表示
- システムパフォーマンスメトリックの取得

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
- データベースとモジュールのアップデート
- アップデート元と更新シナリオ
- 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
- 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
- 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 Update Utility を使用したアップデート
- 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

ファイル脅威対策
- Web コンソールでのファイル脅威対策の設定
- 管理コンソールでのファイル脅威対策の設定
  - 「スキャン範囲」ウィンドウ
  - 「<新しいスキャン範囲>」ウィンドウ
  - 「スキャンの設定」ウィンドウ
  - 「脅威検出」ウィンドウでの処理

ファイル脅威対策の除外
「除外範囲」ウィンドウ
「<新しい除外範囲>」ウィンドウ
「マスクによる除外」ウィンドウ
「脅威の名前による除外」ウィンドウ
「プロセスによる除外」ウィンドウ
「信頼するプロセス」ウィンドウ
コマンドラインでのファイル脅威対策の設定
ファイル脅威対策タスクの設定
ネットワークディレクトリのスキャンの最適化
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
マルウェアのスキャン
Web コンソールでのマルウェアのスキャン
「スキャン範囲の追加」ウィンドウ
「スキャン範囲」セクション
「スキャン範囲」ウィンドウ
「除外範囲」セクション
「除外範囲」ウィンドウ
「除外範囲の追加」ウィンドウ
「マスクによる除外」ウィンドウ
「脅威の名前による除外」ウィンドウ
管理コンソールでのマルウェアのスキャン
「スキャン範囲」ウィンドウ
「<新しいスキャン範囲>」ウィンドウ
「スキャン範囲の設定」ウィンドウ
「スキャン範囲」ウィンドウ
「スキャンの設定」ウィンドウ
「脅威検出」ウィンドウでの処理
除外セクション
「除外範囲」ウィンドウ
「新しい除外範囲」ウィンドウ
「マスクによる除外」ウィンドウ
「脅威の名前による除外」ウィンドウ
コマンドラインでのマルウェアのスキャン
マルウェアスキャン事前定義済みタスクの設定
コマンドラインでのファイルとディレクトリのオブジェクトスキャン
簡易スキャン
Web コンソールでの簡易スキャン
「スキャン範囲の追加」ウィンドウ
「スキャン範囲」セクション
「スキャン範囲」ウィンドウ
「除外範囲」セクション
「除外範囲」ウィンドウ
「除外範囲の追加」ウィンドウ
「マスクによる除外」ウィンドウ
「脅威の名前による除外」ウィンドウ

- 管理コンソールでの簡易スキャン
  - ［スキャン範囲］ウィンドウ
  - ［新しいスキャン範囲］ウィンドウ
  - ［スキャン範囲の設定］ウィンドウ
  - ［スキャン範囲］ウィンドウ
  - ［スキャンの設定］ウィンドウ
  - ［脅威検出］ウィンドウでの処理
  - 除外セクション
  - ［除外範囲］ウィンドウ
  - ［新しい除外範囲］ウィンドウ
  - ［マスクによる除外］ウィンドウ
  - ［脅威の名前による除外］ウィンドウ
- コマンドラインでの簡易スキャン

リムーバブルドライブのスキャン
- Web コンソールでのリムーバブルドライブスキャンの設定
- 管理コンソールでのリムーバブルドライブスキャンの設定
- コマンドラインでのリムーバブルドライブスキャンの設定

コンテナスキャン
- コンテナの監視
  - Web コンソールからのコンテナ監視の設定
  - 管理コンソールからのコンテナ監視の設定
    - ［コンテナスキャン設定］ウィンドウ
  - コマンドラインからのコンテナ監視の設定
- コンテナとイメージのオンデマンドスキャン
  - Web コンソールでのコンテナースキャン
    - ［除外範囲］セクション
    - ［マスクによる除外］ウィンドウ
    - ［脅威の名前による除外］ウィンドウ
  - 管理コンソールでのコンテナースキャン
    - ［コンテナスキャン設定］ウィンドウ
    - ［スキャンの設定］ウィンドウ
    - ［脅威検出］ウィンドウでの処理
    - 除外セクション
    - ［マスクによる除外］ウィンドウ
    - ［脅威の名前による除外］ウィンドウ
  - コマンドラインでのコンテナスキャン
    - コンテナのスキャンタスクの設定
    - コンテナとイメージのオブジェクトスキャン
    - Jenkins との連携

ファイアウォール管理
- ネットワークパケットルールの概要
- 動的ルールの概要
- 定義済みの使用可能なネットワークについて
- Web Console でのファイアウォール管理
- 管理コンソールでのファイアウォール管理
  - ［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追加］ウィンドウ

「IP アドレスを追加してください」ウィンドウ
「使用可能なネットワーク」ウィンドウ
「ネットワーク接続」ウィンドウ
コマンドラインでのファイアウォール管理
コマンドラインでのネットワークパケットルールのリストの設定
コマンドラインでのネットワークゾーンの設定
ウェブ脅威対策
Web コンソールでのウェブ脅威対策の設定
管理コンソールでのウェブ脅威対策の設定
「信頼する URL」ウィンドウ
「スキャンの設定」ウィンドウ
コマンドラインでのウェブ脅威対策の設定
ネットワークトラフィックのスキャン
ネットワークトラフィック傍受モードについて
Web コンソールでのネットワークトラフィックのスキャン設定
管理コンソールでのネットワークトラフィックのスキャン設定
「信頼するドメイン」ウィンドウ
「信頼する証明書」ウィンドウ
トラフィック読み取りの除外リストウィンドウ
トラフィック読み取りの除外リストウィンドウ
監視対象ポート
コマンドラインでのネットワークトラフィックのスキャン設定
ネットワークトラフィックおよびスキャンする設定の表示および編集
暗号化接続スキャンからの除外の表示
信頼する root 証明書のリストの管理
トラフィック読み取りの除外リストの設定と表示
オペレーティングシステムのツールを使用したトラフィック読み取りの除外リスト
ネットワーク脅威対策
Web コンソールでのネットワーク脅威対策の設定
管理コンソールでのネットワーク脅威対策の設定
「除外」ウィンドウ
コマンドラインでのネットワーク脅威対策の設定
メール脅威対策
Web コンソールでのメール脅威対策の設定
管理コンソールでのメール脅威対策の設定
メール脅威対策の設定ウィンドウ
添付ファイルフィルターウィンドウ
コマンドラインでのメール脅威対策の設定
有害 USB 攻撃ブロック
Web コンソールでの BadUSB 攻撃ブロックの設定
管理コンソールでの BadUSB 攻撃ブロックの設定
コマンドラインでの BadUSB 攻撃ブロックの設定
悪質なリモート暗号化に対する保護
Web コンソールでのアンチクリプターの設定
管理コンソールでのアンチクリプターの設定
「スキャン範囲」ウィンドウ
「新しいスキャン範囲」ウィンドウ

- 「保護の設定」ウィンドウ
- 「除外範囲」ウィンドウ
- 「新しい除外範囲」ウィンドウ
- 「マスクによる除外」ウィンドウ
- コマンドラインでのアンチクリプターの設定

ブロックされるデバイスの管理

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ルールの概要
- アプリケーションコントロールルールのテストモード
- 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
- 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
  - 「アプリケーションコントロールルール」ウィンドウ
  - 「ルールの追加」ウィンドウ
  - 「アプリケーションカテゴリ」ウィンドウ
  - 「ユーザーまたはグループ」ウィンドウ
- コマンドラインでのアプリケーションコントロールの設定
  - アプリケーションコントロールタスクの設定
  - カテゴリのリストの作成と編集
  - カテゴリのリストの表示
  - アプリケーションコントロールのルールリストの設定
- アプリケーションコントロール設定のエクスポートとインポート

インベントリ

- Web コンソールでのインベントリの設定
  - 「スキャン範囲の追加」ウィンドウ
  - 「除外範囲」セクション
  - 「除外範囲」ウィンドウ
  - 「除外範囲の追加」ウィンドウ
- 管理コンソールでのインベントリの設定
  - 「スキャン範囲」ウィンドウ
  - 「新しいスキャン範囲」ウィンドウ
  - 除外セクション
  - 「除外範囲」ウィンドウ
  - 「新しい除外範囲」ウィンドウ
- コマンドラインでのインベントリの設定
  - インベントリタスクの設定
  - 検知されたアプリケーションのリストの表示

デバイスコントロール

- Web コンソールでのデバイスコントロールの設定
- 管理コンソールでのデバイスコントロールの設定
  - 「信頼するデバイス」ウィンドウ
  - 「信頼するデバイス」（デバイス ID）ウィンドウ
  - クライアントデバイスのデバイスウィンドウ
  - デバイスコントロールイベントウィンドウに基づくデバイスのリスト
  - 「信頼するデバイスへのアクセス」ウィンドウ
  - 「ユーザーまたはグループ」ウィンドウ
  - 「デバイス種別」ウィンドウ
  - 「デバイスアクセスルールの設定」ウィンドウを設定

- 「ユーザーまたはグループ」ウィンドウ
- スケジュールウィンドウにアクセス
- 「接続バス」ウィンドウ
- デバイスコントロールメッセージテンプレートの設定
- コマンドラインでのウェブコントロールの設定
- デバイスコントロールタスクの設定
- コマンドラインでの接続デバイスリストの表示とエクスポート
- コマンドラインでの信頼するデバイスリストの管理
- デバイスへの一時的なアクセスの許可
- Web コンソールでのブロックされたデバイスへのアクセスの許可
- コマンドラインでのデバイスへの一時アクセス

ウェブコントロール

- Web リソースアクセスルールについて
- Web コンソールでの ウェブコントロールの設定
- 管理コンソールでの ウェブコントロールの設定
- 「ウェブコントロールルール」ウィンドウ
- 「コンテンツカテゴリの選択」ウィンドウ
- 「データ種別カテゴリの選択」ウィンドウ
- 「アドレスを選択」ウィンドウ
- 「アドレスグループの選択」ウィンドウ
- 「アドレスグループの追加」ウィンドウ
- 「ユーザーを選択」ウィンドウ
- 「ユーザーまたはグループ」ウィンドウ
- スケジュールウィンドウにアクセス
- ウェブコントロールメッセージテンプレートの設定
- コマンドラインでのウェブコントロールの設定
- ウェブコントロールタスクの設定
- ウェブコントロール設定の表示と編集
- Web リソースアドレスマスクを作成するためのルール

システム変更監視

- リアルタイムのシステム整合性監視
- Web コンソールでのシステム変更監視の設定
- 管理コンソールでのシステム変更監視の設定
- 「スキャン範囲」ウィンドウ
- 「新しいスキャン範囲」ウィンドウ
- 「除外範囲」ウィンドウ
- 「新しい除外範囲」ウィンドウ
- 「マスクによる除外」ウィンドウ
- コマンドラインからのシステム変更監視の設定
- システム整合性チェック
- Web コンソールでのシステム整合性チェックの設定
- 「スキャン範囲の追加」ウィンドウ
- 「除外範囲」セクション
- 「除外範囲」ウィンドウ
- 「除外範囲の追加」ウィンドウ
- 「マスクによる除外」ウィンドウ

管理コンソールでのシステム整合性チェックの設定
「スキャン範囲」ウィンドウ
「新しいスキャン範囲」ウィンドウ
「除外範囲」セクション
「除外範囲」ウィンドウ
「新しい除外範囲」ウィンドウ
「マスクによる除外」ウィンドウ
コマンドラインでのシステム変更チェックの設定
ふるまい検知
Web コンソールでのふるまい検知の設定
管理コンソールでのふるまい検知の設定
「プロセスによる除外」ウィンドウ
「信頼するプロセス」ウィンドウ
コマンドラインでのふるまい検知の設定
脆弱性攻撃ブロック
Web コンソールでの脆弱性攻撃ブロックの設定
管理コンソールでの脆弱性攻撃ブロックの設定
脆弱性攻撃ブロック除外ウィンドウ
脆弱性攻撃ブロック除外ウィンドウ
コマンドラインでの脆弱性攻撃ブロックの設定
Kaspersky Security Network の使用
Web コンソールでの Kaspersky Security Network の使用を設定します。
管理コンソールでの Kaspersky Security Network の使用を設定します。
Kaspersky Security Network の設定
Kaspersky Security Network に関する声明
Kaspersky Private Security Network に関する声明
コマンドラインでの Kaspersky Security Network の使用の設定
コマンドラインを使用した Kaspersky Security Network への接続のチェック
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
アプリケーションの詳細設定
プロキシサーバーの設定
Web コンソールでのプロキシサーバーの設定
管理コンソールでのプロキシサーバーの設定
プロキシサーバーの除外ウィンドウ
コマンドラインでのプロキシサーバー設定の構成
グローバル除外の設定
Web コンソールでのグローバル除外リストの設定
管理コンソールでのグローバル除外リストの設定
マウントポイントのパス
コマンドラインでのグローバル除外の設定
プロセスメモリのスキャンからの除外
ファイル操作の読み取りモードの選択
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
本製品の安定性監視の有効化
アプリケーションの起動設定の構成
本製品による常駐メモリの使用の制限
メモリーとプロセッサリソースの使用の制限

- オブジェクトスキャンタスク数の制限
- Kaspersky Security Center ストレージへのデータ転送の設定
- タスク管理の許可設定
- バッテリー駆動時のタスクのキャンセル
- システムイベントインターセプターの設定
  - アップデート可能なカーネルモジュールをインストールできるかどうかの確認
  - 更新可能なカーネルモジュールを使用する場合の「セーフ」モード
  - Web コンソールでの読み取り設定の管理
  - 管理コンソールでの読み取り設定の管理
  - コマンドラインでの読み取り設定の管理
- テレメトリの詳細設定の管理

バックアップ
- Web コンソールでのバックアップの設定
- 管理コンソールでのバックアップの設定
- コマンドラインでのバックアップ設定の構成
- コマンドラインでのバックアップオブジェクトの操作

Detection and Response ソリューションとの連携
- Detection and Response ソリューションからのコマンドに基づく脅威対応処理について
- Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携
  - EDR Expert（オンプレミス）と正しく連携するための参照イメージを準備する方法
  - Web コンソールでの Kaspersky Endpoint Detection and Response Expert（オンプレミス）の連携の設定
  - コマンドラインでの Kaspersky Endpoint Detection and Response Expert（オンプレミス）の連携の設定
    - Kaspersky Endpoint Detection and Response Expert（オンプレミス）の連携設定
    - OSMP サーバーに接続するための証明書の管理
- Kaspersky Anti Targeted Attack Platform との連携
  - Web コンソールで Kaspersky Endpoint Detection and Response (KATA) の連携の設定
  - 管理コンソールで Kaspersky Endpoint Detection and Response (KATA) の連携の設定
    - KATA サーバー接続の設定
    - KATA サーバー接続の全般設定の管理
    - KATA サーバーへのデータ転送の設定
  - コマンドラインで Kaspersky Endpoint Detection and Response (KATA) の連携の設定
    - Kaspersky Endpoint Detection and Response（KATA）連携設定
    - KATA サーバーに接続するための証明書の管理
  - Web コンソールで Kaspersky Network Detection and Response (KATA) との連携の設定
  - 管理コンソールで Kaspersky Network Detection and Response (KATA) との連携の設定
    - NDR サーバー接続の設定
    - NDR サーバー接続の全般設定の管理
    - NDR サーバーへのデータ転送の設定
  - コマンドラインで Kaspersky Network Detection and Response (KATA) の連携の設定
    - Kaspersky Endpoint Detection and Response (KATA) の連携設定
    - NDR サーバーに接続するための証明書の管理
- サンドボックス統合
  - Web コンソールでのサンドボックス連携の設定
  - コマンドラインでの サンドボックス連携の設定
    - Sandbox との連携の設定
    - Sandbox サーバーに接続するための証明書の管理

Kaspersky Endpoint Detection and Response Optimumの連携
Kaspersky Endpoint Detection and Response Optimum 連携の有効化または無効化
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
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
Kaspersky Endpoint Detection and Response Optimum の連携ステータスの表示
検知された脅威と対応処理に関する情報の表示
Kaspersky Managed Detection and Response との連携
MDR と正しく連携するための参照イメージの作成に関する推奨事項
Kaspersky Managed Detection and Response との連携のための KPSN 設定情報ファイルのアップロード
Web コンソールでの Kaspersky Managed Detection and Response の連携の設定
管理コンソールでの Kaspersky Managed Detection and Response の連携の設定
コマンドラインで Kaspersky Managed Detection and Response の連携の設定
ネットワーク分離
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
自動ネットワーク分離の期間設定
ネットワーク分離の手動構成
Web コンソールでのネットワーク分離からの除外設定
自動ネットワーク分離からの除外の設定
ネットワーク分離除外を追加するウィンドウ
ネットワークプロファイル辞書ウィンドウ
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
隔離の管理
Web コンソールを使用したファイルの隔離
Web コンソールでの隔離設定の編集
管理コンソールでの隔離設定の編集
コマンドラインでの隔離設定の編集
コマンドラインでの隔離されたファイルの管理
プロセスの開始
プロセスの終了
デバイスからのファイルの受信
デバイスからのファイルの削除
侵害の兆候の調査
Web コンソールでの侵害の兆候の検索
コマンドラインでの侵害の兆候の検索
IOC ファイルの要件
オブジェクトの実行防止
Web コンソールでのオブジェクトの実行防止の設定
管理コンソールでのオブジェクト実行防止の設定
コマンドラインでのオブジェクトの実行防止の管理
Cloud Sandbox
Kaspersky Unified Monitoring and Analysis Platform との連携
Webコンソールで KUMA 連携の設定
管理コンソールで KUMA 連携の設定
［KUMA サーバー］ウィンドウ
［KUMA サーバー］ウインドウ
［KUMA サーバー接続設定］ウィンドウ

「サーバー証明書の追加」ウィンドウ
「クライアント証明書を追加する」ウィンドウ
コマンドラインで MDR 連携の設定
Kaspersky Unified Monitoring and Analysis Platform 統合タスク設定
KUMA サーバーに接続するための証明書の管理
Light Agent モードで本製品を使用する際の設定
Web コンソールでの Light Agent の設定
管理コンソールでの Light Agent の設定
Integration Server への接続
「Integration Server への接続」ウィンドウ
「Integration Server の証明書を検証」ウィンドウ
「Integration Server での認証」ウィンドウ
SVM 検出設定
SVM 接続タグ
SVM 選択アルゴリズム
接続の保護
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
イベントとレポートの表示
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
アプリケーションのイベントログの設定
Kaspersky Security Center でのイベントの表示
コマンドラインでのイベントの表示
グラフィカルユーザーインターフェイスでポップアップ通知の表示を設定する
グラフィカルインターフェイスを使用したアプリケーションの管理
グラフィカルインターフェイス
製品コンポーネントの有効化または無効化
スキャンタスクの開始と停止
オブジェクトスキャンとサンドボックススキャンの開始
アップデートタスクの開始と停止
Kaspersky Security Network の設定
レポートの表示
Backup オブジェクトの表示
ライセンスの管理
ライセンスの追加
ライセンスの削除
ライセンス情報の表示
デバイスへの一時的なアクセス許可
製品に関する情報の表示
トレースファイルの作成
アプリケーションコンポーネントの変更チェック
テクニカルサポートへの問い合わせ
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
テクニカルサポートに関する情報の入手
アプリケーショントレースファイルを作成
アプリケーショントレースの設定
アプリケーション管理プラグインのトレースファイル

ダンプファイルについて
ダンプファイル設定の管理
Kaspersky Security Center を使用したリモートデバイス診断
補足資料
補足資料 1：Kaspersky Endpoint Security を管理するコマンド
製品のタスクと設定を管理するためのコマンド
本製品の全般設定を管理するコマンド
タスク設定を管理するコマンド
タスクを管理するコマンド
オブジェクトの実行防止を管理するコマンド
コンテナスキャンの全般設定を管理するコマンド
ネットワークトラフィックのスキャン設定を管理するコマンド
統計コマンド
イベントを表示するコマンド
製品イベントを管理するコマンド
ライセンスを管理するコマンド
ファイアウォールを管理するコマンド
ブロックされたデバイスの管理に使用されるコマンド
デバイスコントロールを管理するコマンド
アプリケーションコントロールを管理するコマンド
ウェブコントロール管理コマンド
バックアップを管理するコマンド
隔離を管理するためのコマンド
ユーザーとロールを管理するためのコマンド
EDR Expert（オンプレミス）コンポーネントを管理するためのコマンド
NDR (KATA) コンポーネントを管理するためのコマンド
管理対象デバイスのネットワーク分離を管理するためのコマンド
KUMA との連携の設定を管理するためのコマンド
サンドボックスとの連携の設定を管理するためのコマンド
IOC スキャンを管理するコマンド
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
システムパフォーマンスメトリックを管理するためのコマンド
補足資料 2：設定情報ファイルと既定のアプリケーション設定
タスクの設定情報ファイルの編集ルール
プレセットの設定情報ファイル
コマンドラインタスクの既定
File_Threat_Protection タスク（ID:1）の既定
Scan_My_Computer タスク（ID:2）の既定
Scan_File タスク（ID:3）の既定
Critical_Areas_Scan タスク（ID:4）の既定
Update タスク（ID:6）の既定
System_Integrity_Monitoring タスク（ID:11）の既定
Firewall_Management タスク（ID:12）の既定
Anti_Cryptor タスク（ID:13）の既定
Web_Threat_Protection タスク（ID:14）の既定
Device_Control タスク（ID:15）の既定
Removable_Drives_Scan タスク（ID:16）の既定

Network_Threat_Protection タスク（ID:17）の既定
Container_Scan（ID:18）と Custom_Container_Scan（ID:19）タスクの既定
Behavior_Detection タスク（ID:20）の既定
Application_Control タスク（ID:21）の既定
Inventory_Scan タスク（ID:22）の既定
KATAEDR タスク（ID:24）の既定
Web_Control タスク（ID:26）の既定
Standalone_Sandbox タスク（ID:29）の既定
KATANDR タスク（ID:31）の既定
KUMA タスク（ID:29）の既定
メール脅威対策タスクの既定 (ID: 35)
BadUSB 攻撃ブロックタスクの既定 (ID: 37)
全般的な製品設定
コンテナスキャンの全般設定
ネットワークトラフィックのスキャン設定
タスクのスケジュール設定
補足資料 3：コマンドラインの戻りコード
補足資料 4：Kaspersky Anti-Virus for Linux Mail Server との対話の設定
補足資料 5：Web コンソールでのポリシーの製品設定
ホスト脅威対策
ファイル脅威対策
有害 USB 攻撃ブロック
リムーバブルドライブのスキャン
ふるまい検知
アンチクリプター
脆弱性攻撃ブロック
通信と危険サイト対策
メール脅威対策
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
セキュリティコントロール
デバイスコントロール
ウェブコントロール
アプリケーションコントロール
システム変更監視
信頼ゾーン
全般設定
検知の設定
Kaspersky Security Network
ユーザー対話
パフォーマンス
ネットワークの設定
コンテナスキャン
テクニカルサポート
レポートおよびストレージ
KSC との連携

OS 連携設定
イベントの設定
テレメトリの設定
組み込みエージェント
Managed Detection and Response
Endpoint Detection and Response Optimum
Endpoint Detection and Response Expert（オンプレミス）
Network Detection and Response (KATA)
Sandbox
KUMA との連携
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
補足資料 6：外部サービスとの対話設定
カスペルスキー製品との相互運用性
Kaspersky Security Center Linux
Network Detection and Response (KATA)
Kaspersky Unified Monitoring and Analysis Platform
Kaspersky Endpoint Security に関する情報源
用語解説
Integration Server
License
Light Agent
SIEM システム
SVM
悪意のある URL のデータベース
アンチクリプター
カスペルスキーのアップデートサーバー
感染したオブジェクト
管理グループ
管理サーバー
駆除
グループタスク
グループポリシー
現在のポリシー
現在のライセンス
誤検知
除外
信頼するデバイス
スタートアップオブジェクト
製品設定
製品のアクティベーション
定額制サービス
定義データベース

ファイルマスク
フィッシングサイトの URL のデータベース
プロキシサーバー
ポリシー
予備のライセンス
ライセンス証明書
サードパーティ製のコードに関する情報
商標に関する通知

Kaspersky Endpoint Security 12.4 for Linux ヘルプ

新機能と変更点

Kaspersky Endpoint Security 12.4 for Linux の新機能と変更点

システム要件

アプリケーションのシステム要件

機能の比較

- 異なるライセンス間の製品機能の比較
- Light Agent モードで本製品を使用する際の考慮事項
- 本製品のEndpoint Detection and Response Agent モードでの使用に関する考慮事項

使用開始時に行う設定

- Kaspersky Endpoint Security for Linux のインストールと初期設定のクイックインストールガイド（アプリケーションは標準モードで使用されます）
- 旧バージョンの製品のアップグレード
- 製品をインストールするための準備
- ネットワークエージェントのインストールと初期設定
- 初期設定中にコマンドラインで定義データベースと機能を更新する
- 事前定義済みの更新タスクを使用したコマンドラインでの定義データベースの更新(初期設定後)
- Kaspersky Security Center の使用の開始

ライセンス

- 本製品のライセンス管理
- 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
- コマンドラインでの初期設定中にアプリケーションの有効化
- コマンドラインでのアプリケーションの有効化とライセンスの管理（初期設定後）
- Kaspersky Security Center を使用した本製品のアクティベーション

監視とレポート

- デバイスとアプリケーションパフォーマンスについての情報の保護ステータスを表示する
- 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
- イベントとレポートの表示

データ提供と個人情報の保護

- データの提供

追加機能

- Light Agent モードで本製品を使用する際の設定
- アプリケーションの詳細設定
- Kaspersky Security Network を使用する
- バックアップ
- Detection and Response ソリューションとの連携

オペレーティングシステムのリソース消費の最適化

- リソース消費の最適化

テクニカルサポートへの問い合わせ

- トラブルシューティング
- テクニカルサポートへの問い合わせ

Kaspersky Endpoint Security 12.4 for Linux

Kaspersky Endpoint Security 12.4 for Linux（「Kaspersky Endpoint Security」、「アプリケーション」）は、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、ネットワーク攻撃や詐欺攻撃などの様々な種類の脅威から保護するように設計されています。

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。

このアプリケーションは、自動制御システムを伴う産業プロセスでの使用を目的としたものではありません。このようなシステムのデバイスを保護するには、Kaspersky Industrial CyberSecurity for Linux Nodes の使用を推奨します 。

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**。*コンテナ監視*（*コンテナスキャン*、*コンテナ監視*）コンポーネントを使用すると、名前空間および実行中のコンテナをリアルタイムでスキャンしてマルウェアを検知できます。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。

- **メール脅威対策***メール脅威対策保護*コンポーネントは、受信メールおよび送信メールの添付ファイルをスキャンして、ウイルスやその他の脅威となるアプリケーションを検知します。

- **有害 USB 攻撃ブロック***有害 USB 攻撃ブロック*保護コンポーネントを使用すると、キーボードを模倣した感染した USB デバイスがコンピューターに接続されるのを防止できます。

- **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*コンポーネントは、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、トラフィック消費量を削減し、業務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 NetworkKaspersky Security Network のデータを利用すると、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」属性が維持されません。

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 Anti Targeted Attack Platform との連携により、組織の IT インフラストラクチャが保護され、ゼロデイ攻撃、標的型攻撃、高度な持続的脅威などの脅威が迅速に検出されます。
- Kaspersky Endpoint Detection and Response Optimum との連携は、エクスプロイト、ランサムウェア、ファイルレス攻撃、攻撃者がデバイスやデータに危害を加えるために正規のシステムツールを使用することなどの脅威から、組織の IT インフラストラクチャを保護します。
- Kaspersky Unified Monitoring and Analysis Platform との連携により、情報セキュリティイベントの受信、処理、保存、データの分析と相関、イベントによる検索、情報セキュリティの脅威の兆候の検出に関する通知の作成が可能になります。
- Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携により、ほとんどのサイバーセキュリティリスクを防御し、脅威拡散の主なシナリオに対応できます。

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。

> 仮想化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、本製品の管理には Kaspersky Security Center を使用する必要があります。本製品は、Kaspersky Security Center Cloud コンソールまたはグラフィカルユーザーインターフェイスを使用して管理することはできません。

更新機能（アンチウイルス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 機能は、米国領土内のアプリケーションでは利用できない場合があります。

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 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。
- Endpoint Detection and Response Agent モードでは、保護対象デバイス上でサードパーティのアンチウイルスソリューションと連携する Kaspersky Detection and Response ソリューションに対応します（以下「Endpoint Detection and Response Agent モード」とも表記）。

本製品は一度に 1 つのモードでのみ使用できます。

既定では、本製品は標準モードで使用されます。

本製品の Light Agent モードでの使用

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 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 Light Agent モードで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。

   本製品のインストールを開始する前に、仮想マシンおよび仮想マシンテンプレートに Kaspersky Security Center 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。

   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。

次のアプリケーションコマンドを使用すると、Light Agent モードでの製品の動作に関する情報や、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。
- *「インストールなし」*ステータスは、本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent 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 ソリューションのすべてのコンポーネントを同時にアクティベートします。アクティベーションは、SVM にライセンスを追加することで、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 Security for Virtualization Light Agent のメインライセンスには、Kaspersky Endpoint Security アプリケーションの追加機能（Kaspersky Detection and Response ソリューションとの連携など）が含まれていない場合があります。この場合、追加機能を有効にするには、SVM にライセンスを追加する必要もあります。

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。Light Agent は、接続先の SVM を選択する際、他の設定に加えて、SVM に追加されたライセンスの種別を考慮します。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内の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）と一致しない場合、Light Agent は SVM に接続しません。Light Agent と SVM の接続に関する特別配慮の詳細については、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください。

Kaspersky Security Center またはコマンドラインを使用して Light Agent で保護対象仮想マシン上で、Light Agent for Linux が使用されているライセンスに関する情報をリモートで表示できます。

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製品モジュールのアップデートを取得します。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。

保護対象仮想マシン上のデータベースとソフトウエア機能は、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 で定義データベースと製品モジュールのアップデートがロールバックされると、保護対象仮想マシン上で特別なローカルのアップデートタスクが開始されます。このタスクにより、Light Agent は以前の一連のマルウェア定義データベースを使用する状態に戻ります。

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際のその他の考慮事項

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

- 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。

本製品のEndpoint Detection and Response Agent モードでの使用

Endpoint Detection and Response Agent モードの Kaspersky Endpoint Security では、Kaspersky Detection and Response ソリューションの機能を使用することで、サードパーティのアンチウイルスアプリケーションがインストールされているデバイスをセキュアに保護できます。

Endpoint Detection and Response Agent モードでは、デバイスの保護に Kaspersky Endpoint Security の標準の保護および制御コンポーネントは使用されません。サードパーティのウイルス対策製品は、標準のデバイス保護を提供します。Endpoint Detection and Response Agent モードの Kaspersky Endpoint Security は、デバイス上で実行されているプロセス、開いているネットワーク接続、変更されているファイルを継続的に監視し、次の Detection and Response ソリューションとの連携を提供します：

- Open Single Management Platform（以下「OSMP」とも表記）上の Kaspersky Endpoint Detection and Response Expert（オンプレミス）。
- Kaspersky Anti Targeted Attack Platform（以降、「KATA」とも表記）上の Kaspersky Endpoint Detection and Response および Kaspersky Network Detection and Response コンポーネント。

Kaspersky Endpoint Security 12.4 for Linux は、Dr. Web ウイルス対策製品と連携できます。Dr. Web ウイルス対策製品がインストールされているデバイスに、Kaspersky Endpoint Security を Endpoint Detection and Response Agent モードでインストールできます。

本製品は、最初にサードパーティのウイルス対策製品に、次に Kaspersky Security Center Network Agent、最後に Endpoint Detection and Response Agent モードの Kaspersky Endpoint Security の順にインストールする必要があります。サードパーティ製品のインストーラーは、カスペルスキー製品を互換性のないソフトウェアとして識別し、削除する可能性があるため、これは重要です。デバイスでサードパーティ製品をアップデートした後、サードパーティ製品のインストーラーがデバイスに互換性のないソフトウェアがないか再確認し、カスペルスキー製品を削除する可能性があるため、Kaspersky Endpoint Security とネットワークエージェント が正常に動作していることを確認することを推奨します。

本製品のEndpoint Detection and Response Agent モードでの設定

Kaspersky Endpoint Security を Endpoint Detection and Response Agent モードで使用する場合は、次の手順が必要です：

1. 保護する各仮想マシンに、Kaspersky Endpoint Security を Endpoint Detection and Response Agent モードでインストールします。

   アプリケーションモードに関する情報は、コマンドラインで `kesl-control --app-info` コマンドを実行して確認できます。

2. 本製品をアクティベートします。本製品に「Kaspersky Endpoint Detection and Response Expert（オンプレミス）アドオン」（以降、「EDR Expert（オンプレミス）ライセンス」とも表記）という別のライセンスを追加する必要があります。

   Endpoint Detection and Response Agent モードで本製品をアクティベートするには、追加機能用のライセンスのみが必要です。本製品にメインのライセンスを追加する必要はありません。

3. デバイスの保護に使用する Detection and Response ソリューションとの連携を有効にします。

   - OSMP プラットフォームで Kaspersky Endpoint Detection and Response Expert（オンプレミス）と連携するには、EDR Expert（オンプレミス）コンポーネントを有効にし、Kaspersky Security Center Web コンソールまたはコマンドラインで連携設定を管理する必要があります。
   - Kaspersky Anti Targeted Attack Platform プラットフォームで Kaspersky Endpoint Detection and Response と連携するには、EDR Expert（オンプレミス）コンポーネントを有効にし、Kaspersky Security Center Web コンソール、管理コンソール、またはコマンドラインで連携設定を管理する必要があります。
   - Kaspersky Anti Targeted Attack Platform 上の Kaspersky Network Detection and Response と連携するには、NDR (KATA) コンポーネントを有効にし、Kaspersky Security Center Web コンソール、管理コンソール、またはコマンドラインで連携設定を管理する必要があります。

   EDR Expert（オンプレミス）コンポーネントと NDR (KATA) コンポーネントのステータスは、以下の手順で確認できます。

   - Web コンソールのデバイスプロパティ（**資産（デバイス）→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**）。
   - コマンドラインで次のコマンドを実行します： `kesl-control --app-info`。

本製品のEndpoint Detection and Response Agent モードでの使用に関する考慮事項

Kaspersky Endpoint Security が Endpoint Detection and Response Agent モードで使用されている場合、使用できる製品コンポーネントとタスクの限定されたサブセットのみが表示されます。インストール後の製品設定は次の通りです：

- Detection and Response ソリューションとの連携を提供する次のコンポーネントは、完全に管理可能です：
  - EDR Expert（オンプレミス）
  - NDR (KATA)

  これらのコンポーネントは既定では無効になっており、本製品を Endpoint Detection and Response Agent モードで動作させるには、これらを有効にする必要があります。オブジェクトの実行防止の機能を含め、連携設定を管理できます。
- スキャン中はファイルへのアクセスがブロックされません：［**スキャン中は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ます（`FileBlockDuringScan=No`）。この設定は変更できません。
- ファイル脅威対策およびアンチクリプター保護コンポーネントは、機能制限モードで使用可能です。脅威が検知される時、これらのコンポーネントは悪意のあるオブジェクトの駆除または削除を試行したり、アクセスおよびアプリケーションアクティビティをブロックしたりせず、Detection and Response ソリューションとの連携を提供する Integration Server に脅威検知に関する情報を送信するだけです。

  ファイル脅威対策およびアンチクリプターを有効または無効にし、コンポーネント設定を管理できます（脅威の検知時の処理を除く）。次のパラメータは変更できません：
  - ファイル脅威対策：**脅威の検知時の処理**は［**スキップ**］です（`ActionOnThreat=Skip`）。
  - アンチクリプター：**暗号化検知時の処理**は［**通知**］です（`ActionOnDetect=Notify`）。

- ふるまい検知コンポーネントは完全に管理可能です。
- その他のすべての保護および制御コンポーネントは無効になっており、管理できません。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response（KATA）と連携している場合、脅威対応処理の一環として、Kaspersky Endpoint Security はデバイス上での実行ファイルとスクリプトの起動を制御できます。オブジェクト実行防止機能は、次の制限付きで使用可能です：

- スクリプトがインタープリターから起動された場合、本製品はスクリプトの起動を制御しません。
- 本製品は、デバイス上でのオフィスソフトウェアファイルの起動も制御しません。

製品の購入

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。

Kaspersky Endpoint Security 配布キットには、次のファイルが含まれています：

- kesl-12.4.0-<ビルド番号>.i386.rpm、kesl_12.4.0-<ビルド番号>_i386.deb

  これらには、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-12.4.0-<ビルド番号>.x86_64.rpm、kesl_12.4.0-<ビルド番号>_amd64.deb

  これらには、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-12.4.0-<ビルド番号>.aarch64.rpm、kesl_12.4.0-<ビルド番号>_arm64.deb

  これらには、メインのアプリケーションファイルが含まれています。該当するパッケージマネージャー用のパッケージは、Arm® アーキテクチャ向けの 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-12.4.0-<ビルド番号>.i386.rpm、kesl-gui_12.4.0-<ビルド番号>_i386.deb

  これらには、本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-12.4.0-<ビルド番号>.x86_64.rpm、kesl-gui_12.4.0-<ビルド番号>_amd64.deb

  これらには、本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-12.4.0-<ビルド番号>.aarch64.rpm、kesl-gui_12.4.0-<ビルド番号>_arm64.deb

  これらには、本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-12.4.0.<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。

- ksn_license.<言語 ID>

  このファイルには、Kaspersky Security Network に関する声明の本文が含まれています。

- license.<言語 ID>

  このファイルには、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手段、またはテクニカルサポートによって推奨されていない手段を使用してアプリケーションの設定情報ファイルを編集すると、アプリケーションとオペレーティングシステムのパフォーマンスが低下したり、障害が発生したり、端末の保護が低下したり、データにアクセスできなくなったり、データが破損したり、KSN への追加統計の送信が有効になったりす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

- AMD64 アーキテクチャ、2 GHz 以上、2 つ以上のコア、SSE2 命令セット対応の CPU。
- 1 GB 以上のスワップ領域
- 64 ビットオペレーティングシステムの場合、本製品で 2 GB の RAM が使用可能（32 ビットオペレーティングシステムの場合、本製品で 1 GB の RAM が使用可能）。
- 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）

  トレースファイルとアプリケーションメモリダンプファイルを保存するには、追加のディスク容量が必要です。

  `ScanArchived=Yes` と `ScanSfxArchived=Yes`（既定では、スキャンタスクの場合は `Yes`、ファイル脅威対策の場合は `No` に設定されています）のいずれかまたは両方で圧縮ファイルおよび複合オブジェクトをスキャンする場合、ファイル脅威対策およびスキャンタスクでは、オブジェクトの種別と解凍後のサイズに応じて追加のディスク容量が必要になります。

  圧縮ファイルと複合オブジェクトをスキャンするために、ディレクトリ /tmp に十分な空き容量があることを確認することを推奨します。各タスクの `SizeLimit` 設定を指定して、スキャンできる圧縮ファイルのサイズを（圧縮された状態で）制限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 100 Mbps の帯域幅が必要です。

Arm アーキテクチャのハードウェア最小要件

- Armv8.2-A Kunpeng 920 または Armv8-A Baikal-M (BE-M1000) CPU または m-TrusT ターミナルプラットフォーム

- 1 GB 以上のスワップ領域

- アプリケーションで 2 GB の RAM が使用可能

- 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）

  トレースファイルとアプリケーションメモリダンプファイルを保存するには、追加のディスク容量が必要です。

  `ScanArchived=Yes` と `ScanSfxArchived=Yes`（既定では、スキャンタスクの場合は `Yes`、ファイル脅威対策の場合は `No` に設定されています）のいずれかまたは両方で圧縮ファイルおよび複合オブジェクトをスキャンする場合、ファイル脅威対策およびスキャンタスクでは、オブジェクトの種別と解凍後のサイズに応じて追加のディスク容量が必要になります。

  圧縮ファイルと複合オブジェクトをスキャンするために、ディレクトリ /tmp に十分な空き容量があることを確認することを推奨します。各タスクの `SizeLimit` 設定を指定して、スキャンできる圧縮ファイルのサイズを（圧縮された状態で）制限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：

- サポートされる 32 ビットオペレーティングシステム：

  - Debian GNU/Linux 12.7、12.8、12.9、12.10、12.11、12.12

- サポートされる 64 ビットオペレーティングシステム：
  - AlmaLinux OS 8.6、8.7、8.8、8.9
  - AlmaLinux OS 9.4、9.5、9.6
  - AlterOS® 2025。
  - Amazon™ Linux 2023
  - 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.10015-01 (operational update 1.8)
  - Astra Linux Special Edition RUSB.10015-03 (operational update 7.6)
  - Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6)
  - Astra Linux Special Edition RUSB.10015-17 (operational update 1.7.3)
  - Astra Linux Special Edition RUSB.10015-37 (operational update 7.7)

    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、7.3、7.4、7.5、7.6、7.7、7.8、7.9
  - CentOS Stream 8
  - CentOS Stream 9
  - CentOS Stream 10
  - Debian GNU/Linux 12.7、12.8、12.9、12.10、12.11、12.12
  - Debian GNU/Linux 13.0、13.1、13.2
  - EMIAS 1.0
  - EulerOS 2.0 SP10
  - Fedora Linux 41

- Kylin Desktop OS V10 SP1。
- Linux Mint 21.3
- Linux Mint 22.2
- Mostech 12 リリース 2021.1
- openSUSE Leap 15.6
- Oracle Linux 7.3、7.4、7.5、7.6、7.7、7.8、7.9
- Oracle Linux 8.5、8.6、8.7、8.8、8.9
- Oracle Linux 9.4、9.5、9.6
- Red Hat Enterprise Linux 7.2、7.3、7.4、7.5、7.6、7.7、7.8、7.9
- Red Hat Enterprise Linux 8.5、8.6、8.7、8.8、8.9
- Red Hat Enterprise Linux 9.4、9.5、9.6
- Red Hat Enterprise Linux 10.0、10.1
- Rocky Linux 8.6、8.7、8.8、8.9
- Rocky Linux 9.4、9.5、9.6
- SberLinux 8.10、9.1、9.5、9.6
- SberOS 3.4.0、3.5.0
- SUSE Linux Enterprise Server 12.5、12.6、12.7
- SUSE Linux Enterprise Server 15.4、15.5、15.6、15.7
- Ubuntu® 22.04 LTS
- Ubuntu 24.04 LTS
- ALT Education 10
- ALT Education 11
- ALT Workstation 11
- ALT Server 11
- ALT SP Workstation リリース 10
- ALT SP Server リリース 10
- Atlant、 Alcyone build、 version 2022.02
- GosLinux 7.2

- M OS 12 Server リリース 2021.1。
- MoS OS 15.5 Arbat
- MSVSphere 9.4 Workstation
- MSVSphere 9.4 Server
- MES OS 12 V release 2021.1
- MES OS 12 Panel リリース 2021.1
- MES OS 12 Desktop リリース 2021.1
- OSnova 2.14
- OSnova 3.0.5
- RED OS® 7.3
- RED OS 8.0
- ROSA「Cobalt」7.9 ワークステーション
- ROSA「Cobalt」7.9 サーバー
- ROSA「Chrome」12 ワークステーション
- ROSA "Chrome" 12 サーバー
- SintezM-Client 8.6
- SintezM-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 15.4、15.5、15.6、15.7
  - Ubuntu 22.04 LTS
  - ALT SP Workstation リリース 10
  - ALT SP Server リリース 10
  - RED OS 8.0

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。

Light Agent モードの追加ソフトウェア要求

Kaspersky Endpoint Security は、Kaspersky Security for Virtualization Light Agent 6.4 の一部として Light Agent として使用することができます。Light Agent モードにおけるアプリケーションの仮想インフラストラクチャ要求は、Kaspersky Security for Virtualization Light Agent のヘルプで確認できます。

Kaspersky Endpoint Security のソフトウェアおよびハードウェア要件は、指定された制限付きで、Kaspersky Endpoint Security の Light Agent モードで仮想マシンに適用されます。

保護対象仮想マシンの BIOS は、SMBIOS 仕様バージョン 2.1 以降に対応している必要があります。

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必要があります：

- 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 Private Cloud、TIONIX Cloud Platform、Astra Linux、ALT Server Virtualization、Basis.Dynamix、または Basis Dynamix Standard に基づくインフラストラクチャでは、仮想マシンに QEMU Guest Agent をインストールする必要があります。

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 Windows 14、14.2、15.1 では、Kaspersky Endpoint Security は、管理コンソールで MMC 管理プラグインを使用して、または Kaspersky Security Center Web コンソールで Web 管理プラグインを使用して管理できます。
- Kaspersky Security Center Linux 15.1、15.2、15.3、15.4、16.0、16.1、16.2 では、Web 管理プラグインを使用して、Kaspersky Security Center Web コンソールから Kaspersky Endpoint Security を管理できます。

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 Windows 14.2、15.1。
- Kaspersky Security Center 15.4、16.0、16.1、16.2。

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 Anti Targeted Attack Platform の Kaspersky Endpoint Detection and Response 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 Windows 14.2、15.1。
- Kaspersky Security Center Linux 15.3、15.4、16.0、16.1、16.2。

Kaspersky Endpoint Detection and Response Optimum 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 Windows 15.1。
- Kaspersky Security Center Linux 15.3、15.4、16.0、16.1、16.2。

KATA および OSMP プラットフォームに対応しているソリューションのバージョン

Kaspersky Endpoint Security は、Kaspersky Anti Targeted Attack Platform ベースの次のソリューションと互換性があります：

- Kaspersky Anti Targeted Attack Platform 6.0（Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA)、およびサンドボックス）。
- Kaspersky Anti Targeted Attack Platform 6.1（Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA)、およびサンドボックス）。
- Kaspersky Anti Targeted Attack Platform 7.0（Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA)、およびサンドボックス）。
- Kaspersky Anti Targeted Attack Platform 7.1（Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA)、およびサンドボックス）。
- Kaspersky Anti Targeted Attack Platform 8.0（Kaspersky Network Detection and Response (KATA) およびサンドボックス）。

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。

Kaspersky Endpoint Security は、Open Single Management Platform（以下「OSMP」とも表記）上の Endpoint Detection and Response Expert（オンプレミス）8.0 と互換性があります。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）8.0の製品情報については、Kaspersky Endpoint Detection and Response Expert（オンプレミス）のヘルプを参照してください。

新機能

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

- 新しい機能コンポーネント「メール脅威対策」を導入しました。このコンポーネントは、受信メールおよび送信メールの添付ファイルをスキャンして、ウイルスやその他の脅威となるアプリケーションを検知します。

- 新しい機能コンポーネント「有害 USB 攻撃ブロック」を導入しました。このコンポーネントは、キーボードを模倣した感染した USB デバイスがクライアントデバイスに接続するのを防ぎます。

- デバイスコントロールが改善されました。ユーザーのリクエストに応じて、ブロックされたデバイスへの一時的なアクセスを許可できるようになりました。

- 脆弱性攻撃ブロックコンポーネントの強化。オブジェクトに対して、コンポーネント固有のスキャン除外を設定できるようになりました。

- 更新可能なカーネルモジュールの強化：

  - 更新可能なカーネルモジュールにより、ファイル操作のインターセプトを最適化できるようになりました。スキャンする必要のないファイルとプロセスのキャッシュを使用することで、本製品のパフォーマンスが向上します。

  - 更新可能なカーネルモジュールを使用することで、グローバル除外リストをより細かく設定できるようになりました。fanotify テクノロジに基づくインターセプトメカニズムを使用している場合、指定されたマウントポイント全体が、ファイル操作のインターセプトから除外されます。更新可能なカーネルモジュールを使用すると、デバイスにマウントされた特定のローカルディレクトリまたはリモートディレクトリを除外できます。

- Kaspersky Endpoint Detection and Response (KATA) との連携を提供する EDR (KATA) コンポーネントの名称が EDR Expert (OSMP) に変更されました。このコンポーネントは、Kaspersky Endpoint Detection and Response Expert（オンプレミス）Integration も提供します。連携タスクの名称が *Kaspersky Endpoint Detection and Response Expert（オンプレミス）Integration*（KATAEDR、ID: 24）に変更されました。

- ほとんどのサイバーセキュリティリスクを防御し、脅威拡散の主なシナリオを網羅するエンタープライズサイバーセキュリティソリューションである Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携を設定できるようになりました。Open Single Management Platform (OSMP) 上で Kaspersky Endpoint Detection and Response Expert（オンプレミス）のコンポーネントを導入します。Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携は、Kaspersky Endpoint Detection and Response (KATA) との連携のすべての機能と、次の新機能に対応します：

  - YARA スキャンの開始。*YARA* スキャンでは、Kaspersky Endpoint Security は YARA ファイルを使用して、デバイス上の悪意のある活動のシグネチャを検索します。

  - フォレンジック、つまりサイバー犯罪およびデータ流出を含むインシデントの調査に役立つ可能性のあるデジタルデータを収集します。

  - デバイス上のイベントに関する拡張データ（テレメトリ）を OSMP プラットフォーム上のテレメトリサーバーに送信します。

  - Indicator of Attack（IOA）を含むテレメトリのみの送信。Web コンソールポリシーでカスタムフィルターを設定することもできるようになりました。

- ライセンスを追加することで、Kaspersky Endpoint Detection and Response Expert（オンプレミス）および Kaspersky Endpoint Detection and Response (KATA) との連携を提供する EDR Expert (OSMP) コンポーネントをアクティベートします。

- コマンドラインまたは Web コンソールのポリシープロパティで、*Kaspersky Endpoint Detection and Response Expert（オンプレミス）Integration* タスクの設定で連携モードを選択します。

- 本製品を Endpoint Detection and Response Agent モードで使用することで、保護対象デバイスでサードパーティのアンチウイルスソリューションと連携する Kaspersky Detection and Response ソリューションに対応します。このモードでは、デバイスは Kaspersky Endpoint Security の標準の保護およびコントロールコンポーネントによって保護されません。サードパーティ製品がデバイスの標準的な保護を担います。

- インストール後、本製品の初回起動時にトレースファイルを作成できます。Web コンソール、管理コンソール、または初期設定情報ファイルの設定で、本製品の初回起動時にトレースファイルの作成を有効にできるようになりました。

- Web コンソールのポリシー管理インターフェイスがアップデートされました。ポリシーのセクションが再構成され、必要な機能がより早く見つかるようになりました。

- トラフィック傍受モードとして、eBPF テクノロジーまたは iptables ユーティリティを選択できるようになりました。

- テレメトリソース（eBPFのみ、または eBPF と auditd の組み合わせ）を選択できるようになりました。auditd の場合は、操作モード（排他モードまたはマルチキャストモード）も選択できます。

- スキャンするためにファイルおよびディレクトリをサンドボックスに送信するモードを選択できるようになりました：手動、自動のみ、自動および手動。

- 本製品を Light Agent モードで使用する場合、さらに多くの機能を利用できるようになりました：

  - 更新可能なカーネルモジュールに基づくシステムイベント傍受メカニズムを利用できます。

  - 脆弱性攻撃ブロック機能コンポーネントを利用できるようになりました。

  - 脅威の検知が強化されました。

- 管理サーバーで KSN プロキシサービスを使用せずに、Kaspersky Private Security Network（KPSN）の使用が直接できるようになりました。

- Web コンソールと管理コンソールで不在ポリシーを作成できるようになりました。不在ポリシーは、デバイスが組織のネットワークから離れると有効になります。

- Web コンソールまたは管理コンソールでマウントポイントのリストを表示およびエクスポートする時、またはコマンドラインでこのリストを表示する時に、マウントポイントが名前空間で見つかったことに関する情報も表示されるようになりました。

- eBPF 対応のカーネルバージョン 4.18 以降で、64 ビットオペレーティングシステム上のふるまい検知コンポーネントでシステムテレメトリを取得するための代替メカニズムを強化しました。これにより、auditd カーネル監査サブシステムのリソースを解放できます。

- Kaspersky Managed Detection and Response と連携する時に、テレメトリデータに次の情報を含めることができるようになりました。
  - コンテナで発生しているイベントの表示
  - コンテナの namespace の ID
  - コンテナ名
- 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。

修正された問題

以下の表は、Kaspersky Endpoint Security の以前のバージョンで検出され、現在のバージョンで修正されたすべての問題を示しています。

Web プラグイン 12.4.0.8289 で修正された問題の一覧

識別子	説明
10724878	デバイスにポリシーを適用した際、`InterceptorApplyStrategy` の設定には既定値の `RestartServiceAutomatically` ではなく、`RestartServiceManually` の値が使用されました。

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。
- Kaspersky Security Center を使用して Kaspersky Endpoint Security を管理する予定の場合は、デバイスに Kaspersky Security Center ネットワークエージェントをインストールする準備をしてください（詳細については、『Kaspersky Security Center ヘルプ』を参照してください）。

  > 仮想化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、本製品の管理には Kaspersky Security Center を使用する必要があります。

- SELinux のアクセス制御システムを使用する場合は、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する必要があります。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。
- 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は、デバイス上で GUI パッケージの依存関係が満たされていることを確認する必要があります。デバイスが分離されたネットワークセグメントにあり、パッケージマネージャーのリポジトリにアクセスできない場合は、参照デバイス（libice6、libsm6、libx11-6、libx11-xcb1、libxcb-icccm4、libxcb-image0、libxcb-keysyms1、libxcb-randr0、libxcb-render-util0、libxcb-render0、libxcb-shape0、libxcb-shm0、libxcb-sync1、libxcb-xfixes0、libxcb-xinerama0、libxcb-xkb1、libxcb1、libxi6、libxml2、zlib1g）の依存関係のリストを確認し、GUI をインストールする前にすべてのデバイスにパッケージをダウンロードして配布することを推奨します。
- 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は、オペレーティングシステムに Zenity ユーティリティがインストールされていることを確認する必要があります。
- 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：
  - アプリケーション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
- 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。

- 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**）。

  カーネルパラメータと値のペア `kernel.yama.ptrace_scope=3` を指定すると、ptrace トレースを無効にすることができます。この場合、本製品では次のように処理されます：

  - 本製品に障害が発生した場合、kesl プロセスのダンプファイルは作成できません。
  - ふるまい検知コンポーネントは、プロセスの環境設定を受け取ることができません。
  - カーネルバージョンが 5.7 以降のオペレーティングシステムでは、/proc/pid/syscall および /proc/pid/mem の読み取りが禁止されているため、アプリケーションコントロールコンポーネントはコマンドライン引数およびプロセス環境変数を読み取ることができません。カーネルバージョン 5.0 のオペレーティングシステムでは、アプリケーションコントロールコンポーネントは正しく機能しません。
  - /proc/pid/mem の読み取りが禁止されているため、スキャンタスクではプロセスメモリとカーネルメモリのスキャンは機能しません。
  - 必須アクセスコントロールモードでは、/proc/PID/mem の読み取りが許可されていないため、プロセスのメモリを YARA でスキャンすることは保証されません。

- 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 MMC 管理プラグインを機能させるには、Microsoft® Visual C++® 2015 再頒布可能パッケージ Update 3 RC（https://www.microsoft.com/en-us/download/details.aspx?id=52685 を参照）を、Kaspersky Security Center 管理サーバー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。

- 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、/

- オペレーティングシステムベンダーが推奨するファイル記述子の制限がオペレーティングシステムで設定されていることを確認します。制限を確認するには、コマンド `cat /proc/sys/fs/file-max` を実行します。本製品の実行中、オペレーティングシステムはより多くの記述子を使用する場合があります。一般的には、/etc/sysctl.conf ファイルで `fs.file-max=9223372036854775807` を指定してファイル制限を無効にすることを推奨します。この設定の値を変更した後は、オペレーティングシステムを再起動する必要があります。

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：

- 保護対象の仮想マシンが Light Agent モードの全般要求を満たしていることを確認してください。
- 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。Light Agent で使用するポートは、 Kaspersky Security for Virtual Environment Light Agent のヘルプに記載されています。

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 および Kaspersky Endpoint Security の管理プラグインのインストール方法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。

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。

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 Security Center を使用して Kaspersky Endpoint Security を管理する場合は、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 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。本製品と本製品のグラフィカルユーザーインターフェイスは、異なるパッケージとして提供されます。Kaspersky Endpoint Security と、必要に応じてグラフィカル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**

   アプリケーションを操作できるように準備し、クライアントデバイスの保護を有効にするには、初期設定が必要です。

Kaspersky Security Center を使用して Kaspersky Endpoint Security をインストールした場合、インストールパッケージで指定されたパラメータに従って、インストール中に初期設定が自動的に実行されました。インストールが完了したら、「はじめに」の手順を実行してください。

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、初期セットアップウィザードを実行し、初期設定を対話または自動で実行します。

デバイス上でアプリケーションの初期設定が完了していない場合、そのデバイス上でアプリケーションを使用したりアップデートしたりすることはできません。

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 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。本製品と本製品のグラフィカルユーザーインターフェイスは、異なるパッケージとして提供されます。

   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、本製品のグラフィカルインターフェイスには対応していません。

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、インストールパッケージのパラメータまたはインストールパッケージに含まれる設定情報ファイルで初期構成の設定を指定する必要があります。

  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`）。

  設定値では、大文字と小文字が区別されます。

- 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、対話または自動モードで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**

   アプリケーションを操作できるように準備し、クライアントデバイスの保護を有効にするには、初期設定が必要です。

   Kaspersky Security Center を使用して Kaspersky Endpoint Security をインストールした場合、インストールパッケージで指定されたパラメータに従って、インストール中に初期設定が自動的に実行されました。インストールが完了したら、「はじめに」の手順を実行してください。

   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、初期セットアップウィザードを実行し、初期設定を対話または自動で実行します。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：

   - 初期セットアップウィザードの「アプリケーションを Light Agent モードで使用する」手順で **yes** と入力します。
   - 初期設定情報ファイルで `KSVLA_MODE=Yes` 設定を指定します。

     設定値では大文字と小文字が区別されます。

   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。

   デバイス上でアプリケーションの初期設定が完了していない場合、そのデバイス上でアプリケーションを使用したりアップデートしたりすることはできません。

Endpoint Detection and Response Agent モード

デバイスにサードパーティのウイルス対策製品をインストールしてからインストールを実行することを推奨します。

Kaspersky Endpoint Security を Endpoint Detection and Response Agent 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 Security Center を使用して Kaspersky Endpoint Security を管理する場合は、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 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。本製品と本製品のグラフィカルユーザーインターフェイスは、異なるパッケージとして提供されます。

   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、インストールパッケージのパラメータまたはインストールパッケージに含まれる設定情報ファイルで初期構成の設定を指定する必要があります。

     Endpoint Detection and Response Agent モードを選択する必要があります（設定情報ファイルで `ENDPOINT_AGENT_MODE=Yes`）。

     > 設定値では大文字と小文字が区別されます。

   - 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、対話または自動モードで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**

   アプリケーションを操作できるように準備し、クライアントデバイスの保護を有効にするには、初期設定が必要です。

   Kaspersky Security Center を使用して Kaspersky Endpoint Security をインストールした場合、インストールパッケージで指定されたパラメータに従って、インストール中に初期設定が自動的に実行されました。インストールが完了したら、「はじめに」の手順を実行してください。

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、初期セットアップウィザードを実行し、初期設定を対話または自動で実行します。初期設定の際に次のいずれかの方法で Endpoint Detection and Response Agent モードを選択します：

- 初期セットアップウィザードの「アプリケーションを Endpoint Detection and Response Agent モードで使用する」手順で `yes` と入力します。
- 初期設定情報ファイルで `ENDPOINT_AGENT_MODE=Yes` 設定を指定します。

設定値では大文字と小文字が区別されます。

デバイス上でアプリケーションの初期設定が完了していない場合、そのデバイス上でアプリケーションを使用したりアップデートしたりすることはできません。

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

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。

Linux デバイスにネットワークエージェントのインストールを開始する前に、いくつかの準備手順を実行する必要があります。ネットワークエージェントをインストールするためにデバイスを準備する方法については、Kaspersky Security Center のヘルプを参照してください。手順は OS によって異なります。

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。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。
- コマンドラインを使用：
  - 応答ファイルを使用したサイレントモード。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。ネットワークエージェントのインストールオプションと初期設定の説明については、Kaspersky Security Center ヘルプ（「Linux用ネットワークエージェントをサイレントモードでインストールする（応答ファイルを使用）」セクション）を参照してください。
  - パッケージマネージャーに応じて、RPM または DEB パッケージから対話的に実行します。この場合、インストール後に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構成を実行する必要があります。

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。

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 管理 MMC 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。

管理アプリケーションに Kaspersky Security Center 管理コンソールを使用している場合は、以前のバージョンの管理プラグインで作成したポリシーやタスクを、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 プラグインをインストールするには、次の操作を実行します：

- Kaspersky Security Center Web コンソールのクイックスタート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クイックスタート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**] → [**クイックスタートウィザード**]）。クイックスタートウィザードでは、インストールされている Web プラグインが最新バージョンか確認したり、必要なアップデートをダウンロードできます。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**] の順に選択します。

   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。

  e. これにより、［**Web プラグイン設定**］ウィンドウが開きます。

  > Kaspersky Security Center Web コンソール 14.2 では、［**Web プラグイン設定**］ウィンドウを開くにはブラウザーページを更新する必要があります。

  f. 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。

- サードパーティのソースから Web プラグインをインストールする場合（Web プラグインのインストールに要求される圧縮ファイルは、配布キットに含まれているか、カスペルスキーの Web サイトからダウンロードできます）：

  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。

  e. これにより、［**Web プラグイン設定**］ウィンドウが開きます。

  > Kaspersky Security Center Web コンソール 14.2 では、［**Web プラグイン設定**］ウィンドウを開くにはブラウザーページを更新する必要があります。

  f. 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 管理 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のと同じデバイスにインストールする必要があります。

Kaspersky Endpoint Security MMC 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にあるインストール済み MMC 管理プラグインのリストに、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管理 MMC 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**管理サーバーのプロパティ**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 管理 MMC 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。

Kaspersky Security Center を使用してインストールするには、次の手順を実行します：

1. インストールパッケージの作成。

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。

本製品の初期設定は、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 設定情報ファイルで指定できます。

Kaspersky Endpoint Security を 仮想環境を保護するために Light Agent モード（Kaspersky Security for Virtualization Light Agentソリューションの一部として）または Endpoint Detection and Response Agent モードで使用する場合、本製品の初期設定を管理する必要があります。既定では、本製品は標準モードで使用されます。

Kaspersky Endpoint Security を基本モードまたは Endpoint Detection and Response Agent モードで使用する場合は、インストールパッケージの作成時に次の内容を追加できます：

- インストール中にアプリケーションを自動的にアクティベートするためのライセンス
- インストール後に定義データベースをアップデートする必要がないように事前にダウンロードされた製品データベース

開始手順の一環として、本製品をアクティベートし、後で定義データベースをアップデートすることもできます。

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。

2. 企業ネットワーク内のデバイスに Kaspersky Endpoint Security アプリケーションを展開します。

   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。

   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。

3. スタートガイド。

   本製品を使用する前に、本製品の初期設定を完了し、本製品を操作できるように準備する必要があります。

デバイス上でアプリケーションの初期設定が完了していない場合、そのデバイス上でアプリケーションを使用したりアップデートしたりすることはできません。

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。

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、または Endpoint Detection and Response Agent モードで使用する場合は、初期設定でアプリケーションのモードを指定する必要があります。本製品の初期設定は、作成されたインストールパッケージのプロパティの［**設定**］タブ、またはインストールパッケージに含まれる設定情報ファイルで指定できます。

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-12.4.0-<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_12.4.0-<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-12.4.0-<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-12.4.0-<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-12.4.0-<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-12.4.0-<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）

- 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インストールします：
  - kesl-gui-12.4.0-<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-12.4.0-<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-12.4.0-<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-12.4.0-<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-12.4.0-<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-12.4.0-<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追加しないことで、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。

グラフィカルインターフェイスをインストールする予定がない場合は、作成済みの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、該当する設定（`USE_GUI=No`）を編集して無効にします。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さまざまな OS やパッケージマネージャーで使用する場合は、必要なすべての種類の OS とパッケージマネージャーのファイルをディレクトリに配置します。

3. Kaspersky Endpoint Security を標準モードで使用する予定で、事前にダウンロードした製品データベースを使用する場合は、次の手順を実行します：

   a. すべての OS タイプ用の定義データベースを含む準備した圧縮ファイルをフォルダーに配置します。

   b. 初期構成設定では、製品のインストール後に定義データベースのアップデートタスクを無効にします。作成済みの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（`UPDATE_EXECUTE=No`）で、該当する設定を設定できます。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。

4. 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。

   Kaspersky Endpoint Security を 仮想環境を保護するために Light Agent モードで使用する場合は、autoinstall.ini 設定情報ファイルで `KSVLA_MODE=Yes` を設定する必要があります。

   Kaspersky Endpoint Security を Endpoint Detection and Response Agent モードで使用する場合は、autoinstall.ini 設定情報ファイルで `ENDPOINT_AGENT_MODE=Yes` を設定する必要があります。

autoinstall.ini ファイルの設定値では大文字と小文字が区別されます。

後で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、初期設定を管理することもできます。

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。

3. インストールパッケージの作成に使用する方法を選択します。

   - **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. 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全体的に理解して同意することを確認します。

6. ウィザードを終了します。
   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。

7. 必要に応じて、初期設定を管理します。このためには、インストールパッケージのプロパティを開き、［**設定**］タブに移動します。

Kaspersky Security Center Web コンソールの 14.2 以前のバージョンでは、Kaspersky Endpoint Security インストールパッケージのプロパティでの初期構成設定の提供には対応していません。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。

Web コンソールでの初期設定

Kaspersky Security Center Web コンソールでは、インストールパッケージのプロパティの［**設定**］タブで、Kaspersky Endpoint Security の初期設定を指定できます。作成されたインストールパッケージは、Web コンソールのメインウィンドウの次のいずれかのセクションで利用できます：

- ［**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**］。

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、本製品の初期設定を実行することもできます。

初期設定

設定	説明
KSC のイベントの言語	Kaspersky Security Center に送信される製品イベントのローカリゼーション言語選びます。 • **システム**（既定） は OS のロケールを使用します。 本製品が OS のロケールを検知できない場合、またはこのロケールに対応していない場合は、イベントの言語化に英語が使用されます。 • Kaspersky Endpoint Security が対応している言語の 1 つ。 本製品は UTF-8 エンコードを使用します。 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 環境変数から引用されます。本製品がこのローカリゼーションに対応していない場合は、既定で英語のローカリゼーションが適用されます。
アプリケーションのアクティベーション	インストール中にアプリケーションをアクティベートする場合は、このチェックボックスをオンにします。表示されたフィールドにアクティベーションコードを入力します。既定では、このチェックボックスはオフです。 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	定義データベースと機能のアップデート元を選択します： • **カスペルスキーのアップデートサーバー**（既定）。 • **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**。このオプションを選択した場合は、開いたフィールドにアップデート元のアドレスを入力します。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されている場合にのみ適用されます。

設定	説明
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する	このチェックボックスをオンにすると、本製品のインストール後に、定義データベースと機能のアップデートタスクが開始されます。既定では、このチェックボックスはオンです。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されている場合にのみ適用されます。
プロキシサーバーの設定を指定する	インターネットアクセスにプロキシサーバーを使用する場合は、このチェックボックスをオンにします。表示されたフィールドに、次のいずれかの形式でプロキシサーバーのアドレスを入力します。 • `[<connection protocol>://]<IP address of the proxy server>:<port>` - プロキシサーバーへの接続に認証が不要な場合。 • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>` - プロキシサーバーへの接続に認証が必要な場合。 HTTPS 経由のプロキシサーバーへの接続には対応していません。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されている場合にのみ適用されます。
カーネルソースコードをインストールする	このチェックボックスをオンにすると、ファイル脅威対策が起動され、fanotify に対応していない OS でカーネルモジュールのコンパイルが自動的に開始します。既定では、このチェックボックスはオンです。
グラフィカルユーザーインターフェースを使用します	本製品のグラフィカルインターフェイスをインストールして使用する場合は、このチェックボックスをオンにします。グラフィカルインターフェイスをインストールするためのファイルをインストールパッケージに追加する必要があります。既定では、このチェックボックスはオフです。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されている場合にのみ適用されます。
admin ロールでユーザーを指定	管理者ロールを割り当てるユーザーを指定するには、このチェックボックスをオンにします。管理者ロールでは、 sudo コマンドを使用せずに、本製品のグラフィカルインターフェイスとコマンドラインで製品設定とタスク設定を管理できます。 表示されたフィールドにユーザー名を入力します。
自動的に SELinux を設定	このチェックボックスをオンにすると、SELinux は Kaspersky Endpoint Security と連携するように自動的に設定されます。既定では、このチェックボックスはオンです。
権限付きグループからユーザーを削除する	本製品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自動的に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。既定では、このチェックボックスはオフです。 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。
インストール後、アプリケーションの初回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する	インストールプロセスの完了後、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実行する場合は、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状態でのインストールは、たとえば、本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場合に便利です。 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。
インストール後に本製品を初めて起動したときにトレースファイルを作成します。	インストール後に初めて本製品を起動したときにトレースファイルを作成する場合は、チェックボックスをオンにします。 トレースを作成するために、/var/ ログ /kaspersky/kesl/ ディレクトリにログファイルが自動的に作成されます。このファイルには、通常のアプリケーショントレースファイルのサイズ制限は適用されません。トレースは5分後、またはファイル脅威対策タスクの開始後に停止します。

設定	説明
アプリケーションモード	アプリケーションのモードを選択します。 • **ワークステーションとサーバーを保護する標準モード**（既定）。このオプションを選択すると、アプリケーションは Linux ワークステーションとサーバーを保護するためのスタンドアロンアプリケーションとして使用されます。 • **Endpoint Detection and Response Agent**。このオプションを選択すると、アプリケーションは保護対象デバイス上でサードパーティのアンチウイルスソリューションと連携して動作する Kaspersky Detection and Response ソリューションをサポートするために使用されます。 • **仮想環境を保護するための Light Agent**。このオプションを選択すると、本製品は仮想環境保護用 Light Agent モードで使用されます（Kaspersky Security for Virtualization Light Agent の一部として）。
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。既定では、このチェックボックスはオフです。 この設定は、本製品が Light Agent モードで使用されている場合にのみ適用されます。
保護対象仮想マシンをサーバーとして使用	本製品がインストールされる仮想マシンのロールは サーバーまたはワークステーションです。既定では、このチェックボックスはオンになっています（仮想マシンは仮想インフラストラクチャでサーバーとして使用されます）。 この設定は、本製品が Light Agent モードで使用されている場合にのみ適用されます。
インターセプターメカニズム	本製品が使用するシステムイベントインターセプターメカニズムを選択します。 • **Fanotify テクノロジー**（既定）。このオプションを選択すると、本製品はシステムイベントインターセプターのために fanotify テクノロジーを使用します。 • **アップデート可能なカーネルモジュール**。このオプションを選択すると、本製品のインストール中にアップデート可能なカーネルモジュールがインストールされます。本製品はこのモジュールを使用してシステムイベントを読み取ります。 この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。
アップデート可能なカーネルモジュールが起動に失敗した場合	アップデート可能なカーネルモジュールの起動に失敗した場合、本製品が実行する処理を選択します。 • **fanotify を使用**（既定）。このオプションを選択すると、本製品はシステムイベントインターセプターのために fanotify テクノロジーに切り替わります。 • **システムイベントインターセプターを無効にする**。本製品がシステムイベントインターセプターを使用しない場合、リアルタイムスキャンは実行されず、デバイスの保護レベルが低下します。 このオプションは、**アップデート可能なカーネルモジュール**インターセプターメカニズムが選択されている場合に使用できます。 この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイス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。

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、または Endpoint Detection and Response Agent モードで使用する場合は、初期設定でアプリケーションのモードを指定する必要があります。初期構成設定は、インストールパッケージの作成時、または作成されたインストールパッケージのプロパティの［**設定**］セクション、およびインストールパッケージに含まれる設定情報ファイルで指定できます。

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-12.4.0-<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_12.4.0-<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-12.4.0-<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-12.4.0-<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-12.4.0-<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-12.4.0-<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）
   - 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インストールします：
     - kesl-gui-12.4.0-<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-12.4.0-<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-12.4.0-<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-12.4.0-<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-12.4.0-<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-12.4.0-<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追加しないことで、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。

グラフィカルインターフェイスをインストールする予定がない場合は、インストールパッケージの作成時、作成済みの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、該当する設定（`USE_GUI=No`）を編集して無効にします。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さまざまな OS やパッケージマネージャーで使用する場合は、必要なすべての種類の OS とパッケージマネージャーのファイルをディレクトリに配置します。

3. Kaspersky Endpoint Security を標準モードで使用する予定で、事前にダウンロードした製品データベースを使用する場合は、次の手順を実行します：

   a. すべての OS タイプ用の定義データベースを含む準備した圧縮ファイルをフォルダーに配置します。

   b. 初期構成設定では、製品のインストール後に定義データベースのアップデートタスクを無効にします。インストールパッケージの作成時、作成済みの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（`UPDATE_EXECUTE=No`）で、該当する設定を編集できます。Autoinstall.ini ファイルは、アーカイブ kesl.zip を解凍したディレクトリにあります。

4. 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。

Kaspersky Endpoint Security を 仮想環境を保護するために Light Agent モードで使用する場合は、autoinstall.ini 設定情報ファイルで `KSVLA_MODE=Yes` を設定する必要があります。

Kaspersky Endpoint Security を Endpoint Detection and Response Agent モードで使用する場合は、autoinstall.ini 設定情報ファイルで `ENDPOINT_AGENT_MODE=Yes` を設定する必要があります。

autoinstall.ini ファイルの設定値では大文字と小文字が区別されます。

インストールパッケージの作成時、または作成されたインストールパッケージのプロパティの［**設定**］セクションで、初期設定を後で管理することもできます。

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. **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**ボタンをクリックします。

4. 新しいインストールパッケージの名前を指定して、ウィザードの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。

   製品名とバージョンがウィンドウに表示されます。

   ウィザードの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全体的に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。

   ウィザードの次のステップに進みます。

7. 必要に応じて、初期設定を管理します。

   後で作成したインストールパッケージのプロパティの［**設定**］セクションで、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。

8. 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。

9. ウィザードを終了します。

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。

管理コンソールでの初期設定

Kaspersky Security Center 管理コンソールでは、インストールパッケージの作成時、またはインストールパッケージのプロパティの［**設定**］セクションで、Kaspersky Endpoint Security の初期設定を指定できます。作成されたインストールパッケージは、［**追加**］→［**リモートインストール**］→［**インストールパッケージ**］フォルダーの管理コンソールツリーに保存されます。

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、本製品の初期設定を実行することもできます。

設定	説明
KSC のイベントの言語	Kaspersky Security Center に送信される製品イベントのローカリゼーション言語選びます。 • **システム**（既定） は OS のロケールを使用します。 本製品が OS のロケールを検知できない場合、またはこのロケールに対応していない場合は、既定の英語が使用されます。 • 明示的に指定された言語。 本製品は UTF-8 エンコードを使用します。 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` 環境変数から引用されます。本製品がこのローカリゼーションに対応していない場合は、既定で英語のローカリゼーションが適用されます。
アクティベーションコード	インストール中に本製品をアクティベートする場合は、アクティベーションコードを入力します。 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する	［**設定**］をクリックすると、定義データベースとソフトウェアモジュールのアップデート元を選択できるウィンドウが開きます。 • **カスペルスキーのアップデートサーバー**（既定）。 • 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**。このオプションを選択した場合は、**アドレス**フィールドにアップデート元のアドレスを入力します。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されてい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する	このチェックボックスをオンにすると、本製品のインストール後に、定義データベースと機能のアップデートタスクが開始されます。既定では、このチェックボックスはオンです。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されてい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	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： • `[<connection protocol>://]<IP address of the proxy server>:<port>` - プロキシサーバーへの接続に認証が不要な場合。 • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>` - プロキシサーバーへの接続に認証が必要な場合。 HTTPS 経由のプロキシサーバーへの接続には対応していません。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されている場合にのみ適用されます。
カーネルソースコードをインストールする	このチェックボックスをオンにすると、ファイル脅威対策が起動され、fanotify に対応していない OS でカーネルモジュールのコンパイルが自動的に開始します。既定では、このチェックボックスはオンです。

設定	説明
グラフィカルユーザーインターフェースを使用します	本製品のグラフィカルインターフェイスをインストールして使用する場合は、このチェックボックスをオンにします。グラフィカルインターフェイスをインストールするためのファイルをインストールパッケージに追加する必要があります。既定では、このチェックボックスはオフです。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されている場合にのみ適用されます。
管理者権限を持つユーザー	管理者ロールを割り当てるユーザーを入力します。管理者ロールでは、 sudo コマンドを使用せずに、本製品のグラフィカルインターフェイスとコマンドラインで製品設定とタスク設定を管理できます。
自動的に SELinux を設定	このチェックボックスをオンにすると、SELinux は Kaspersky Endpoint Security と連携するように自動的に設定されます。既定では、このチェックボックスはオンです。
権限付きグループからユーザーを削除する	本製品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自動的に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。既定では、このチェックボックスはオフです。 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。
インストール後、アプリケーションの初回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する	インストールプロセスの完了後、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実行する場合は、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状態でのインストールは、たとえば、本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場合に便利です。 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。
インストール後に本製品を初めて起動したときにトレースファイルを作成します。	インストール後に初めて本製品を起動したときにトレースファイルを作成する場合は、チェックボックスをオンにします。 トレースを作成するために、/var/ ログ /kaspersky/kesl/ ディレクトリにログファイルが自動的に作成されます。このファイルには、通常のアプリケーショントレースファイルのサイズ制限は適用されません。トレースは5分後、またはファイル脅威対策タスクの開始後に停止します。
アプリケーションモード	この設定グループには［**設定**］ボタンが含まれており、これをクリックすると［**トラフィック読み取りモード**］ウィンドウが開きます。このウィンドウでは、製品モードを選択できます。 • **ワークステーションとサーバーを保護する標準モード**（既定）。このオプションを選択すると、アプリケーションは Linux ワークステーションとサーバーを保護するためのスタンドアロンアプリケーションとして使用されます。 • **Endpoint Detection and Response Agent**。このオプションを選択すると、アプリケーションは保護対象デバイス上でサードパーティのアンチウイルスソリューションと連携して動作する Kaspersky Detection and Response ソリューションをサポートするために使用されます。 • **仮想環境を保護するための Light Agent**。このオプションを選択すると、本製品は仮想環境保護用 Light Agent モードで使用されます（Kaspersky Security for Virtualization Light Agent の一部として）。
保護対象仮想マシンをサーバーとして使用 （［**アプリケーションモード**］ウィンドウ）	本製品がインストールされる仮想マシンのロールは サーバーまたはワークステーションです。既定では、このチェックボックスはオンになっています（仮想マシンは仮想インフラストラクチャでサーバーとして使用されます）。 この設定は、本製品が Light Agent モードで使用されている場合にのみ適用されます。
VDI 保護モードを有効にする （［**アプリケーションモード**］ウィンドウ）	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。既定では、このチェックボックスはオフです。 この設定は、本製品が Light Agent モードで使用されている場合にのみ適用されます。

設定	説明
システムイベントインターセプター	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、［**システムイベントインターセプターの設定**］ウィンドウが表示されます。このウィンドウでは、本製品で使用するシステムイベントインターセプターのモードを選択できます。 • **Fanotify テクノロジー**（既定）。このオプションを選択すると、本製品はシステムイベントインターセプターのために fanotify テクノロジーを使用します。 • **アップデート可能なカーネルモジュール**。このオプションを選択すると、本製品のインストール中にアップデート可能なカーネルモジュールがインストールされます。本製品はこのモジュールを使用してシステムイベントを読み取ります。 この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。
アップデート可能なカーネルモジュールが起動に失敗した場合 （［**システムイベントインターセプターの設定**］ウィンドウ）。	アップデート可能なカーネルモジュールの起動に失敗した場合、本製品が実行する処理を選択します。 • **fanotify を使用**（既定）。このオプションを選択すると、本製品はシステムイベントインターセプターのために fanotify テクノロジーに切り替わります。 • **システムイベントインターセプターを無効にする**。本製品がシステムイベントインターセプターを使用しない場合、リアルタイムスキャンは実行されず、デバイスの保護レベルが低下します。 このオプションは、**アップデート可能なカーネルモジュール**インターセプターメカニズムが選択されている場合に使用できます。 この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。

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

リモートインストール用のインストールパッケージを作成し、事前にダウンロードした製品データベースをそこに含めることができます。これは、たとえば、Astra Linux Special Edition OS を搭載したデバイスに本製品をインストールする場合に役立ちます。統合データベースを含むインストールパッケージを使用している場合、本製品は定義データベースと共にインストールされます。この場合、インストール直後に定義データベースをアップデートする必要はありません。

本製品をインストールするための定義データベースを含むアーカイブを作成するには、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。製品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 Update 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 *Update* 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。

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。

設定値では、大文字と小文字が区別されます。

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 Light Agent モードでの使用。	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 は標準モードまたは Endpoint Detection and Response Agent モードで使用されます（ENDPOINT_AGENT_MODE 設定を参照）。
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、本製品が 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。 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、本製品が 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 – 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。
ENDPOINT_AGENT_MODE	Endpoint Detection and Response Agent モードでの Kaspersky Endpoint Security の使用	Yes - セキュアなデバイス上でサードパーティのアンチウイルスソリューションと連携する Kaspersky Detection and Response ソリューションに対応するために、Kaspersky Endpoint Security が Endpoint Detection and Response Agent モードで使用されています。 No（既定値）- Kaspersky Endpoint Security は標準モードまたは Light Agent モードで使用されます（KSVLA_MODE 設定を参照）。
EULA_AGREED	必須の設定。 使用許諾契約書の条項に同意する。	Yes（既定）– 使用許諾契約書の利用規約に同意します。 No – 使用許諾契約書の利用規約に同意しません。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）– プライバシーポリシーの利用規約に同意します。 No – プライバシーポリシーの規約に同意しません。製品のインストールが中断されます。

設定	説明	値
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。 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。	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 に関する声明の条項に同意しません。KSN をオプトアウトしても、アプリケーションのインストール プロセスは中止されません。
GROUP_CLEAN	必須の設定。 本製品をインストールする前に、kesladmin および keslaudit 特権グループからユーザーを自動的に削除します。	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。 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 環境変数から引用されます。本製品がこのローカリゼーションに対応していない場合は、既定で英語のローカリゼーションが適用されます。	RFC 3066 形式のロケール。可能な値： • de_DE.UTF-8 – ドイツ語 • en_US.UTF-8 – 英語 • fr_FR.UTF-8 – フランス語 • ja_JP.UTF-8 – 日本語 • ru_RU.UTF-8 – ロシア語 • zh_TW.UTF-8 – 中国語（繁体字） • zh_CN.UTF-8 – 中国語（簡体字） 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。 本製品が OS のロケールを検知できない場合、またはこのロケールに対応していない場合は、イベントのローカライズに英語（RFC 3066 形式の en_US.UTF-8）が使用されます。
INSTALL_LICENSE	本製品にライセンスを追加するためのアクティベーションコード。 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。	<**アクティベーションコード**> インストール中に本製品をアクティベートする場合。 インストール中に本製品をアクティベートしない場合は None を選択します。例えば、インターネットにアクセスできない分離されたネットワークセグメントに本製品をインストールする場合などです。
UPDATER_SOURCE	定義データベースと機能のソースをアップデートします。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されてい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** >。

設定	説明	値
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。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されている場合にのみ適用されます。	次のいずれかの形式でのプロキシサーバーのアドレス： • `[<connection protocol>://]<IP address of the proxy server>:<port>` - プロキシサーバーへの接続に認証が不要な場合。 • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>` - プロキシサーバーへの接続に認証が必要な場合。 HTTPS 経由のプロキシサーバーへの接続には対応していません。
UPDATE_EXECUTE	初期構成中に製品データベースアップデートタスクを開始します。 本製品がスタンドアロンモードまたは Endpoint Detection and Response 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）– 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	fanotify テクノロジーに対応していない OS でファイル脅威対策タスクが開始されたときに、カーネルモジュールのコンパイルを自動的に開始します。	`Yes`（既定）– 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ません。
USE_GUI	アプリケーションのグラフィカルインターフェイスをインストールして使用します。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されている場合にのみ適用されます。	`Yes` – 本製品のグラフィカルインターフェイスをインストールして使用します（グラフィカルインターフェイスをインストールするためのファイルはインストールパッケージに追加する必要があります）。 `No`（既定）– グラフィカルインターフェイスを使用しません。
ADMIN_USER	管理者ロール（admin）を割り当てられたユーザー。 管理者ロールでは、`sudo` コマンドを使用せずに、本製品のグラフィカルインターフェイスとコマンドラインで製品設定とタスク設定を管理できます。	
CONFIGURE_SELINUX	Kaspersky Endpoint Security と連携するための SELinux の自動設定。	`Yes`（既定値）– Kaspersky Endpoint Security と連携するよう SELinux を自動設定します。 `No` – SELinux の自動設定を実行しません。
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。

設定	説明	値
INTERCEPTOR_MODE	Kaspersky Endpoint Security が使用するシステムイベントインターセプターメカニズム： この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。	`UseFanotify`（既定）– fanotify テクノロジーを使用してシステムイベントを遮断します。 `UseUpdatableKernelModule` – 更新可能なカーネルモジュールを使用してシステムイベントを遮断します。
INTERCEPTOR_FALLBACK_STRATEGY	アップデート可能なカーネルモジュールの起動に失敗した場合のアプリケーションの処理。 この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。	`FallbackToFanotify`（既定）– システムイベントの遮断のために fanotify に切り替えます。 `FallbackToLimitedMode` – システムイベントの遮断を使用しません。その結果、リアルタイムスキャンが実行されず、デバイスの保護レベルが低下します。
INTERCEPTOR_APPLY_STRATEGY	本製品がアップデート可能なカーネルモジュールの使用に切り替えた場合、モジュールを起動するには本製品を再起動する必要があります。この設定では、本製品を自動的に再起動するか、手動で再起動するかを指定できます。 この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。	`RestartServiceAutomatically`（既定値）は、アップデート可能なカーネルモジュールを起動するために本製品を自動的に再起動します。 `RestartServiceManually` は、ユーザーが本製品を手動で再起動した後に、アップデート可能なカーネルモジュールを起動します。 更新可能なカーネルモジュールの使用に切り替えるには、本製品を自動的に再起動することを推奨します。本製品を再起動した後、更新可能なカーネルモジュールを手動で起動すると、アプリケーションエラーが発生する可能性があります。
ENABLE_TRACES_ON_FIRST_STARTUP	インストール後に本製品を初めて起動したときにトレースファイルを作成します。 トレースを作成するために、/var/ ログ /kaspersky/kesl/ ディレクトリにログファイルが自動的に作成されます。このファイルには、通常のアプリケーショントレースファイルのサイズ制限は適用されません。トレースは5分後、またはファイル脅威対策タスクの開始後に停止します。	`Yes` - インストール後、本製品を初めて起動したときにトレースファイルを作成します。 `No` - 本製品の初めて起動したときにトレースファイルを作成しません。

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にスペースは入れません）。

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：

1. アプリケーションのインストールパッケージに追加されたライセンスを使用してアクティベーションが実行されなかった場合は、アプリケーション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 のライセンスストレージから、ライセンスをデバイスへ配信します。

2. 事前にダウンロードした製品データベースを本製品のインストールパッケージに追加しなかった場合は、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 管理 Web 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 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。

3. Kaspersky Security Center 管理コンソール（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）または Web コンソールを使用して、アプリケーションを一元管理するためのポリシーを設定します。このタスクは、管理 MMC プラグインまたは Kaspersky Endpoint Security 管理 Web 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る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。ポリシーを管理するには、管理コンソール（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）または Web コンソールを使用できます。

   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。Kaspersky Security Center を使用するか、保護対象仮想マシンのコマンドラインで、ソリューションの一部として Kaspersky Endpoint Security アプリケーションによって使用されるライセンスに関する情報をリモートで表示できます。

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 コンソールのポリシーおよびアプリケーション管理タスクを使用してアプリケーションを設定することもできます。

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

コマンドラインを使用して、クライアントデバイスに Kaspersky Endpoint Security アプリケーションをインストールできます。

コマンドラインを使用したインストールには、次の手順が含まれます：

1. アプリケーションとグラフィカルインターフェイスをインストールします。Kaspersky Endpoint Security を使用するモードに応じて、次のインストールオプションを選択できます：
   - Kaspersky Endpoint Security を基本モードで使用する場合、次のことが可能です：
     - アプリケーションをインストール（グラフィカルインターフェイスあり）します。
     - アプリケーションをインストール（グラフィカルユーザーインターフェイスなし）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。

- Kaspersky Endpoint Security を Light Agent モードで使用する場合は、グラフィカルインターフェイスなしでアプリケーションをインストールする必要があります。グラフィカルインターフェイスには対応していません。

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、インストールに dpkg 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）を使用する必要があります。

2. アプリケーションの初期設定

   アプリケーションを操作できるように準備し、クライアントデバイスの保護を有効にするには、初期設定が必要です。

   デバイス上でアプリケーションの初期設定が完了していない場合、そのデバイス上でアプリケーションを使用したりアップデートしたりすることはできません。

   本製品の初期設定は、Kaspersky Endpoint Security の配布キットから初期セットアップウィザードを使用することで実行されます。本製品の初期設定は、対話モードまたは自動モードで実行できます。

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

アプリケーションのインストール（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-12.4.0-<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-12.4.0-<ビルド番号>.x86_64.rpm
```

Kaspersky Endpoint Security を RPM パッケージから 64 ビットの ALT 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-12.4.0-<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-12.4.0-<ビルド番号>.aarch64.rpm
```

Kaspersky Endpoint Security を RPM パッケージから Arm アーキテクチャ用の 64 ビットの ALT 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-12.4.0-<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_12.4.0-<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_12.4.0-<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_12.4.0-<ビルド番号>_arm64.deb
```

アプリケーションのグラフィカルインターフェイスのインストール

グラフィカル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-12.4.0-<ビルド番号>.i386.rpm
```

グラフィカル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-12.4.0-<ビルド番号>.x86_64.rpm
```

グラフィカルインターフェイスを RPM パッケージから 64 ビットの ALT 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-12.4.0-<ビルド番号>.x86_64.rpm
```

グラフィカル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-12.4.0-<ビルド番号>.aarch64.rpm
```

グラフィカルインターフェイスを RPM パッケージから Arm アーキテクチャ用の 64 ビットの ALT 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-12.4.0-<ビルド番号>.aarch64.rpm
```

グラフィカル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_12.4.0-<ビルド番号>_i386.deb
```

グラフィカル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_12.4.0-<ビルド番号>_amd64.deb
```

グラフィカル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_12.4.0-<ビルド番号>_arm64.deb
```

対話モードでの製品のインストール後の設定

本製品の初期設定を対話モードで実行するには、Kaspersky Endpoint Security の初期セットアップウィザードを実行する必要があります。

初期セットアップウィザードは root として実行する必要があります。

初期セットアップウィザードを実行するには、次のコマンドを実行します：

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

ウィザードにより、Kaspersky Endpoint Security の設定値の段階的な入力が要求されます。ウィザードが終了し、コンソールが解放されると、インストール後の設定が完了したことが示されます。

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 0 を返す場合、アプリケーションのインストール後の設定は正常に完了しています。

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。

標準モードまたは Light Agent モードの選択

この手順では、Kaspersky Security for Virtualization Light Agent ソリューションのコンポーネントとして仮想環境を保護するために、Kaspersky Endpoint Security を Light Agent モードで使用するかどうかを指定します。

- Kaspersky Endpoint Security を Live Agent モードで使用したい場合は、 yes を入力してください。
- ワークステーションやサーバーを保護するためのスタンドアロンアプリケーションとして Kaspersky Endpoint Security を標準モードで使用する場合は、 no と入力します。

  アプリケーションを Endpoint Detection and Response Agent モードで使用する場合も、この手順で no と入力する必要があります。次の手順で Endpoint Detection and Response Agent モードを選択できるようになります。

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。

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。

モードの選択：標準モードまたは Endpoint Detection and Response Agent

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。本製品では、Light Agent モードおよび Endpoint Detection and Response Agent モードを同時に使用することはできません。

この手順では、Kaspersky Endpoint Security を Endpoint Detection and Response Agent モードで使用するかどうかを指定します：

- 保護対象デバイス上でサードパーティのアンチウイルスソリューションと連携して動作する Kaspersky Detection and Response ソリューションに対応するアプリケーションとして、Kaspersky Endpoint Security を Endpoint Detection and Response Agent モードで使用する場合は、 yes と入力します。
- ワークステーションやサーバーを保護するためのスタンドアロンアプリケーションとして Kaspersky Endpoint Security を標準モードで使用する場合は、 no と入力します。

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。

ロケールの選択

このステップでは、対応ロケールのリストが RFC 3066 形式で表示されます。

ここに記載されているロケールを指定します。このロケールは次の目的で使用されます。

- インストール中に表示される使用許諾契約書、プライバシーポリシー、およびKaspersky Security Network に関する声明のテキストのローカライズ。
- Kaspersky Security Center に送信される製品イベントのローカライズ。

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 環境変数から引用されます。本製品がこのローカリゼーションに対応していない場合は、既定で英語のローカリゼーションが適用されます。

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。

表示モードを終了したら、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かった場合、Kaspersky Endpoint Security の設定プロセスは中止されます。

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。

表示モードを終了したら、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利用規約に同意しなかった場合、Kaspersky Endpoint Security の設定プロセスは中止されます。

Kaspersky Security Network の使用

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。これにより、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。sudo コマンドを使用せずに、本製品のグラフィカルインターフェイスとコマンドラインで製品設定とタスク設定を管理するには、管理者ロールが必要です。

初期設定が完了したら、後でユーザーに管理者ロールを割り当てることができます。

システムイベントインターセプターメカニズムの設定

このステップでは、さまざまなシステムイベントインターセプターメカニズムを使用する可能性を判断します。デバイスのオペレーティングシステムが fanotify 技術をサポートしている場合は、本製品が使用するシステムイベントを読み取る方法を選択できます。

- アップデート可能なカーネルモジュールを使用する場合は、 yes と入力します。
- fanotify を使用する場合は no と入力します。

OS がアップデート可能なカーネルモジュールのインストール要件を満たしている場合、本製品はアップデート可能なカーネルモジュールに基づくインターセプターメカニズムを使用できます。デバイスの OS が fanotify に対応しているが、更新可能なカーネルモジュールをインストールする要件を満たしていない場合、本製品は fanotify を使用してシステムイベントを読み取ります。

インターセプターメカニズムとしてアップデート可能なカーネルモジュールを選択する場合は、次の設定を指定します：

- アップデート可能なカーネルモジュールの起動に失敗した場合のアプリケーションの処理：
  - アップデート可能なカーネルモジュールの起動に失敗した場合、本製品がシステムイベントインターセプターのために fanotify にフォールバックするようにするには、yes と入力します。
  - アップデート可能なカーネルモジュールの起動に失敗した場合、システムイベントを読み取らずに本製品の実行を継続するには、no と入力します。

    本製品がシステムイベントインターセプターを使用しない場合、リアルタイムスキャンは実行されず、デバイスの保護レベルが低下します。

- アップデート可能なカーネルモジュールの使用に切り替えるときの製品再起動モード。モジュールを実行するには、本製品を自動または手動で再起動する必要があります。

  更新可能なカーネルモジュールの使用に切り替えるには、本製品を自動的に再起動することを推奨します。本製品を再起動した後、更新可能なカーネルモジュールを手動で起動すると、アプリケーションエラーが発生する可能性があります。

  モジュールを実行するために本製品を自動的に再起動できるようにする場合は、yes と入力します。

デバイスの OS が fanotify に対応していない場合、本製品はファイル脅威対策のカーネルモジュールを使用します。すべての依存関係が利用可能な場合、ファイル脅威対策の起動時にカーネルモジュールのコンパイルが自動的に開始されます。

デバイス上で依存関係が見つからない場合、Kaspersky Endpoint Security 製品は関連するパッケージのインストールを提案します。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。

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、SELinux のアクセス制御システムの自動設定を有効にし、Kaspersky Endpoint Security と連携させることができます。

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（たとえば、semanage ユーティリティが存在しない場合など）、本製品はエラーメッセージを表示し、ユーザーに SELinux を手動で設定するよう促します。

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。

本製品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、ウィザードの最初のステップで Kaspersky Endpoint Security を標準モードまたは Endpoint Detection and Response Agent モードで使用することを選択した場合にのみ表示されます。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、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元を指定する必要があります。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。

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。
- ［Custom］- 本製品はカスタムソースから更新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。

プロキシサーバーの設定

このステップは、ウィザードの最初のステップで Kaspersky Endpoint Security を標準モードまたは Endpoint Detection and Response Agent モードで使用することを選択した場合にのみ表示されます。

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、次の処理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：
  - **<接続プロトコル>://<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）
  - **<接続プロトコル>://<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）

    HTTPS 経由のプロキシサーバーへの接続には対応していません。

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。

- 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。

初期設定が完了したら、後でプロキシサーバーの設定を管理できます。

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、ウィザードの最初のステップで Kaspersky Endpoint Security を標準モードまたは Endpoint Detection and Response Agent モードで使用することを選択した場合にのみ表示されます。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、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。

初期設定を完了後、アップデートタスクを後で実行できます。

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、ウィザードの最初のステップで Kaspersky Endpoint Security を標準モードまたは Endpoint Detection and Response Agent モードで使用することを選択した場合にのみ表示されます。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、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。

製品のアクティベーション

このステップは、ウィザードの最初の手順で 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 Endpoint Detection and Response Agent モードで使用している場合は、アプリケーションの初期設定を完了した後、Kaspersky Endpoint Detection and Response Expert（オンプレミス）機能を有効にする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完全パスを指定します。

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。

初期設定を完了後、本製品を後で有効化できます。

自動モードでの製品のインストール後の設定

自動モードでの本製品の初期設定を実行します：

1. 初期設定を含む構成ファイルを準備します。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。

2. 設定ファイルへのパスを Kaspersky Endpoint Security アプリケーションの初期セットアップウィザードに渡します。

   初期セットアップウィザードは root として実行する必要があります。

本製品の自動初期設定を開始するには、次のコマンド：

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

< 初期設定情報ファイル > は、初期設定を含む設定情報ファイルへのパスです。

初期セットアップウィザードが終了してコンソールが使用できるようになったら、本製品のインストール後の設定は完了です。

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 0 を返す場合、アプリケーションのインストール後の設定は正常に完了しています。

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。

ウィザードが完了した後に製品モジュールを正しくアップデートするには、本製品を再起動する必要がある場合があります。`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。

インストール後の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。

設定値では、大文字と小文字が区別されます。

インストール後の設定情報ファイルの設定

設定	説明	値
KSVLA_MODE	Kaspersky Endpoint Security の Light Agent モードでの使用。	`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 は標準モードまたは Endpoint Detection and Response Agent モードで使用されます（ENDPOINT_AGENT_MODE 設定を参照）。
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、本製品が 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` – 保護対象仮想マシンを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、本製品が 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` – 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。

設定	説明	値
ENDPOINT_AGENT_MODE	Endpoint Detection and Response Agent モードでの Kaspersky Endpoint Security の使用	Yes - セキュアなデバイス上でサードパーティのアンチウイルスソリューションと連携する Kaspersky Detection and Response ソリューションに対応するために、Kaspersky Endpoint Security が Endpoint Detection and Response Agent モードで使用されています。 No - Kaspersky Endpoint Security は標準モードまたは Light Agent モードで使用されます（KSVLA_MODE 設定を参照）。
EULA_AGREED	必須の設定。 使用許諾契約書の条項に同意する。	Yes – 使用許諾契約書の利用規約に同意します。 No – 使用許諾契約書の利用規約に同意しません。アプリケーションの初期構成は中止されます。
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します。 No – プライバシーポリシーの規約に同意しません。アプリケーションの初期構成は中止されます。
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。 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。	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。KSN をオプトアウトしても、初期構成プロセスは中止されません。
GROUP_CLEAN	必須の設定。 本製品のインストール前に、［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。 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 環境変数から引用されます。本製品がこのローカリゼーションに対応していない場合は、既定で英語のローカリゼーションが適用されます。	RFC 3066 形式のロケール。可能な値： • de_DE.UTF-8 – ドイツ語 • en_US.UTF-8 – 英語 • fr_FR.UTF-8 – フランス語 • ja_JP.UTF-8 – 日本語 • ru_RU.UTF-8 – ロシア語 • zh_TW.UTF-8 – 中国語（繁体字） • zh_CN.UTF-8 – 中国語（簡体字） 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。 本製品が OS のロケールを検知できない場合、またはこのロケールに対応していない場合は、イベントのローカライズに英語（RFC 3066 形式の en_US.UTF-8）が使用されます。

設定	説明	値
INSTALL_LICENSE	本製品にライセンスを追加するための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へのパス。 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。	**<アクティベーションコード>** インストール中に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する場合。 **<ライセンス情報ファイルへの完全パス>** インストール中にライセンス情報ファイルを使用して本製品をアクティベートする場合。 インストール中に本製品をアクティベートしない場合は `None` を選択します。例えば、インターネットにアクセスできない分離されたネットワークセグメントに本製品をインストールする場合などです。
UPDATER_SOURCE	定義データベースと機能のソースをアップデートします。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されてい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。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されている場合にのみ適用されます。	次のいずれかの形式でのプロキシサーバーのアドレス： • `[<connection protocol>://]<IP address of the proxy server>:<port>` - プロキシサーバーへの接続に認証が不要な場合。 • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>` - プロキシサーバーへの接続に認証が必要な場合。 HTTPS 経由のプロキシサーバーへの接続には対応していません。
UPDATE_EXECUTE	初期構成中に製品データベースアップデートタスクを開始します。 本製品がスタンドアロンモードまたは Endpoint Detection and Response Agent モードで使用されてい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	fanotify テクノロジーに対応していない OS でファイル脅威対策タスクが開始されたときに、カーネルモジュールのコンパイルを自動的に開始します。	`Yes` – 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ません。
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` – SELinux の自動設定を実行しません。

設定	説明	値
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。 保護コンポーネントを無効にした状態でのインストールは、たとえば、本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場合に便利です。 `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。	`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。
INTERCEPTOR_MODE	Kaspersky Endpoint Security が使用するシステムイベントインターセプターメカニズム： この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。	`UseFanotify` fanotify テクノロジーを使用してシステムイベントをインターセプトします。 `UseUpdatableKernelModule` – 更新可能なカーネルモジュールを使用してシステムイベントを遮断します。
INTERCEPTOR_FALLBACK_STRATEGY	アップデート可能なカーネルモジュールの起動に失敗した場合のアプリケーションの処理。 この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。	`FallbackToFanotify` – システムイベントの遮断のために fanotify に切り替えます。 `FallbackToLimitedMode` – システムイベントの遮断を使用しません。その結果、リアルタイムスキャンが実行されず、デバイスの保護レベルが低下します。
ENABLE_TRACES_ON_FIRST_STARTUP	インストール後に本製品を初めて起動したときにトレースファイルを作成します。 トレースを作成するために、/var/ ログ /kaspersky/kesl/ ディレクトリにログファイルが自動的に作成されます。このファイルには、通常のアプリケーショントレースファイルのサイズ制限は適用されません。トレースは5分後、またはファイル脅威対策タスクの開始後に停止します。	`Yes` - インストール後、本製品を初めて起動したときにトレースファイルを作成します。 `No` - 本製品の初めて起動したときにトレースファイルを作成しません。

<設定名>=<設定値> の形式で設定値を指定します（設定名とその値の間のスペースは処理されません）。

SELinux システムの許可ルールの設定

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、**<実行ファイル>**は次を表します：

   - /var/opt/kaspersky/kesl/12.4.0.<ビルド番号>_<インストール日時>/opt/kaspersky/kesl/libexec/kesl
   - /var/opt/kaspersky/kesl/12.4.0.<ビルド番号>_<インストール日時>/opt/kaspersky/kesl/bin/kesl-control
   - /var/opt/kaspersky/kesl/12.4.0.<ビルド番号>_<インストール日時>/opt/kaspersky/kesl/libexec/kesl-gui
   - /var/opt/kaspersky/kesl/12.4.0.<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］タスクを実行するには、SELinux の追加設定が必要です。

SELinux を設定して「プロセスの開始」タスクを実行するには：

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、閉鎖ソフトウェア環境モードの 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（アップデート 1.6、1.7、1.8）の場合

Astra Linux Special Edition OS（アップデート 1.6、1.7、または 1.8）でアプリケーションを実行する場合：

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
   ```

6. オペレーティングシステムを再起動します。

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
   ```

5. オペレーティングシステムを再起動します。

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。

閉鎖ソフトウェア環境モードの ALT SP での本製品の実行

このセクションでは、ALT SP オペレーティングシステムにおいて、閉鎖ソフトウェア環境モードで本製品を起動するために、コマンドラインで実行する必要があるステップについて説明します。

ALT SP オペレーティングシステムでアプリケーションを実行する場合：

1. 次のコマンドを実行して、閉鎖ソフトウェア環境モード（有効になっている場合）を無効にします。

   ```
   integrity-remover
   ```

2. 次のコマンドを実行して、IMA ポリシーをさらに変更するための kesl グループを作成します。

   ```
   groupadd kesl
   ```

3. 次のコマンドを実行して、作成されたグループの一意の識別子 (GUID) を確認します：

   ```
   cat /etc/group | grep kesl
   ```

4. kesl グループを除外するように IMA ポリシーを編集します。次の手順に従います：

   a. 次のコマンドを実行して、ファイル /usr/share/integrity/policy をコピーします：

      ```
      cp /usr/share/integrity/policy /etc/integrity/policy
      ```

   b. 次のコマンドを実行して、テキストエディター（vim など）を使用してファイル /etc/integrity/policy を編集します：

      ```
      vim /etc/integrity/policy
      ```

   c. `dont_measure fsmagic=0xf97cff8c` 行の後（通常、`dont_measure` セクションの最後の行）に、`dont_measure fgroup=<GUID>` 行を追加します。ここで、`<GUID>` は本手順のステップ 2 で作成したグループの一意の ID です）。

   d. `dont_appraise fsmagic=0x27e0eb` 行の後（通常、`dont_appraise` セクションの最後の行）に、`dont_appraise fgroup=<GUID>` 行を追加します。ここで、`<GUID>` は本手順のステップ 2 で作成したグループの一意の ID です）。

   e. 変更内容を保存します。

5. ファイル usr/sbin/integrity-sign で、list_all_files 機能を編集し、閉鎖環境モードで実行を許可する本製品の許可リストに Kaspersky Endpoint Security を追加します。次の手順に従います：

   a. 次のコマンドを実行して、テキストエディター（vim など）を使用してファイル /usr/sbin/integrity-sign を編集します：

      ```
      vim /usr/sbin/integrity-sign
      ```

   b. list_all_files 機能を探し、機能本体の `find -P` で始まる行で、/var/opt および /opt の下にある Kaspersky Endpoint Security のディレクトリを、各ディレクトリの列挙の末尾に追加します。

   c. 変更内容を保存します。

6. Kaspersky Endpoint Security をインストールします。インストール後に製品データベースのアップデートが正しく機能することを確認するには、初期設定段階で製品データベースのアップデートの開始を拒否します（そのためには、製品データベースのアップデート手順で「no」を入力します）。

7. 次のコマンドを実行して、Kaspersky Endpoint Security のアップデート可能なコンポーネントに kesl グループおよびディレクトリ権限の継承を割り当てます：

   ```
   cd /var/opt/kaspersky/kesl/<ビルド番号_*>/var/opt/kaspersky/kesl/private
   chown -R root:kesl updates/
   find updates -type d -exec chmod g+s {} \;
   cd /opt/kaspersky/kesl/lib64
   chown -R root:kesl updatable_modules/
   find updatable_modules -type d -exec chmod g+s {} \;
   cd /var/opt/kaspersky/kesl/common/
   chown -R root:kesl temp/
   find temp -type d -exec chmod g+s {} \;
   ```

8. 次のコマンドを実行して、ネットワークエージェントのアップデート可能なコンポーネントに kesl グループとディレクトリ権限の継承を割り当てます：

   ```
   cd /var/opt/kaspersky/
   chown -R root:kesl klnagent/
   find klnagent/ -type d -exec chmod g+s {} \;
   cd /opt/kaspersky/
   chown -R root:kesl klnagent64/
   find klnagent64/ -type d -exec chmod g+s {} \;
   ```

9. 次のコマンドを使用してシステムの署名を開始し、閉鎖ソフトウェア環境モードを有効にします：

   ```
   integrity-applier -i -A
   ```

10. 次のコマンドを実行して、IMA サブシステムが有効になっていることを確認します：

    ```
    cat /proc/cmdline
    ```

    コマンドの出力には、次の行が含まれている必要があります：`lsm=integrity ima_hash=sha512 ima_appraise=enforce.`

11. 定義データベースのアップデートタスクを起動するには、次のコマンドを実行します：

    ```
    kesl-control --start 6 -W
    ```

出力に *EventType=BasesApplied* イベントが含まれている場合、定義データベースのアップデートが正しく実行されたことを意味します。

12. 次のコマンドを実行して、本製品を再起動します：

```
systemctl restart kesl
```

アプリケーションの動作のための OSnova オペレーティングシステムの設定

OSnova 2.4 の場合

以下の方法で、OSnova 2.4 オペレーティングシステムを搭載したデバイスをネットワークエージェントのリモートインストール用に備えます：

1. /etc/systemd/logind.conf ファイルを開き、`[Login]` セクションで `#KillUserProcesses=yes` 行をコメントアウトします。

2. /usr/lib/NESS/pam-user-session ファイルを開き、`#loginctl terminate-session "$XDG_SESSION_ID"` 行をコメントアウトします。

OSnova 2.4 オペレーティングシステムでアプリケーションを実行する場合：

1. /etc/NESS/systemd/kesl.service.config ファイルを開き、`NESSCTX_MODIFY=t+ADDEQUSOCK,OMIT,70,SSUID_SAVE_CTX_PERMANENT"` を設定します。

2. `systemctl daemon-reload` コマンドを実行して、サービス設定を更新します。

3. プロセスメモリとカーネルメモリのスキャンを実行する場合は、カーネル内の mprotect（または PaX）メモリ保護を無効にする必要があります。つまり、カーネルコマンドラインパラメーターに `mprotect=off` を追加します。詳細については、OSnova のヘルプを参照してください。

4. オペレーティングシステムを再起動します。

グラフィカルインターフェース（kesl-guiパッケージ）をインストールした後、以下のコマンドを root 権限でコマンドラインから実行します。

```
rm /etc/xdg/autostart/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/autostart.desktop /etc/xdg/autostart/kaspersky-kesl.desktop

rm /usr/share/applications/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/app.desktop /usr/share/applications/kaspersky-kesl.desktop

rm /usr/share/autostart/kaspersky-kesl.desktop
```

```
cp /opt/kaspersky/kesl/resource/autostart.desktop /usr/share/autostart/kaspersky-kesl.desktop

rm /usr/share/kde4/services/ServiceMenus/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/kde.desktop /usr/share/kde4/services/ServiceMenus/kaspersky-kesl.desktop

rm /usr/share/kservices5/ServiceMenus/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/kde.desktop /usr/share/kservices5/ServiceMenus/kaspersky-kesl.desktop

rm /usr/share/Thunar/sendto/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/sendto.desktop /usr/share/Thunar/sendto/kaspersky-kesl.desktop
```

OSnova 2.5.1 以降の場合

OSnova オペレーティングシステム 2.5.1 を搭載したデバイスをネットワークエージェントのリモートインストール用に備えます：

1. /usr/lib/systemd/logind.conf.d/10-enable-kill-user-processes.conf ファイルを開き、`[Login]` セクションで `#KillUserProcesses=yes` 行をコメントアウトします。
2. /usr/lib/NESS/pam-user-session ファイルを開き、`#loginctl terminate-session "$XDG_SESSION_ID"` 行をコメントアウトします。

OSnova オペレーティングシステム 2.5.1 以降でアプリケーションを実行する場合：

1. /etc/NESS/systemd/kesl.service.config ファイルを開き、`NESSCTX_MODIFY="t+ADDEQUSOCK,OMIT,OMIT_PID,SSUID_SAVE_CTX_PERMANENT"` を設定します。
2. `systemctl daemon-reload` コマンドを実行して、サービス設定を更新します。
3. /etc/sysctl.d/30-disable-ptrace.conf ファイルを開き、`kernel.yama.ptrace_scope=0.` を設定します。
4. プロセスメモリとカーネルメモリのスキャンを実行する場合は、カーネル内の mprotect（または PaX）メモリ保護を無効にする必要があります。つまり、カーネルコマンドラインパラメーターに `mprotect=off` を追加します。詳細については、OSnova のヘルプを参照してください。
5. オペレーティングシステムを再起動します。

OSnova 2.14 以降のバージョンが搭載されたデバイスに Kaspersky Endpoint Security をインストールする際、エラーが発生する場合があります。`"dpkg: error processing package kesl (--install): installed kesl package post-installation script subprocess returned error exit status 1"` これは、/etc/os-release ファイルに `SUPPORT_URL` 行が 2 つ存在するためです。本製品を正しくインストールするには、/etc/os-release ファイルにある 2 つの `SUPPORT_URL` 行のうち 1 つを削除する必要があります。

製品によるリソース消費の最適化

このセクションには、システムリソースの消費を最適化するための Kaspersky Endpoint Security の構成について、カスペルスキーのエキスパートによる推奨事項が記載されています。既定で本製品を実行すると、本製品と Kaspersky Endpoint Security で同じリソースが使用されるため、一部のデバイスのシステムパフォーマンスに影響を及ぼす可能性があります。パフォーマンスの低下を避けるため、本製品をインストールして初期設定を完了した後、このセクションの内容の手順に従って操作することを推奨します。

アプリケーションによるシステムリソースの消費を最適化するには、次の手順を推奨します：

1. **インフラストラクチャ内の各デバイスのロールに応じて、デバイスを管理グループに配置します。**

   デバイスとそれらが実行する機能のインベントリを作成し、それらの機能に基づいてデバイスを異なる管理グループに配置します。たとえば、Web サーバーを含む管理グループ、定義データベースサーバーを含む別の管理グループ、ユーザーワークステーションを含む 3 番目の管理グループなどを作成できます。

2. **一般的なサーバーロールに合わせて本製品を設定します。**

   推奨に従って、インフラストラクチャ内のロールに応じてデバイス上で本製品を設定します。

3. **パイロットデバイスのパフォーマンスを分析します。**

   各管理グループで 1 台または 2 台のパイロットデバイスを選択します。各デバイスについて、Kaspersky Endpoint Security がシステムリソースをどのように使用し、それがインストールされているアプリケーションのパフォーマンスにどのように影響するかを分析します。

4. **パフォーマンス分析の結果に基づいて、パイロットデバイス上で本製品を設定します。**

   本製品のパフォーマンスが著しく低下している場合、または Kaspersky Endpoint Security によって消費されるシステムリソースの量が OS と本製品の動作に重大な影響を与える場合は、推奨に従ってファイル脅威対策とスキャンタスクを設定してください。

   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最適化することもできます。

5. **すべてのデバイス上の本製品の設定を更新します。**

   上記の手順でパイロットデバイスのパフォーマンスが向上した場合は、同じ種類の他のデバイスでも同じ変更を行ってください。

一般的なサーバーのロールに関する推奨事項

Web サーバー

HTTPS を使用する場合、サーバーのクライアント負荷が高くなると、ウェブ脅威対策およびネットワーク脅威対策保護コンポーネントによってシステムリソースの消費量が大幅に増加することがあります。これは、アプリケーションが HTTPS トラフィックを復号化してスキャンすることによって発生します。

これらのコンポーネントの実行中にサーバーの負荷がどのように変化するかを分析します。最適なパラメータの選択や互換性の問題の解決方法については、カスペルスキーテクニカルサポートにお問い合わせください。

プロキシサーバー

プロキシサーバーまたはロードバランサーとして機能するデバイスでは、ウェブ脅威対策コンポーネントとネットワーク脅威対策コンポーネントを無効にすることを推奨します。

コンテナ化されたサーバー

コンテナ化サービスに使用されるサーバー上のウェブ脅威対策コンポーネントとネットワーク脅威対策コンポーネントを無効にすることを推奨します。コンテナ環境を保護するには、Kaspersky Container Security アプリケーションを使用できます。

デバイス上のアプリケーションパフォーマンスの分析

オブジェクトのスキャン時に、Kaspersky Endpoint Security は CPU リソース、ディスクサブシステムの入出力、および RAM を使用します。

製品によるリソース消費の詳細を表示するには、次のコマンドを実行します：

```
top -bn1|grep kesl
```

このコマンドは、システムに負荷がかかっている状態で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。

Kaspersky Endpoint Security によってシステムの速度が著しく低下する場合は、どの製品コンポーネントとタスクがシステムリソースを消費しているかを特定する必要があります。これを行うには、コマンドラインを使用してデバイス上で次の内容を確認します：

1. ファイル脅威対策タスク（OAS タイプのタスク）のリソース消費を分析します。このようにして、パフォーマンスの問題がファイル脅威対策タスクに関連しているのか、スキャンするタスク（ODS および ContainerScan タイプのタスク）に関連しているのかを確認し、関連するタスクの推奨事項に従って操作します。

2. 最も頻繁にスキャンされるオブジェクトを識別します。安全なオブジェクトとファイルをスキャンから除外することで、パフォーマンスを最適化できます。

コマンドラインでタスクのパフォーマンスを分析できます。デバイスが Kaspersky Security Center ポリシーの管理対象である場合は、調査を実行する際にローカルタスク管理を許可する必要があります。

ファイル脅威対策タスクの消費元の分析

ファイル脅威対策タスクの動作を分析します：

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. 調査中にオンデマンドスキャンタスク（ODS および ContainerScan タイプのタスク）が実行されるようにスケジュールされていないことを確認します。
   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. 次のコマンドを実行して、ODS および ContainerScan タイプのすべてのタスクのスケジュール設定を取得します：

      ```
      kesl-control --get-schedule <タスク ID / 名>
      ```

      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. `RuleType` が `Manual` 以外のすべてのタスクについては、次のコマンドを実行してスケジュールを変更します：

      ```
      kesl-control --set-schedule <タスク ID / 名> 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実行されていない場合は、次のコマンドで開始します：

   ```
   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。
6. 結果のトレースファイルを分析します。既定で、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。

   > 負荷がかかると、アプリケーションはトレースファイルに大量の情報を書き込みますが、保持されるのは各 500 MB の 10 ファイルのみなので、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解決しない場合は、ファイル脅威対策を最適化する必要がある可能性があります。

   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、問題の原因はオンデマンドスキャンタスク（ODS および Containerスキャンするタイプのタスク）である可能性が最も高くなります。つまり、これらのタスクを最適化する必要があります。
7. 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
   ```

最も頻繁にスキャンするオブジェクトの特定

最も頻繁にスキャンされたオブジェクトのリストを取得するには、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。

ルートディレクトリ / から特定の深さまでのサブディレクトリ内のオブジェクトスキャン統計を集計する必要がある場合は、コマンドに cut -d/ -f 1-X を追加します。ここで、X はネストの深さです。次に例を示します：

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | cut -d/ -f 1-4 | sort | uniq -c | sort -k1 -n -r|less
```

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取得するには、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 $10}' | 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。

ルートディレクトリ / から特定の深さまでのサブディレクトリ内のオブジェクトスキャン統計を集計する必要がある場合は、コマンドに cut -d/ -f 1-X を追加します。ここで、X はネストの深さです。次に例を示します：

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $10}' | tr -d ',' | cut -d/ -f 1-3 | sort | uniq -c | sort -k1 -n -r
```

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ことを推奨します。安全であると確認されたオブジェクトとファイルを除外リストに追加して、ファイル脅威対策とスキャンするタスクを最適化できます。たとえば、定義データベースファイル、ディレクトリ、およびログファイルは、書き込み操作が信頼するプロセスによって実行される場合、安全であると見なすことができます。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。

ファイル脅威対策とスキャンするタスクに関する推奨事項

ファイル脅威対策の最適化

ファイル脅威保護コンポーネントを最適化するには、次の操作を実行できます：

- 最も頻繁にスキャンされ、安全なオブジェクトのスキャン除外を設定します。
- ファイル操作の読み取りから除外リストを設定します。
- ファイルが開かれたときにのみファイルをスキャンするようにファイルスキャンモードを変更します。既定では、本製品は、ファイルが開こうとすると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、ファイルが閉じようとしたときに再度スキャンします。ファイル脅威対策設定でファイルをスキャンするモードを変更できます。

  - Web コンソールまたは管理コンソールを使用したポリシーで、**ファイル脅威対策モードを**［**開いた時**］に設定します。
  - 次のコマンドを使用してデバイス上でローカルに実行します：

    ```
    kesl-control --set-set 1 ScanByAccessType=Open
    ```

  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。

- 圧縮ファイルスキャンが無効になっていることを確認します（既定値）。圧縮ファイルをスキャンすると、ファイルが /tmp 一時ディレクトリに解凍されてスキャンされている間、圧縮ファイルへのアクセスがブロックされるため、パフォーマンスに影響します。圧縮ファイルの定義には、従来の圧縮ファイルだけでなく、.jar などのパッケージ化されたオブジェクトも含まれます。

  圧縮ファイルスキャンは、Web コンソールまたは管理コンソール（**アーカイブをスキャン**設定）を使用するか、デバイス上でローカルにコマンドライン（`ScanArchived`設定）を使用して有効または無効にすることができます。

- アプリケーションが使用できる RAM の量を制限します。

スキャンタスクの最適化

スキャンタスク（ODS および ContainerScan タイプのタスク）を最適化するには、次の操作を実行できます：

- スキャンタスクが重複しないようにスケジュールされたスキャンを設定します。アプリケーションではスキャンするタスクを同時に実行できますが、これによりリソースの消費量が大幅に増加する可能性があります。すべての ODS および ContainerScan タスクのスケジュールをデバイス上でローカルタスクとして、または Kaspersky Security Center で確認します。
- サーバーの負荷が最小限のときにスキャンを実行します。

- スキャンタスクの範囲に、SMB および NFS 経由でデバイスにマウントされたリモートディレクトリが含まれていないことを確認してください。このようなディレクトリは、リソースを提供するリソースプロバイダー上で直接スキャンすることを推奨します。これが不可能な場合は、重要なサービスを実行するサーバー上でスキャンを実行しないでください。このようなタスクは、接続速度とファイル数に応じて、かなり長い時間がかかる可能性があります。

- 最も頻繁にスキャンされ、安全なオブジェクトのスキャン除外を設定します。

- ファイル操作の読み取りから除外リストを設定します。

- アプリケーションが使用できる RAM の量を制限します。

ウイルススキャンの除外設定

スキャン除外は、システムのセキュリティとパフォーマンスのバランスを図るのに役立ちます。たとえば、カスペルスキーのウイルスエキスパートによると、定義データベースのデータファイルとインデックスファイルを安全に除外リストに追加できます。このようなファイルがウイルスベクターになる危険性はないと考えられています。

最も頻繁にスキャンするオブジェクトのリストから安全なオブジェクトを除外できます。

ファイルパス（マウントタイプも指定可能）、ファイルマスク、ファイル脅威の種類、およびファイル操作を実行するプロセスへのパスによって除外を設定できます。

本製品はスキャンから除外されたオブジェクトをスキャンしませんが、ファイル操作の読み取りとブロックは引き続き実行されるため、ファイル操作の遅延は最小限に抑えられます。最小限の遅延さえも防止する必要がある場合は、ファイル操作の読み取りから除外リストを設定することを推奨します。

ファイル脅威対策の除外は、Web コンソールまたは管理コンソールを使用してポリシーで設定することも、コマンドラインを使用してデバイス上でローカルに設定することもできます。

ODS および ContainerScan タイプのスキャンタスクの除外を設定することもできます。除外は、Kaspersky Security Center のタスク設定で、またはコマンドラインを使用してデバイス上でローカルに設定されます。

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。

コマンドラインでファイル脅威対策の除外を設定する例は、次の通りです。

/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
```

ファイル操作の読み取りの除外リストの設定

スキャンから除外されたファイルでも、ファイル脅威対策およびスキャンタスク中にアプリケーションによって読み取られる可能性があります。アプリケーションはファイル操作イベントを読み取り、イベントが処理されるまで処理をブロックします。スキャン後、本製品でできる操作は次の通りです：

- ブロックを解除してオペレーターの操作を許可する。
- オペレーターをブロックし、保護または検証設定で指定された処理を実行する。

イベントの読み取りには時間がかかり、他のアプリケーションや OS のパフォーマンスに影響します。

次のコマンドを使用して、ファイル読み取りの統計を取得できます。

```
kesl-control --get-statistic --files
```

このコマンドを使用すると、過去 24 時間のファイル操作読み取りの統計を表示できます。

必要に応じて、本製品のトレースファイルを使用してより詳細な分析を行うことができます。既定では、本製品はトレースファイルを生成しません。次のコマンドを使用してトレースを有効にできます：

```
kesl-control --set-app-settings TraceLevel=Detailed
```

> トレースを有効にすると、システム全体のパフォーマンスに影響する可能性があります。トレースファイルが不要になった場合は、トレースを無効にすることを推奨します。

次のコマンドを使用してトレースを無効にすることができます：

```
kesl-control --set-app-settings TraceLevel=None
```

トレースファイルを分析することで、アプリケーションによって読み取られたファイルのリストを取得し、多数のファイル操作の読み取りに関連付けられたパスを特定できます。次のコマンドを実行すると、読み取られたファイルのリストを取得できます：

```
grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print $2}'|sort | uniq -c | sort -k1 -n -r
```

ルートディレクトリ / から特定の深さまでのサブディレクトリ内のファイル操作の読み取り統計を集計する必要がある場合は、コマンドに `cut -d/ -f 1-X` を追加します。ここで、X はネストの深さです。次に例を示します：

```
grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print $2}'| cut -d/ -f 1-3|sort | uniq -c | sort -k1 -n -r|less
```

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読み取りからも除外する場合は、マウントポイント全体を除外する必要があります。マウントポイントを除外（グローバル除外）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読み取りから除外できます。

グローバル除外はマウントポイントではないパスには影響しません。

カスペルスキーのエキスパートは、次のような場合にグローバル除外を使用することを推奨しています：

- NFS や SMB などのマウントされたリモートリソースへの接続が遅い場合。
- たとえわずかな遅れであっても許容されない場合。

共有ネットワークリソースを保護するには、リソースが物理的に保存されているデバイスで Kaspersky Endpoint Security 製品を使用します。

グローバル除外は、Web コンソールまたは管理コンソールを使用してポリシー内で設定することも、コマンドラインを使用してデバイス上でローカルに設定することもできます。

コマンドラインを使用したファイル操作の読み取りの除外リストの設定例は次の通りです。

/tmp ディレクトリ内のすべてのファイルを読み取りから除外する場合：

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）。

製品のメモリ使用制限の設定

ファイル脅威対策コンポーネントを使用してファイルをスキャンするとき、および ODS および ContainerScan タイプのスキャンタスクを実行するときに、Kaspersky Endpoint Security が使用する RAM の量を制限できます。

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。

既定では、アプリケーションは最大 8192 MB の RAM を使用する場合があります。アプリケーションが使用する RAM の量を調整できます：

- ポリシーでは、**スキャンのメモリ使用率を制限する（MB)** 設定を使用します。
- デバイス上でローカルに、kesl.ini 設定情報ファイルの `ScanMemoryLimit=<メガバイト単位のメモリ量>` 設定を使用します。

2 MB 未満の値を設定すると、本製品は最小値のメモリを使用します（2 MB）。指定した値がデバイスで使用可能な RAM の容量より大きい場合、アプリケーションは RAM の最大 25% を使用します。この値は変更できません。

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。

ウェブ脅威対策タスクおよびネットワーク脅威対策タスクの推奨事項

ウェブ脅威対策およびネットワーク脅威対策保護コンポーネントがアプリケーションのパフォーマンスに与える影響を軽減するには、次の手順を実行することを推奨します：

- OS のファイアウォールを設定します。システムに Drop ポリシーを含む独自のネットワークルール（または firewalld ルール）がある場合、アプリケーションが正しく動作するために、ローカルデバイスからの着信接続を許可する accept ルール（ループバック）を追加する必要があります。

  iptables のコマンド例：

  ```
  iptables -A INPUT -i lo -j ACCEPT
  ```

- REDIRECT ルール（ポート 443 から 8443 へのリダイレクトなど）とネットワーク脅威対策の保護コンポーネントの読み取りルールとの互換性を確保するには、次の手順を実行します：

  a. 次のようなルールを削除します：

  ```
  iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
  ```

  b. これを次のルールに置き換えます：

  ```
  iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400 -j REDIRECT --to-ports 8443
  ```

  ```
  iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype ! --src-type LOCAL -j DNAT --to-destination :8443
  ```

- 証明書検証ポリシーを設定します。既定では、ウェブ脅威保護コンポーネントは、暗号化された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てスキャンします。その際、コンポーネントは検証にインターネットを使用し、証明書の検証に必要な不足しているチェーンをダウンロードできます。デバイスが直接インターネットにアクセスできない場合は、ローカル証明書検証方法（インターネットを使用しない）を選択するか、インターネットアクセスにプロキシサーバーを使用する必要があります。

  ネットワークトラフィックのスキャン設定で、ローカル証明書の検証方法を選択できます：

  - Web コンソールまたは管理コンソールを使用したポリシーで、**証明書検証ポリシーを［ローカルチェック］**に設定します。
  - 次のコマンドを使用してデバイス上でローカルに実行します：

    ```
    kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
    ```

  証明書の検証にインターネットを使用しません。

  Web コンソール、管理コンソール、またはローカルのコマンドラインを使用して、ポリシー内でプロキシサーバーを設定できます。

- アプリケーションによって監視されるネットワークポートのリストを制限します。既定では、アプリケーションは選択されたネットワークポートのみを監視します。デバイスが SMB 接続を使用する場合は、既定値が使用されていることを確認してください。

  - Web コンソールまたは管理コンソールのポリシーのネットワークトラフィックのスキャン設定で、［**選択したネットワークポートのみを監視**］が選択されています。

  - デバイスのローカル：`MonitorNetworkPort` 暗号化接続のスキャン設定が`Selected`に設定されています。

本製品を HAProxy ロードバランサーと一緒に使用する場合、次の手順を実行することを推奨します：

1. /var/opt/kaspersky/kesl/common/kesl.ini 設定情報ファイルを開き、`[Environment]` セクションを作成して、`TcpSynInterceptDisabled=1` の設定を追加します。

2. 本製品を再起動します：

   ```
   systemctl restart kesl
   ```

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 Kubernetes コンテナ化と一緒に使用するには、OS のファイアウォールをさらに入念に微調整する必要があります。Cillium CNI も使用している場合、コンポーネントを Kubernetes で使用することはできません。

旧バージョンからの本製品のアップデート

Kaspersky Endpoint Security 12.3 for Linux からのみ、Kaspersky Endpoint Security 12.4 for Linux にアップグレードできます。

Kaspersky Endpoint Security の以前のバージョンからバージョン 12.4 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 12.4 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。

   > 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 を基本モードまたは Endpoint Detection and Response Agent モードで使用し、本製品のグラフィカルインターフェイスを使用している場合は、グラフィカルインターフェイスもアップデートが必要になります。

   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。

本製品をアップデートすると、以前のバージョンのイベントデータベースファイルが、現在のバージョンのファイルセットの最初のイベントファイルになります。このファイルは、残りのファイル内のイベント数が指定された最大数（`MaxEventsNumber` 設定）に達するまで保持されます。したがって、本製品が `MaxEventsNumber` 設定で指定された数の 2 倍のイベントを保存するような状況が一時的に発生する場合があります。

Kaspersky Endpoint Security を基本モードまたは Endpoint Detection and Response Agent モードで使用している場合は、本製品のアップデート後に定義データベースのアップデートタスクを開始することを推奨します。

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

以前のバージョンの Kaspersky Endpoint Security 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、MMC 管理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）。

変換されたポリシーとタスクの名前は「<Original policy/task name>（変換済み）」。

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値の一部を、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。

同じバージョンの本製品用の MMC 管理プラグインの新しいビルドをインストールする場合は、まず現在インストールされている同バージョンの MMC プラグインをアンインストールしてから、このバージョンの新しい MMC プラグインをインストールする必要があります。

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、グラフィカルインターフェイスには対応していません。

Kaspersky Security Center を使用してアップデートするには、次の手順を実行します：

1. インストールパッケージの作成。

   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。

2. 企業ネットワーク内のデバイスに Kaspersky Endpoint Security アプリケーションを展開します。

   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。

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、グラフィカルインターフェイスには対応していません。

使用許諾契約書およびプライバシーポリシーの規定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規定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。

アップグレード中に新しい契約条件に同意するには、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します：

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-12.4.0-<ビルド番号>.<arch>.rpm [kesl-gui-12.4.0-<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 タイプのパッケージマネージャーを備えた OS では、アプリケーションパッケージと GUI パッケージの両方がインストールされている場合、一方のパッケージのみをアップデートし、もう一方のパッケージをアップデートしない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_12.4.0-<ビルド番号>_<arch>.deb [./kesl-gui_12.4.0-<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 タイプのパッケージマネージャーを備えた OS では、アプリケーションパッケージと 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。

例：
64 ビットオペレーティングシステム用の *GUI パッケージを含む RPM アプリケーションパッケージをアップデートします：*

```
# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes rpm -U --replacefiles --replacepkgs kesl-12.4.0-< ビルド番号 >.x86_64.rpm kesl-gui-12.4.0-< ビルド番号 >.x86_64.rpm
```

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する場合、ポリシーとタスクを変換して、本製品の以前のバージョンで構成されたポリシーとタスク設定の値を使用できます（詳細については、Kaspersky Security Center ヘルプを参照してください）。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。

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、ほとんどの設定は以前のバージョンから引き継がれます。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。

定義データベースのアップデート元

本製品の新しいバージョンでは、定義データベースのアップデートタスクに次の変更が加えられました：

- **他のアップデート元が使用可能で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**（UseKLServersWhenUnavailable）設定が削除されました。この機能は、他のタスク設定を使用して構成できます。

- 複数のアップデート定義データベースのアップデート元を同時に指定できます。本製品は、アップデート元のリストに表示されている順序でこれらのアップデート元を使用します。

MMC プラグインでタスクを変換すると、アップデート元は次のように設定されます：

- 以前のバージョンで［**カスペルスキーのアップデートサーバー**］が選択されていた場合、アップデート元のリストで［**カスペルスキーのアップデートサーバー**］チェックボックスがオンになります。

- 以前のバージョンで［**Kaspersky Security Center**］が選択されていた場合、アップデート元のリストで［**Kaspersky Security Center**］チェックボックスがオンになります。

  ただし、以前のバージョンで［**他のアップデート元が使用可能で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**］チェックボックスが選択されていた場合、アップデート元のリストで［**カスペルスキーのアップデートサーバー**］チェックボックスもオンになり、**Kaspersky Security Center** アップデート元がリストの先頭に移動されます。

- 以前のバージョンでカスタムアップデート元（**ローカルネットワークまたはグローバルネットワーク上のその他のアップデート元**）が設定されていた場合、指定されたパラメータ（アップデート元のパスまたは URL）を持つカスタムアップデート元がアップデート元のリストに追加され、このチェックボックスがオンになります。

  ただし、以前のバージョンで［**他のアップデート元が使用可能で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**］チェックボックスが選択されていた場合、アップデート元のリストで［**カスペルスキーのアップデートサーバー**］チェックボックスもオンになり、カスタムアップデート元がリストの先頭に移動されます。

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。

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

- 以前のバージョンで SourceType が KLServers に設定されていた場合、**[Sources]** セクションに次のアップデート元が作成されます：SourceType=KLServers、Enabled=Yes。

- 以前のバージョンで SourceType が SCServer に設定されていた場合、**[Sources]** セクションに次のアップデート元が作成されます：SourceType=SCServer、Enabled=Yes。

  ただし、以前のバージョンでパラメータが UseKLServersWhenUnavailable=Yes に設定されていた場合、**[Sources]** セクションに 2 番目のアップデート元が作成されます：SourceType=KLServers、Enabled=Yes。

- 以前のバージョンで SourceType が Custom に設定され、カスタムアップデート元が **[CustomSources.item_#]** セクションで構成されていた場合、**[Sources]** セクションにカスタムアップデート元が作成されます：SourceType=Custom、URL=< **アップデート元のパスまたは**URL >、Enabled=Yes。

  ただし、以前のバージョンでパラメータが UseKLServersWhenUnavailable=Yes に設定されていた場合、**[Sources]** セクションに 2 番目のアップデート元が作成されます：SourceType=KLServers、Enabled=Yes。

システムイベントインターセプターの設定

以前のバージョンのアプリケーションで、更新可能なカーネルモジュールに基づくシステムイベント傍受メカニズムが選択されていた場合、アップデート後、アプリケーションは fanotify を使用してシステムイベントを傍受するようになります。その後、定義データベースと機能が更新され、自動的に再起動すると、アプリケーションは再び更新可能なカーネルモジュールを使用するようになります。

Kaspersky Security Network の設定

MMC プラグインでポリシーを変換した後、ポリシープロパティの Kaspersky Security Network 設定は、ポリシーとタスクのバッチ変換ウィザードで Kaspersky Security Network に関する声明の条件を承諾したか拒否したかによって異なります。

- 声明の条件に同意した場合は、［**拡張 KSN モード**］オプションが選択されます。
- 声明の条件を拒否した場合は、［**KSN 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。

コマンドラインで本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` を設定していた場合は `UseKSN` 設定が `No` に設定され、`KESL_USE_KSN=Yes` を設定していた場合は `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。

クラウドモード設定

MMC プラグインでポリシーを変換した後、クラウドモードの使用に関する設定は、ポリシーとタスクのバッチ変換ウィザードで Kaspersky Security Network に関する声明の条件を承諾したか拒否したかによって異なる場合があります。

- 声明の条件に同意した場合は、［**クラウドモードを有効にする**］チェックボックスがオンになります。
- 声明の条件を拒否した場合、［**クラウドモードを有効にする**］チェックボックスはオフになります。

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。
- アップデート後に `UseKSN=Basic/Extended` が設定され、アップデート前に `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` パラメータを `Basic` または `Extended` に設定し、`CloudMode` パラメータを `Yes` に設定します。

Kaspersky Endpoint Detection and Response (KATA) 連携設定

MDR コンポーネントが有効になっている場合、MMC プラグインでポリシーを変換した後、MDR コンポーネントのステータスは、ポリシーとタスクの変換ウィザードで Kaspersky Security Network に関する声明の条件に同意したか拒否したかによって異なります。

- 声明の条件に同意した場合、MDR コンポーネントは有効なままになります（「**Managed Detection and Responseを有効にする**」チェックボックスが選択されています）。
- ステートメントの条件を拒否した場合、「**Managed Detection and Responseを有効にする**」チェックボックスはオフになります。

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、`UseMDR` 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 `UseMDR=No` になります。
- アップデート後に `UseKSN=Basic/Extended` が設定され、アップデート前に `UseMDR=Yes` が設定されていた場合は、`UseMDR=Yes` になります。

Kaspersky Managed Detection and Response 機能を使用する場合は、 Kaspersky Security Network の拡張モードを有効にする必要があります。

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、グラフィカルインターフェイスを使用している場合は、グラフィカル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。

> 本製品を削除すると、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。アプリケーションインストールの一意のID（SensorID）も保存されます。

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 ヘルプ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削除

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。

Kaspersky Endpoint Security MMC 管理プラグインを削除する場合：

1. Kaspersky Security Center 管理コンソールを閉じます。
2. 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、Windows レジストリエディターを開き、次の場所に移動します：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins
   ```

   このライセンスには、管理コンソールにインストールされているすべての管理プラグインに関する情報が含まれています。管理対象アプリケーションの名前は **DisplayName** 値にあります。
3. Kaspersky Endpoint Security アプリケーションプラグインの該当するバージョンに対応するセクションを選択します。
4. **UninstallString** 値を開いてコピーします。
5. 管理者としてコマンドプロンプトを開き、コピーした値を貼り付けて **Enter** キーを押します。

製品のライセンス

このセクションには、カスペルスキー製品のライセンスに関連する基本的な概念に関する情報と、Kaspersky Endpoint Security のアクティベーションの詳細に関する情報が記載されています。

製品をアクティベートした後は、必要に応じてライセンスを適時にアップデートできるように、ライセンスの有効期間に注意することを推奨します。Kaspersky Security Center または保護対象デバイスのコマンドラインを使用して、Kaspersky Endpoint Security で使用されるライセンスに関する情報を表示できます。

使用許諾契約書について

*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。

使用許諾契約書と、データの処理および提供について説明しているプライバシーポリシーは、次の場所で確認できます：

- アプリケーションをインストールする前は、license.<language identifier> ファイルで確認できます。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。

- 本製品のインストール後、カスペルスキー製品の使用許諾契約書およびプライバシーポリシーの本文を含むファイルは、保護対象デバイスの /opt/kaspersky/kesl/doc/license.<language ID> ディレクトリに保存されます。

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。

次の種類のライセンスが提供されています：

- *試用版*

アプリケーションを試用するための無償ライセンスです。試用版ライセンスの有効期間は短く設定されています。

試用版ライセンスの有効期間が終了すると、すべての Kaspersky Endpoint Security 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。

- *製品版*

  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。

Kaspersky Endpoint Security アプリケーションを有効化するには、アプリケーションの基本機能を対象とするライセンスが必要です。メインライセンスには、アプリケーションの追加機能（たとえば、Kaspersky Detection and Response ソリューションとの連携機能）も含まれる場合があります。本製品に使用しているメインライセンスで必要な追加機能が対象でない場合は、追加機能を有効にするために別のライセンスを購入する必要があります。

メインライセンスと追加機能ライセンスに含まれる機能の範囲を明確にするには、ライセンスを購入するカスペルスキーパートナーにお問い合わせください。

ライセンス証明書について

ライセンスの証明書とは、ライセンス情報ファイルまたはアクティベーションコードとともに提供される文書です。

ライセンスの証明書に含まれるライセンス情報は次のとおりです：

- ライセンス ID の数値または注文番号
- ライセンスが付与されているユーザーの詳細
- ライセンスでアクティベートできる製品の詳細
- ライセンス単位の数の制限（例：ライセンスを使用してアプリケーションを使用できるデバイスの数）
- 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ライセンスの有効期間
- 種別：

ライセンスについて

*ライセンス*は、アクティベーションに使用するビットシーケンスで、使用許諾契約書の条件に従ってアプリケーションを使用します。ライセンスは、カスペルスキーにより生成されます。

本製品をアクティベートするには、メインのライセンスが必要です。本製品に使用しているメインライセンスに必要な追加機能（Kaspersky Endpoint Detection and Response Optimum 機能など）が含まれていない場合は、追加機能をアクティベートするためのライセンスも必要になります。

保護対象デバイス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。保護対象デバイス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。

ライセンスは、現在のライセンスまたは予備のライセンスとして追加できます。

- *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。現在のライセンスとして追加できるメインライセンスは1つだけです。追加機能のために、現在のライセンスを複数持つことは可能です。

- *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。

  本製品のメインライセンスの期間を延長するには、基本機能の予備のライセンスを追加できます。別のライセンスで追加機能を有効化している場合は、追加機能用の予備のライセンスを追加することもできます。

  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 文字からなる一意の英数字列です。アクティベーションコードを入力して、Kaspersky Endpoint Security をアクティベートするライセンスを追加します。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について

*ライセンス情報ファイル*は、カスペルスキーから受け取った拡張子が .key のファイルです。ライセンス情報ファイルの用途は、製品をアクティベートするライセンスを追加することです。

ライセンス情報ファイルは、Kaspersky Endpoint Security の購入後にカスペルスキーから受け取ります。

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、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。たとえば、カスペルスキーカンパニーアカウントの登録に、ライセンス情報ファイルが必要と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
- 既存のアクティベーションコードに基づき、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

月額制サービスについて

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。

月額制サービスは期限付き（たとえば1年間）とすることも、無期限（有効期限なし）とすることもできます。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 アプリケーションの利用可能な機能は、メイン ライセンスの種別によって異なります。

本製品のメインライセンスには、本製品の基本機能だけでなく追加機能も含まれる場合があります。たとえば、「Kaspersky Optimum Security」ライセンスを使用すると、主要な保護および制御コンポーネントと、Kaspersky Endpoint Detection and Response Optimum Integration 機能をアクティベートできます。

本製品の追加機能には、Kaspersky Unified Monitoring and Analysis Platform 機能をアクティベートするライセンスなど、別のライセンスを使用できます。

メインライセンスと追加機能ライセンスに含まれる機能の範囲を明確にするには、ライセンスを購入するカスペルスキーパートナーにお問い合わせください。

メインのアプリケーションライセンス対象のソリューション機能のリストを開く

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にするプロセスです。

保護対象デバイスで Kaspersky Endpoint Security アプリケーションをアクティベートするには、アプリケーションにメインライセンスを追加する必要があります。本製品に使用しているメインライセンスで必要な追加機能が対象でない場合は、Kaspersky Endpoint Security の追加機能を有効にするために別のライセンスを追加する必要があります：

- Kaspersky EDR Optimum コンポーネントを有効にするための別のライセンス「Kaspersky Endpoint Detection and Response Optimum Add-on」（以下、「EDR Optimum ライセンス」とも表記）。
- Kaspersky Unified Monitoring and Analysis Platform 機能を有効にするための別のライセンス「Kaspersky Unified Monitoring and Analysis Platform Add-on」（以下、「KUMA」とも表記）。
- Kaspersky MDR コンポーネントをアクティベートするための別のライセンス「Kaspersky Managed Detection and Response Optimum/Expert Add-on」（以下、「MDR ライセンス」とも表記）。
- EDR Expert（オンプレミス）コンポーネントをアクティベートするには、別のライセンス「Kaspersky Endpoint Detection and Response Expert（オンプレミス）アドオン」（以下、「EDR Expert（オンプレミス）ライセンス」とも表記）が必要です。

EDR Expert（オンプレミス）ライセンスは、Kaspersky Endpoint Security を Endpoint Detection and Response Agent モードでアクティベートするためにも使用されます。このモードでは、本製品にメインのライセンスを追加する必要はありません。

本製品にライセンスを追加するには、次のいずれかの方法があります：

- ライセンス情報ファイルを使用する。
- アクティベーションコードを使用する。

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、製品を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。アクティベーションは、SVM にライセンスを追加することで、Protection Server 側（Kaspersky Security for Virtualization Light Agent のコンポーネント）で実行されます。必要に応じて、追加機能をアクティベートするためのライセンスも SVM に追加します。

インストール中に Kaspersky Endpoint Security アプリケーションをアクティベートしなかった場合（インストールパッケージにライセンスを追加するか、初期設定を完了して）、インストールしたアプリケーションを次のいずれかの方法でアクティベートする必要があります：

- Kaspersky Security Center を使用してリモートでアップデートする：
  - ライセンスの追加タスクを使用する。
  - 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。
- コマンドラインで管理コマンドを使用。

本製品に追加機能のライセンスを追加するには、ライセンスの追加タスク、クライアントデバイスにライセンスを配布する手順、またはライセンス管理コマンドを使用することもできます。追加機能を提供するライセンスを追加することは、本製品のメインライセンスを追加することと変わりません。

Kaspersky Endpoint Security を標準モードで使用している場合、追加機能のライセンスは本製品のメインのライセンスを追加した後にのみ追加できます。

本製品の基本機能用の予備のライセンスと追加機能用の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。

保護対象デバイス上の Kaspersky Security Center またはコマンドラインを使用して、本製品にリモートで追加されたライセンスに関する情報を表示できます。

グラフィカルユーザーインターフェイスを使用して本製品をアクティベートし、ライセンスを管理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

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。

- 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。タスクを作成するときは、Kaspersky Security Center ライセンスストアに追加されたライセンスが使用されます。ライセンスは、事前にライセンスストアに追加することも、アクティベーション タスクを作成するときに追加することもできます。

- 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、事前に Kaspersky Security Center のライセンスストアにライセンスを追加します。

Kaspersky Security Center Web コンソールまたは Kaspersky Security Center 監理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、ライセンスストア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 Security Center Web コンソールを使用して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. タスクの設定を指定します：

   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. タスク範囲の指定方法に応じて、対象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、［**キーの追加**］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. ウィザードを終了します。
   タスクのリストに新しいタスクが表示されます。

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、本製品に*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。

アプリケーションがデバイス上でまだ有効化されていない場合、またはライセンスの有効期限が 14 日以内に切れる場合にのみ、新しいライセンスがデバイスに追加されます。

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 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操作を実行できます。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。

ライセンス管理コマンドは、本製品が標準モードまたは Endpoint Detection and Response Agent モードで実行されている場合にのみ使用できます。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/アクティベーションコードのパス>
```

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/アクティベーションコードのパス>
```

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。

add key コマンドを使用すると、アプリケーションのメインライセンスと追加機能の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。

メインライセンスと追加機能ライセンスを削除するためのさまざまなコマンドを用意しています。

現在のメイ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
```

予備のメイ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
```

現在の KUMA 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 --kuma
```

予備の KUMA 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 --kuma
```

現在の MDR 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 --mdr
```

予備の MDR 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 --mdr
```

現在の EDR Expert（オンプレミス）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-kata
```

予備の EDR Expert（オンプレミス）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-kata
```

使用済みのライセンスに関する情報の表示

Kaspersky Endpoint Security で使用されているライセンスに関する情報は、次の方法で表示できます：

- Kaspersky Security Center のライセンスの追加タスクのプロパティで。

  *ライセンスの追加タスク*のプロパティでは、このタスクによってアプリケーションに追加されるライセンスに関する情報を確認できます。

- Kaspersky Security Center で、クライアントデバイスにインストールされている関連するカスペルスキーアプリケーションのプロパティ。

  保護対象デバイス上の Kaspersky Endpoint Security アプリケーションのプロパティでは、このデバイス上のアプリケーションに追加された現在のライセンスと予備のライセンスに関する情報を確認できます。本製品のプロパティは、Web コンソールと管理コンソールを使用して表示できます。

- Kaspersky Security Center のライセンス使用状況レポート。

  ライセンスの使用状況レポートは、Web コンソール（[**監視とレポート**] → [**レポート**]）と管理コンソール（[**レポート**] タブ）を使用して表示できます。レポートを表示するには、レポートのリストで「ライセンスの使用状況に関するレポート」テンプレートを選択し、レポートの生成を開始する必要があります。

- Kaspersky Security Center の Kaspersky Security Center ライセンスストアで。

  ライセンスストアは、Web コンソール（［**操作**］→［**カスペルスキーライセンス**］）または管理コンソール（**カスペルスキーライセンス**フォルダー）を使用して開くことができます。ストアには、Kaspersky Security Center 管理サーバーに追加されたすべてのライセンスに関する情報が表示されます。

- Kaspersky Endpoint Security がインストールされているデバイス。Kaspersky Endpoint Security アプリケーションで使用されるライセンスに関する情報をコマンドラインで表示できます。

Kaspersky Security Center イベントに関する通知を使用して、使用されている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を取得することもできます。アプリケーションは、期限切れのライセンスとライセンス違反に関する情報をKaspersky Security Center 管理サーバーに送信します。

Kaspersky Endpoint Security アプリケーションを標準モードまたは Endpoint Detection and Response Agent モードで使用し、 Kaspersky Security Center を使用してアプリケーションを管理する場合、既定では、ライセンスの追加と削除、およびライセンスの有効期限に関する情報が OS ログに記録されます。

Web コンソールを使用してデバイスのライセンスに関する情報を表示する

Web コンソールでデバイスに追加されたライセンスに関する情報を表示する場合：

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済みのアプリケーションのリストで、［Kaspersky Endpoint Security］をクリックします。

6. これにより、アプリケーションのプロパティウィンドウが開きます。そのウィンドウで、［**全般**］タブを選択し、［**ライセンス**］セクションに移動します。

   このセクションには、アプリケーションに追加されたライセンスと、これら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。

   - **ライセンスのステータス**は、ライセンスのステータス（現在または予備）です。
   - **アプリケーション名は**、ライセンスに関連付けられたライセンスの名前と、このライセンスに関する情報です。
   - **ライセンスは**、一意の英数字シーケンスであるライセンスです。
   - **ライセンス種別** – 試用版、製品版、または定額制サービス。

- **アクティベーション日**は、このライセンスが追加された日付です。
- **有効期限**は、このライセンスを追加してアクティベートされた製品の使用権が期限切れになる日付です。

管理コンソールを使用してデバイスのライセンスに関する情報を表示する

Kaspersky Security Center 管理コンソールでデバイスに追加されたライセンスに関する情報を表示する場合：

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 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。または、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。
6. ウィンドウが開きます。そのウィンドウで、［**ライセンス**］セクションに移動します。
   このセクションには、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（現在または予備など）。
   - **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** – このライセンスを追加して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。

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。追加機能をアクティベートするために本製品に別のライセンスが追加されている場合は、追加機能用に追加された現在のライセンスと予備の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。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

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：

- このライセンスが追加された場合の現在のメイン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。
- 予備のメインライセンスに関する情報。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。アプリケーションを仮想環境保護用 Light Agent モードで使用している場合、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。
  - 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。
- 予備のライセンス（固有の英数字文字列）。
- 現在のライセンスに関連付けられたライセンスの有効期限が切れる日時 (UTC)。

- 別のライセンスが追加された場合の追加機能の現在のライセンスに関する情報：
  - 追加機能を有効にするライセンスの有効期限。
  - ライセンス期間が終了するまでの日数。
  - 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。

- 追加機能のための予備のライセンスに関する情報。本製品が基本モードまたは Endpoint Detection and Response Agent モードで使用されており、追加機能用に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。アプリケーションを仮想環境保護用 Light Agent モードで使用している場合、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。
  - 追加機能を有効にするライセンスの有効期限。
  - 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。
  - 予備のライセンス（固有の英数字文字列）。
  - 現在のライセンスに関連付けられたライセンスの有効期限が切れる日時 (UTC)。

`kesl-control --app-info` コマンドを使用して本製品の動作に関する情報を表示するときに、本製品が使用されているライセンスに関する情報も取得できます。

データ提供

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、使用許諾契約書、KSN に関する声明をお読みの上、カスペルスキーの Web サイトにあるプライバシーポリシーを参照してください。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または Endpoint Detection and Response Agent 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
- ユーザーの端末の日時、
- 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 を標準モードまたは Endpoint Detection and Response Agent 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、製品の配布と使用状況に関する統計情報を提供するために、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
    - 製品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ための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状態と実行結果、およびタスクの設定。
- 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）とルール適用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

Kaspersky Security Network がカスペルスキーに提供するデータセットは、Kaspersky Security Network のモードによって異なります。

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。

基本 KSN モードのデータ提供

Kaspersky Security Network を標準 KSN モードで使用している場合（Web コンソールで **Kaspersky Security Network（KSN）の使用**トグルスイッチがオン、**拡張 KSN モードを使用する**チェックボックスがオフ、管理コンソールで **標準 KSN モード**オプションが選択されている場合）、Kaspersky Security Network に関する声明の諸条件に同意することにより、以下の情報をカスペルスキーに自動的に提供することに同意したものとみなされます。

拡張 KSN モードでのデータ提供

Kaspersky Security Network を拡張 KSN モードで使用している場合（Web コンソールで **Kaspersky Security Network（KSN）の使用**トグルスイッチがオン、**拡張 KSN モードを使用する**チェックボックスがオン、管理コンソールで **拡張 KSN モード**オプションが選択されている場合）、Kaspersky Security Network に関する声明の諸条件に同意することにより、上記の情報に加えて、以下の情報をカスペルスキーに自動的に提供することに同意したものとみなされます。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携で拡張 KSN モードを使用する場合のデータ提供

Kaspersky Endpoint Security を Kaspersky Endpoint Detection and Response Expert（オンプレミス）の一部として使用し、Kaspersky Security Network も拡張モードで使用している場合、「Kaspersky Security Network に関する声明」の諸条件に同意することにより、上記の情報に加えて、以下の情報をカスペルスキーに自動的に提供することに同意したものとみなされます。

Kaspersky Endpoint Security を基本モードまたは Endpoint Detection and Response Agent モードで使用する場合のデータ提供

Kaspersky Endpoint Security をBasic モードまたは Endpoint Detection and Response Agent モードで使用し、Kaspersky Security Network も拡張モードで使用している場合、Kaspersky Security Network に関する声明の諸条件に同意することにより、上記の情報に加えて、以下の情報をカスペルスキーに自動的に提供することに同意したものとみなされます。

Kaspersky Endpoint Detection and Response Optimum と連携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および名前
  - 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：
  - ボリュームの名前
  - ボリュームの文字
  - 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：
  - ブラウザー名
  - ブラウザーのバージョン
  - 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 リクエストの実行時間
  - HTTP リクエストを作成したプロセスの一意な ID

脅威の活動連鎖の作成用データ

脅威の活動連鎖の作成用データには次のデータが含まれることがあります：

- 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詳細名
  - 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
  - 処理中のオブジェクトのサイズ、
  - 処理中のオブジェクトのファイル属性、
  - 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名
  - 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名
  - 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 Web アドレス
- 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 Web 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（インバウンドまたはアウトバウンド）
- 悪意のあるコードが挿入されたプロセスの ID

Kaspersky Endpoint Detection and Response (KATA) コンポーネントと連携時に提供されるデータ

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情報を保存します：

- Kaspersky Endpoint Detection and Response (KATA) との連携を提供する Central Node サーバー （以降、「*KATA サーバー*」とも表記）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
- 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 Expert（オンプレミス）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
    - ライセンスのステータス
- リクエストからタスク実行レポートの EDR Expert（オンプレミス）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
    - タスクの実行エラーとリターンコード
    - タスクの完了ステータス
    - タスクの完了時刻
    - 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
- サーバーにより要求されたファイル
- 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知されたかどうか、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知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。
- 隔離されたオブジェクトの場合：
  - ファイルパス
  - ファイルサイズ
  - 隔離時に割り当てられたファイル ID
  - 元のファイル削除フラグ
- 隔離から取得したファイルの場合：
  - 隔離時に割り当てられたファイル ID
- 実行ファイルまたはスクリプトの実行を阻止する場合：
  - プロセス ID
  - 親プロセス ID
  - システム ID
  - ログオンセッション ID

        - プロセスのステータス
        - 実行を読み取った日時
    - オフィスアプリケーションによる禁止文書の閲覧の場合：
        - プロセス ID
        - ファイル ID
        - 実行を読み取った日時
- ファイルに関する情報：
    - 端末の一意な ID
    - オブジェクトの MD5 ハッシュ
    - ファイルの内容
- 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 ID
        - プロセス 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
        - 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）

- 別の処理のメモリにアクセスするプロセスに関する製品情報：
  - プロセス ID
  - 挿入の方法とアドレス。
  - プロセスの変更に使用されるコマンドライン（引数を含む）。
  - プロセスのシステムコール引数。
- 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
- プロセスのアドレス空間へのライブラリの読み込みに関する情報：読み込まれたライブラリの ID
- 確立されたネットワーク接続に関する情報：
  - ローカル IP アドレス
  - リモート IP アドレス

- 接続の方向
- プロトコル

- 特定のポートで外部ネットワーク接続をリスニングしているプロセスに関する情報：
  - ローカルアドレス（ポートと IP アドレス）
  - プロトコル
- DNS サーバークエリ情報：
  - クエリ対象リソースのドメイン名
  - クエリ対象リソースの IP アドレス
  - DNS サーバー IP アドレス
  - クエリタイプ

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ファイルに保存することもできます。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）コンポーネントと連携時に提供されるデータ

Kaspersky Endpoint Security を Kaspersky Endpoint Detection and Response Expert（オンプレミス）と連携すると、Kaspersky Endpoint Security は次の情報を保存しますが、これには個人情報や機密データが含まれる場合があります：

- Kaspersky Endpoint Detection and Response Expert（オンプレミス）と連携するためのサーバーのリスト。
- Kaspersky Endpoint Detection and Response Expert（オンプレミス）と連携を提供するサーバーの証明書の公開鍵
- Kaspersky Endpoint Detection and Response Expert（オンプレミス）と連携するためのクライアント証明書。
- プロキシサーバー上の認証用資格情報
- Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携を担当するサーバーとの同期頻度の設定、およびこのサーバーのデータ転送設定。
- Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携を処理するサーバーへの接続ステータス、クライアントおよびサーバの証明書エラーに関する情報。

- Kaspersky Endpoint Detection および Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携用にサーバーから送信されるタスクのパラメータ：
  - 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 が Kaspersky Endpoint Detection and Response Expert（オンプレミス）および連携サーバーに連携されている時、本製品は次のデータを保存し、Integration Server に送信できます：

- EDR Expert（オンプレミス）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
  - ライセンスのステータス
- リクエストからタスク実行レポートの EDR Expert（オンプレミス）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
- タスクの実行エラーとリターンコード
- タスクの完了ステータス
- タスクの完了時刻
- 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
- サーバーにより要求されたファイル
- 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知されたかどうか、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知されたかに関する情報）が表示されます。
- YARA ルールの場合、検索結果（ルールがトリガーされたかどうか、見つかったオブジェクト、およびどの YARA ルールがトリガーされたかに関する情報）が返されます。
- IOC が検知されたオブジェクトおよび YARA ルールの場合、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。
- 隔離されたオブジェクトの場合：
  - ファイルパス
  - ファイルサイズ
  - 隔離時に割り当てられたファイル ID
  - 元のファイル削除フラグ

- 隔離で受信、復元、または削除されたファイルの場合：
  - 隔離時に割り当てられたファイル ID
- 実行ファイルまたはスクリプトの実行を阻止する場合：
  - プロセス ID
  - 親プロセス ID
  - システム ID
  - ログオンセッション ID
  - プロセスのステータス
  - 実行を読み取った日時
- オフィスアプリケーションによる禁止文書の閲覧の場合：
  - プロセス ID
  - ファイル ID
  - 実行を読み取った日時
- 指定されたディレクトリ内のファイルのリスト：
  - ファイル名
  - ファイルへの絶対パス
  - ファイルサイズ
  - ファイル種別
  - 所有者ユーザーと所有者グループの名前と ID
  - ファイルアクセス許可
  - 各ファイルに適用される特別なファイルシステムフラグ
  - ファイルのメタデータ
  - ファイルへのハードリンクの数
  - デバイスの作成、変更、および最終アクセス時刻
- デバイスで実行中のプロセスのリスト：
  - プロセス名
  - プロセス開始時間
  - プロセスのステータス

        - プロセス ID (PID) と親プロセス ID
        - プロセスの現在の作業ディレクトリ
        - 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
        - 環境変数
        - プロセスの実行ファイルへのパス
        - プロセスを開始したユーザーの名前
        - プロセスを開始したユーザーおよびグループの ID
        - プロセスがシステム内のファイルおよびリソースにアクセスする権限を持つユーザおよびグループの ID
    - 自動実行ポイントのリスト
        - 自動実行ポイントの種別
        - ファイル名
        - ファイルへの絶対パス
        - ファイルアクセス許可
        - 各ファイルに適用される特別なファイルシステムフラグ
        - 所有者ユーザーと所有者グループの名前と ID
        - デバイスの作成、変更、および最終アクセス時刻
    - プロセスメモリのイメージ：
        - プロセス名
        - プロセスファイルへの完全パス
        - プロセスダンプファイル
        - プロセスダンプファイルのサイズ
    - デバイスメモリのイメージ：デバイス RAM のダンプファイル
    - デバイスディスクのイメージ
- ファイルに関する情報：
    - 端末の一意な ID
    - オブジェクトの MD5 ハッシュ
    - ファイルの内容

- テレメトリパケット内のデータ：
  - テレメトリイベントのデータ：
    - イベント ID。
    - 送信されるテレメトリパケットのシーケンス内のイベント番号。
    - イベント種別。
    - イベントの日時
  - 保護対象デバイスに関する情報：
    - 保護対象デバイスの名前。
    - Kaspersky Security Center 内の保護デバイスの ID。
    - Kaspersky Endpoint Detection and Response Expert（オンプレミス）内の保護デバイスの ID。
    - 保護対象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、バージョン、ファミリー。
    - 保護対象デバイスにインストールされているオペレーティングシステムの起動時間とシャットダウン時間。
  - 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 ID
    - プロセス 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
    - 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）

- 別の処理のメモリにアクセスするプロセスに関する製品情報：
  - プロセス ID
  - 挿入の方法とアドレス。
  - プロセスの変更に使用されるコマンドライン（引数を含む）。
  - プロセスのシステムコール引数。
- 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リリース日とバージョン
  - 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
- プロセスのアドレス空間へのライブラリの読み込みに関する情報：読み込まれたライブラリの ID

- 確立されたネットワーク接続に関する情報：
  - ローカル IP アドレス
  - リモート IP アドレス
  - 接続の方向
  - プロトコル
- 特定のポートで外部ネットワーク接続をリスニングしているプロセスに関する情報：
  - ローカルアドレス（ポートと IP アドレス）
  - プロトコル
- DNS サーバークエリ情報：
  - クエリ対象リソースのドメイン名
  - クエリ対象リソースの IP アドレス
  - DNS サーバー IP アドレス
  - クエリタイプ
- 接続済みの外部デバイスに関する情報：
  - 操作の種別（デバイス接続）
  - デバイス種別
  - 固有のデバイス ID
  - デバイス名
  - デバイスパス
- アプリケーションとそのモジュールに関する情報：
  - 本ソフトウェアのバージョン。
  - アプリケーションのインストール、起動、停止、またはアンインストールの時刻。
  - アプリケーションによる処理の開始者。
  - 異常停止の場合にアプリケーションを停止した理由。
  - 異常停止の場合のリターンコード。
- タスクスケジューラとの対話に関する情報（タスクの作成および削除）：
  - タスクの名前。
  - スケジュールされたコマンドへのパス。

    - タスクの開始スケジュール。
    - タスクを作成したユーザーの名前。
    - タスクを開始したユーザーの名前。
    - サービスを削除したユーザーの名前。
- サービスの作成、削除、および変更に関する情報：
    - サービスの名前（変更されている場合は以前の名前も含む）
    - サービスの種別（変更された場合は以前の種別も含む）
    - 実行ファイルへのパス（変更された場合は以前のパスも含む）
    - サービスの依存関係（変更された場合は以前の依存関係も含む）
    - サービスを開始したユーザーの名前（変更された場合は以前のユーザー名を含む）
    - サービスの表示名（変更された場合は以前の表示名を含む）
    - サービスを作成、削除、または変更したユーザーの名前
    - 延期削除フラグ
- コンソール入力に関する情報：
    - コンソール入力を開始したプロセスの ID と種別
    - コンソール入力の内容
- マウントされたデバイスに関する情報：
    - ボリュームのシステム名
    - マウントポイント
- プロセスメモリの変更に関する情報：
    - プロセスのシステムコール引数。
    - コードインジェクションを実行したプロセスとその親プロセスに関する情報
        - プロセスIDとプロセスおよび親プロセスの一意の ID
        - プロセスと親プロセスを開始するために使用されたコマンドライン
        - プロセスの環境変数
        - プロセスと親プロセスを開始したユーザーアカウントの種類
        - プロセスを生成するために使用したシステムコール
        - プロセスを開始したユーザーおよびグループの ID

- プロセスと親プロセスの名前と完全名
- プロセスと親プロセスへの完全パス
- プロセスと親プロセスの MD5 および SHA256 ハッシュ
- セッション ID
- プロセスと親プロセスを開始したユーザーの名前、ドメイン名、および ID

- コードインジェクションを実行したプロセスがロードされたプロセスに関する情報
  - プロセスをロードしたプロセスの一意の ID
  - プロセスをロードしたファイルの名前と完全名
  - プロセスをロードしたプロセスへの完全パス
  - プロセスをロードしたプロセスの MD5 ハッシュ
- プロセスの開始元であるプロセスに関する情報
  - プロセスの開始者であるプロセスのプロセス ID と一意の ID
  - プロセスの開始元であるプロセスのコマンドライン
  - プロセスの開始元であるプロセスを開始したユーザーの名前とドメイン名
  - プロセスの開始プロセスの名前とフルネーム
  - プロセスの開始プロセスへの完全パス
  - プロセスの開始プロセスの MD5 および SHA256 ハッシュ

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ファイルに保存することもできます。

Kaspersky Network Detection and Response (KATA) コンポーネントと連携時に提供されるデータ

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 Network 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情報を保存します：

- NDR サーバーアドレス
- Kaspersky Network Detection and Response (KATA) との連携のためのサーバー証明書の公開鍵
- Kaspersky Network Detection and Response (KATA) と連携するためのクライアント証明書
- プロキシサーバー上の認証用資格情報

- NDR サーバーとの同期頻度の設定およびデータを NDR サーバーに送信するための設定
- NDR サーバー接続ステータスとクライアント証明書およびサーバー証明書に関連するエラーに関する情報

Kaspersky Endpoint Security が Kaspersky Network Detection and Response (KATA) コンポーネントと連携されている場合、Kaspersky Endpoint Security アプリケーションは次のデータを保存し、NDR サーバーに送信します：

- NDR サーバーへの同期要求からのデータ：
  - 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、ファミリーおよびバージョン
  - 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
  - ライセンスのステータス
  - ユーザーのデバイスのモデルとメーカー
- テレメトリパケット内のデータ：
  - デバイスとユーザーに関する情報：
    - デバイス名とデバイス上の時刻
    - OS のファミリー、名前およびバージョン
    - ネットワークインターフェイスに関する情報（説明、サブネットマスク付きの IP アドレスのリスト、MAC アドレス、メトリック番号、DNS ドメイン名、ルーティング情報、リスニングポート番号）
    - デバイス内部の一意の ID
    - ユーザー名と ID
    - ユーザーグループ名と ID
  - Kaspersky Endpoint Security アプリケーションに関する情報：
    - 製品名とバージョン
    - 本製品の最新アップデートの日付
    - ライセンスに関する情報（シリアル番号、種別、ライセンスの有効期間、ライセンスのステータス）

- 製品データベースのバージョン
- API 対応バージョンのリスト

- 確立された接続に関する情報：
  - ローカル IP アドレス、ポートおよび MAC アドレス
  - リモート IP アドレス、ポートおよび MAC アドレス
  - ネットワーク IP アドレス。
  - プロトコル種別（IANA に準拠）、プロトコル番号および EtherType
  - 受信および送信されたパッケージの数
- 処理されたファイルに関する情報：
  - ファイル名と一意の ID
  - ファイルの種別とサイズ
  - ファイルイメージへの完全パス
  - ファイルシステム属性マスク
  - ファイルが作成され、変更された日時
  - チェックサム（MD5 および SHA256）
  - 継承されたものと有効なものを含むファイル権限
- 実行中および終了中のプロセスに関する情報：
  - プロセス UID と PID
  - プロセスの種別。
  - セッション ID
  - 実行済みコマンド
  - 環境変数
- 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

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ファイルに保存することもできます。

Kaspersky Unified Monitoring and Analysis Platform と連携時に提供されるデータ

Kaspersky Endpoint Security を Kaspersky Unified Monitoring and Analysis Platform と連携すると、Kaspersky Endpoint Security は次の情報を保存しますが、これには個人情報や機密データが含まれる場合があります：

- KUMA サーバーアドレス
- Kaspersky Unified Monitoring and Analysis Platform との連携のためのサーバー証明書の公開鍵（UDP プロトコルを使用して KUMA サーバーに接続する場合を除く）
- Kaspersky Unified Monitoring and Analysis Platform との連携のクライアント証明書
- プロキシサーバー上の認証用資格情報
- KUMA サーバーとの同期頻度の設定およびデータを KUMA サーバーに送信するための設定
- KUMA サーバー接続ステータスとクライアント証明書およびサーバー証明書に関連するエラーに関する情報

Kaspersky Endpoint Security を Kaspersky Unified Monitoring and Analysis Platform と連携すると、Kaspersky Endpoint Security は次のデータをテレメトリパケットに保存し、KUMA サーバーに送信します：

- ファイルの変更に関する情報：
  - 変更前のファイルの一意のID
  - 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
  - ファイル操作の種別とフラグ
  - ファイルの変更日時
- 実行中および終了中のプロセスに関する情報：
  - プロセスファイル ID
  - プロセス UID と PID
  - 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
  - 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）

- イベントログ内のイベントに関する情報：
  - イベントの日時
  - イベントに関連付けられたプロセスの UID
  - イベントの種別と説明
  - 操作を実行した結果

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
- 本製品のグラフィカルインターフェイス

> 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 コンソールおよび本製品のグラフィカル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も説明します。

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。

- 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、管理 Web 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。

- 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 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。

Kaspersky Endpoint Security は、Kaspersky Next Pro View ソリューションの一部です。このソリューションの一部として利用可能な本製品の機能の詳細については、Kaspersky Next ヘルプを参照してください。

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。

アプリケーションが EDR Agent モードで使用されている場合、使用できるアプリケーションコンポーネントとタスクは一部に限定されます。特定の保護コンポーネントの管理、アプリケーションのアクティベーション、定義データベースのアップデートを実行できます。EDR Agent モードに固有の事項の詳細については、「既知の問題と制限事項」の記事を参照してください。

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 管理 MMC 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。

管理プラグインの詳細については、Kaspersky Security Center のヘルプを参照してください。

Kaspersky Security Center 16.0 または Kaspersky Security Center 16.1 に、Kaspersky Endpoint Security for Windows （ビルド 12.11.0.2004）および Kaspersky Endpoint Security for Linux （ビルド 12.4.0.1354）の Web プラグインがインストールされている場合、Kaspersky Endpoint Security for Windows Web プラグインをバージョン 12.11.0.6004 にアップデートすると、Kaspersky Endpoint Security for Linux のポリシーが正常に動作しなくなる可能性があります。この場合、［**設定**］→［**Web プラグイン**］ウィンドウに移動し、リストから Kaspersky Endpoint Security for Windows Web プラグイン、 Kaspersky Endpoint Security for Linux Web プラグイン、Unified Protection and Management プラグインを削除します。その後、まず Kaspersky Endpoint Security for Linux の Web プラグインをインストールし、続いて Kaspersky Endpoint Security for Windows の Web プラグインをインストールしてください。

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、子ポリシーは親ポリシーの設定を継承します。*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。

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。

一部のリストでは、リスト項目のマージを有効にできます。リスト項目をマージするには、次の操作を実行します：

- 子ポリシーのプロパティの［**全般**］タブで、［**親ポリシーから設定を継承する**］設定を有効にします。

- 親ポリシーのプロパティで、パッドロック（🔒）アイコンをクリックして「ロック」します。

- 親ポリシーのプロパティで、［**継承した値を統合する**］チェックボックスをオンにして、設定のマージを有効にします。チェックボックスをオンにすると、Kaspersky Security Center の親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。

子ポリシー内の継承されたリスト項目を削除または変更することはできません。継承時にマージされたリスト項目は、親ポリシーでのみ削除または変更できます。リスト項目は下位レベルで追加、変更、または削除できます。したがって、親ポリシーでリストを設定して、それをすべての子ポリシーに適用することができます。また、子ポリシーのリストにさらに追加することもできます。

*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、様々なデバイスの製品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。

「パッドロック」でロックされたプロファイル設定はポリシー設定を上書きします。つまり、「パッドロック」でロックされたプロファイル設定がポリシー設定と異なる場合、アプリケーションはプロファイルの設定を適用します。ただし、設定のリストは連携され、互いに補完し合います。つまり、プロファイルのリストにある設定が「基本」ポリシーにない場合は、結果の設定リストに追加されます。

一部のリストはマージされません。このような場合、プロファイルの設定が「ベース」ポリシーの設定よりも優先されます：

- ファイル脅威保護およびふるまい検出コンポーネントのプロセスによる除外

- ファイル脅威保護およびアンチクリプターコンポーネントの保護範囲

- システム整合性監視コンポーネントの監視範囲

- アプリケーションコントロールコンポーネントのルールのリスト（**アプリケーションコントロールルール**ウィンドウ内）

- Web コントロールのルールのリスト

- 製品設定でのプロセスメモリを除外
- ネットワーク設定の信頼されたドメイン
- ネットワーク設定の信頼されたルート証明書
- ネットワーク設定の監視ポート
- SVM検出設定のSVMアドレスのリスト

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。

ポリシーが削除されたときに本製品が実行されていない場合、本製品の起動後、このポリシーはデバイスに引き続き適用され、本製品はこのポリシーで指定された設定で引き続き動作します。

ポリシーとポリシープロファイル、および設定の継承メカニズムの詳細については、Kaspersky Security Center 製品情報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デバイスセットのタスク

  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については、Kaspersky Security Center 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。本製品がLight Agent モードで使用されている場合、*ライセンスの追加*、*アップデート*、*ロールバック*の各タスクは適用されません。

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。

Kaspersky Security Center Web コンソールには、次のいずれかの方法でログインできます：

- ドメイン認証（シングルサインオン）
- ドメインユーザーのユーザー名とパスワード
- 内部ユーザーのユーザー名とパスワード

Kaspersky Security Center Web コンソールへのログインとログアウトの詳細については、Kaspersky Security Center ヘルプを参照してください。

ユーザー名とパスワードを指定して Web コンソールにログインするには：

1. ブラウザーで次のアドレスに移動します：

   ```
   https://<Kaspersky Security Center Web Console address>:<port number>
   ```

   管理サーバーを選択するページが開きます。

2. 複数の信頼済み管理サーバーを追加している場合は、リストから接続する管理サーバーを選択します。

管理サーバーを1台だけ追加している場合、管理サーバーのリストは表示されません。

ブラウザーは `https://<Administration Server address>:4444` にリダイレクトされます。

3. 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。

4. ［**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。

5. モバイルデバイスの認証アプリで生成されたワンタイムセキュリティコードを入力します。

初めてログインする場合は、アカウントに2段階認証を設定します。

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。ポリシーのプロパティウィンドウの［**製品設定**］タブでポリシー設定を構成できます。Web コンソールのポリシー設定については、付録 5 で説明しています。

> 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。

- ポリシー設定をエクスポートおよびインポートします。

  Kaspersky Endpoint Security 12.3 for Linux から Kaspersky Endpoint Security 12.4 for Linux へのポリシー設定のエクスポートまたはインポートは、サポートされていません。

- ポリシーをコピーして移動します。
- ポリシーを削除する。
- 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. 表示されたウィンドウで、リストから Kaspersky Endpoint Security 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：

   - **標準モードまたは Endpoint Detection and Response Agent モード**では、スタンドアロンアプリケーションとして、および Kaspersky Detection and Response ソリューションとサードパーティのアンチウイルスソリューションの連携に対応するアプリケーションとして、本製品は Linux 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 アドレスのカスタムリストを使用する**］をオンにした場合、Light Agent は拡張 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［**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 形式による 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」が指定されていた場合、Integration Server への接続はエラーで終了します。

      - **ポート**

        Integration Server に接続するためのポート。既定ではポート 7271 が指定されます。

      インフラストラクチャに Linux ベースの高可用性 Integration Server のクラスターを展開する場合は、Integration Server に接続するためのアドレスおよびポートとして、ロードバランサーのアドレスおよびポートを指定する必要があります。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。

      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、［**アクションを選択**］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。SVM をリストに追加するには、**追加**ボタンをクリックし、表示されたウィンドウで SVM の IPv4 形式の IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。複数の SVM の IP アドレスまたは完全修飾ドメイン名を 1 行に 1 つずつ入力して入力できます。

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選択されます。
  - **非アクティブ**：このオプションを選択した場合、ポリシーはデバイスに適用されず、**ポリシー**フォルダに残ります。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。
  - **モバイルユーザー**：このオプションを選択すると、デバイスが組織のネットワークから離れた時に、ポリシーがオンになります。

デバイスで現在のネットワークエージェントポリシーの［**ネットワーク**］→［**接続プロファイル**］セクションで、［**管理サーバーが利用できない場合に不在モードを有効にする**］設定を有効にする必要があります。

- ポリシー設定の継承：
  - **親ポリシーから設定を継承する**：このトグルスイッチを有効にすると、ポリシー設定は上位レベルのグループポリシーから継承されます。「パッドロック」（🔒）でロックされた親ポリシー内の設定は編集できません。このトグルスイッチ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**：このトグルスイッチをオンにすると、ポリシー設定が子ポリシーに反映されます。子ポリシーのプロパティで、［**親ポリシーから設定を継承する**］は自動的にオンになり、オフにすることはできません。子ポリシーの設定は、「パッドロック」（🔓）が有効の場合を除き、親ポリシーから継承されます。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全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、アプリケーションのライセンスの種別によって異なります。

ポリシーのプロパティウィンドウの［**製品設定**］タブでポリシー設定を構成できます。

Web コンソールのポリシー設定については、付録 5 で説明しています。

ポリシーの設定

セクション	サブセクション
ホスト脅威対策	**ファイル脅威対策**このサブセクションでは、ファイル脅威対策を管理できます。 **有害 USB 攻撃ブロック**このサブセクションでは、有害 USB 攻撃ブロック設定を管理できます。 **リムーバブルドライブスキャン**このサブセクションでは、保護対象デバイスに接続済みのリムーバブルドライブをスキャンするための設定を構成できます。 **ふるまい検知**このサブセクションでは、アプリケーションのふるまい検知の設定を管理できます。 **アンチクリプター**このサブセクションでは、リモートの悪意のある暗号化に対する保護設定を構成できます。 **脆弱性攻撃ブロック**このサブセクションでは、脆弱税攻撃ブロック設定を管理できます。
コミュニケーションと危険サイトブロック	**メール脅威対策**このサブセクションでは、メール脅威対策設定を管理できます。 **ウェブ脅威対策**このサブセクションでは、ウェブ脅威対策設定を構成できます。 **ネットワーク脅威対策**このサブセクションでは、ネットワーク脅威対策設定を構成できます。 **ファイアウォール**このサブセクションでは、ファイアウォール管理設定を構成できます。
セキュリティコントロール	**デバイスコントロール**このサブセクションでは、デバイスコントロール設定を構成できます。 **ウェブコントロール**このサブセクションでは、ウェブコントロール設定を構成できます。 **アプリ管理**このサブセクションでは、アプリケーションコントロール設定を構成できます。 **システム変更監視**このサブセクションでは、システム変更監視設定を構成できます。
信頼ゾーン	このセクションでは、次の設定を構成できます： • ファイル脅威対策コンポーネントによって適用される除外。 • これらの設定は、ウェブ脅威対策で使用されます。 • ネットワーク脅威対策保護コンポーネントによって適用される除外。 • ネットワークトラフィックスキャンからの除外。 • ファイル操作の傍受からのマウントポイントの除外。 • デバイスコントロールコンポーネントの信頼するデバイス。

セクション	サブセクション
全般設定	**検知の設定**このサブセクションでは、次の設定を管理できます： • 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の検出。 • ファイル操作の読み取りモード。 **Kaspersky Security Network**このサブセクションでは、Kaspersky Endpoint Security による Kaspersky Security Network の使用を設定できます。 **ユーザーインターフェイス**このサブセクションでは、次の設定を管理できます： • アプリケーションの起動設定。 • ユーザーのタスク管理権限。 **Performance**このサブセクションでは、次の設定を管理できます： • バッテリー電源で動作しているデバイスでのスケジュールされたタスクのキャンセル。 • スキャンからプロセスメモリを除外。 • 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。 • アプリケーションの安定性監視。 **ネットワーク設定**このサブセクションでは、次の設定を行うことができます： • 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のプロキシサーバー。 • ネットワークトラフィックのスキャン設定。 **コンテナのスキャン**。このサブセクションでは、コンテナ監視コンポーネントを管理できます。 **テクニカルサポート**このサブセクションでは、トレースとダンプの設定を管理できます。 **Reports and Storage**このサブセクションでは、バックアップと隔離の設定を管理できます。 **KSC 連携**このサブセクションでは、Kaspersky Security Center リポジトリに情報を送信するための設定を管理できます。 **OS の対話設定**。このサブセクションでは、次の設定を行うことができます： • 本製品で使用する**システムイベント傍受**メカニズムを選択します。 Web コンソールでは、ポリシープロパティ（**製品設定 → 全般設定設定 → OS 連携設定**）でシステムイベント遮断を設定できます。 この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。 • 詳細なテレメトリパラメータ設定を管理します。 **通知設定**。このサブセクションでは、イベント通知設定を管理できます。
組み込みエージェントの設定	**Managed Detection and Response**このサブセクションでは、Kaspersky Managed Detection and Response との連携を有効または無効にしたり、連携に必要な MDR BLOB ファイルをアップロードしたりできます。 **Network Detection and Response (KATA)**このサブセクションでは、Kaspersky Network Detection and Response (KATA)との連携を有効または無効にすることができます。 **Endpoint Detection and Response**このサブセクションでは、Kaspersky Detection and Response Optimum との連携を有効または無効にし、連携設定を管理できます。 **Endpoint Detection and Response Expert（オンプレミス）**このサブセクションでは、Kaspersky Endpoint Detection and Response Expert （オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) との連携を有効または無効にし、連携設定を管理できます。 **Sandbox**このサブセクションでは、サンドボックスとの連携を有効または無効にし、連携設定を管理できます。 **KUMA 連携**このサブセクションでは、Kaspersky Unified Monitoring and Analysis Platform との連携を有効または無効にし、連携設定を管理できます。
Light Agent モード このセクションに記述の設定は、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。	**SVM discovery settings**このサブセクションでは、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。 **Integration Server 接続設定**。このサブセクションでは、Kaspersky Security for Virtualization Light Agent のコンポーネントである Integration Server への Light Agent の接続を設定できます。 **SVM connection tag**このサブセクションでは、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。 **SVM selection algorithm**このサブセクションでは、Light Agent が使用する SVM 選択アルゴリズムを指定できます。 **Connection protection**このウィンドウでは、Light Agent と Protection Server 間のリンクの暗号化を有効にすることができます。

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、次の処理を実行できます：

- ポリシーを作成します。
- ポリシーの設定を編集します。ポリシー設定は、ポリシーのプロパティウィンドウで管理できます。

  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。

- ポリシー設定をエクスポートおよびインポートします。
- ポリシーを削除する。
- 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。

ポリシーの管理に関する全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手順として、リストから Kaspersky Endpoint Security 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 のモードの指定

   - **標準モードまたは Endpoint Detection and Response Agent モード**では、スタンドアロンアプリケーションとして、および Kaspersky Detection and Response ソリューションとサードパーティのアンチウイルスソリューションの連携に対応するアプリケーションとして、本製品は Linux 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 アドレスのカスタムリストを使用する**］をオンにした場合、Light Agent は拡張 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［**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 形式による 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」が指定されていた場合、Integration Server への接続はエラーで終了します。

- **ポート**

  Integration Server に接続するためのポート。既定ではポート 7271 が指定されます。

> インフラストラクチャに Linux ベースの高可用性 Integration Server のクラスターを展開する場合は、Integration Server に接続するためのアドレスおよびポートとして、ロードバランサーのアドレスおよびポートを指定する必要があります。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。

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。SVM をリストに追加するには、**追加**ボタンをクリックし、表示されたウィンドウで SVM の IPv4 形式の IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。複数の SVM の IP アドレスまたは完全修飾ドメイン名を 1 行に 1 つずつ入力して入力できます。

> 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. ポリシーの状態を選択します：

    - **現在のポリシー**。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選択されます。
    - **非アクティブポリシー**。このオプションを選択した場合、ポリシーはデバイスに適用されず、**ポリシー**フォルダに残ります。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。
    - **モバイルポリシー**。このオプションを選択すると、デバイスが組織のネットワークから離れた時に、ポリシーがオンになります。

    > デバイスで現在のネットワークエージェントポリシーの［**ネットワーク**］→［**接続プロファイル**］セクションで、［**管理サーバーが利用できない場合に不在モードを有効にする**］設定を有効にする必要があります。

15. 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、アプリケーションのライセンスの種別によって異なります。

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**このサブセクションでは、ファイル脅威対策を管理できます。 **ファイル脅威対策の除外**。このサブセクションでは、ファイル脅威対策の保護コンポーネントに適用される除外を設定できます。 **ファイアウォール管理**。このサブセクションでは、ファイアウォール管理設定を構成できます。 **ウェブ脅威対策**このサブセクションでは、ウェブ脅威対策設定を構成できます。 **メール脅威対策**このサブセクションでは、メール脅威対策設定を管理できます。 **ネットワーク脅威対策**このサブセクションでは、ネットワーク脅威対策設定を構成できます。 **有害 USB 攻撃ブロック**このサブセクションでは、有害 USB 攻撃ブロック設定を管理できます。
先進の脅威対策	**Kaspersky Security Network**このサブセクションでは、Kaspersky Endpoint Security による Kaspersky Security Network の使用を設定できます。 **アンチクリプター**。このサブセクションでは、リモートの悪意のある暗号化に対する保護設定を構成できます。 **ふるまい検知**このサブセクションでは、アプリケーションのふるまい検知の設定を管理できます。

セクション	サブセクション
Detection and Response	**Managed Detection and Response**。このサブセクションでは、Kaspersky Managed Detection and Response との連携を有効または無効にしたり、連携に必要な MDR BLOB ファイルをアップロードしたりできます。 **EDR Expert（オンプレミス）**。このサブセクションでは、Kaspersky Endpoint Detection and Response (KATA) との連携を有効または無効にし、連携設定を管理できます。 **Network Detection and Response (KATA)**。このサブセクションでは、Kaspersky Network Detection and Response (KATA)との連携を有効または無効にすることができます。
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**このサブセクションでは、アプリケーションコントロール設定を構成できます。 **システム変更監視**このサブセクションでは、システム変更監視設定を構成できます。 **デバイスコントロール**このサブセクションでは、デバイスコントロール設定を構成できます。 **ウェブコントロール**このサブセクションでは、ウェブコントロール設定を構成できます。
ローカルタスク	**タスク管理**。このサブセクションでは、ユーザーがタスク管理するための権限を設定できます。 **リムーバブルドライブスキャン**。このサブセクションでは、保護対象デバイスに接続済みのリムーバブルドライブをスキャンするための設定を構成できます。
全般設定	**プロキシサーバー設定**。このサブセクションでは、ユーザがクライアントデバイスからプロキシサーバ経由でインターネットにアクセスする場合のプロキシサーバーの設定を構成できます。 **製品設定**。このサブセクションでは、次の設定を管理できます： • 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の検出。 • 通知設定。 • 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。 • 特権付きユーザーがデバイス上で同時に開始できるカスタムスキャンタスクの数を制限します。 • アプリケーションの起動設定。 • トレースおよびダンプ設定。 • アプリケーションの安定性監視。 • 本製品による常駐メモリの使用を制限。 • ファイル操作の読み取りモード。 **コンテナスキャン設定**。このサブセクションでは、コンテナ監視コンポーネントを管理できます。 **ネットワーク設定**　このサブセクションでは、ネットワークトラフィックをスキャンする設定ができます。 **グローバル除外リスト**。このサブセクションでは、次の設定を行うことができます： • ファイル操作の傍受からのマウントポイントの除外。 • 特定の種類のソフトウェアに関連付けられたプロセス、ファイル、およびディレクトリを除外する産業用ソフトウェアの除外。 **プロセスメモリの除外**。このサブセクションでは、スキャンからプロセスメモリの除外を設定できます。 **保管領域の設定**。このサブセクションでは、次の設定を行うことができます： • バックアップと隔離。 • Kaspersky Security Center の保管領域へのデータ転送の設定。 **OS 対話設定** このサブセクションでは、次の設定を行うことができます： • 本製品で使用するシステムイベント傍受メカニズムを選択します。 • 詳細なテレメトリパラメータ設定を管理します。
KUMA 連携	**KUMA 連携**。このサブセクションでは、Kaspersky Unified Monitoring and Analysis Platform との連携を有効または無効にし、連携設定を管理できます。

セクション	サブセクション
Light Agent モード このセクションに記述の設定は、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。	**Integration Server への接続**。このサブセクションでは、Kaspersky Security for Virtualization Light Agent のコンポーネントである Integration Server への Light Agent の接続を設定できます。 **SVM 検出設定**。このサブセクションでは、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 接続タグ**。このサブセクションでは、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。 **SVM 選択アルゴリズム**。このサブセクションでは、Light Agent が使用する SVM 選択アルゴリズムを指定できます。 **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

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。

- 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、タスク実行結果を監視できます：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の表示。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全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アプリケーションのグラフィカル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 コンソールでデバイスグループまたはデバイスセットの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、製品名 Kaspersky Endpoint Security 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 ヘルプシステム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**］をオンにします。タスクは既定で作成されます。

6. ウィザードを終了します。

タスクのリストに新しいタスクが表示されます。

Web コンソールでローカル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）**］→［**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、タスクを作成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、［**タスク**］タブに移動します。

   このデバイス用に作成されたタスクのリストが表示されます。

5. ［**追加**］をクリックします。

   タスクウィザードが起動します。

6. 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、製品名 Kaspersky Endpoint Security 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。

7. 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**］をオンにします。タスクは既定で作成されます。

8. ウィザードを終了します。

タスクのリストに新しいタスクが表示されます。

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. タスクの設定を指定します：

   - ［**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、再開するには：

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。

- 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、タスク実行結果を監視できます：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の表示。

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全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アプリケーションのグラフィカル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

管理コンソールでデバイスグループまたはデバイスセットの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手順として、Kaspersky Endpoint Security とタスクの種別を選択します。

   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. ウィザードを終了します。

   タスクのリストに新しいタスクが表示されます。

管理コンソールでローカルタスクを作成します：

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、［**タスク**］セクションを選択します。

   このデバイス用に作成されたタスクのリストが表示されます。

5. ［**追加**］をクリックします。
   タスクウィザードが起動します。

6. ウィザードの最初の手順として、Kaspersky Endpoint Security とタスクの種別を選択します。
   ウィザードの次のステップに進みます。

7. 新しいタスクの名前を入力し、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。

8. ウィザードを終了します。
   タスクのリストに新しいタスクが表示されます。

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：

- コンテナスキャンの全般設定。
- ネットワークトラフィックのスキャン設定。
- 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するアプリケーションの全般設定。

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。

アプリケーションが EDR Agent モードで使用されている場合、使用できるアプリケーションコンポーネントとタスクは一部に限定されます。特定の保護コンポーネントの管理、アプリケーションのアクティベーション、定義データベースのアップデートを実行できます。EDR Agent モードに固有の事項の詳細については、「既知の問題と制限事項」の記事を参照してください。

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スキャン*。このタスクを使用すると、リムーバブルメディア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。

- *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 Expert（オンプレミス）の連携*。このタスクでは、Kaspersky Endpoint Detection and Response Expert （オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) との連携を有効または無効にし、連携設定を管理できます。

- *Kaspersky Network Detection and Response (KATA) 連携* このタスクでは、Kaspersky Network Detection and Response (KATA) との連携を有効または無効にし、連携設定を指定できます。

- *サンドボックスとの連携*。このタスクは、サンドボックスとの連携を有効または無効にし、連携の設定を指定します。

- *KUMA 連携*。このタスクは、Kaspersky Unified Monitoring and Analysis Platform との連携を有効または無効にし、連携の設定を指定します。

- *オブジェクトの実行防止（EDR Expert（オンプレミス））*。このタスクでは、Endpoint Detection and Response Expert（オンプレミス） の実行防止ルールの使用を有効または無効にしたり、これらのルールのリストを表示したりできます。

- *オブジェクトの実行防止 (EDR Optimum)*。このタスクでは、Endpoint Detection and Response Optimum 実行防止ルールの使用を有効または無効にしたり、これらのルールのリストを表示したりできます。

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	アップデート	6	アップデート
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	アップデート
ロールバック	ロールバック	7	ロールバック
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	ロールバック
ライセンス管理	License	9	License
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	ファイアウォール
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
コンテナスキャン	Container_Scan	18	ContainerScan
コンテナスキャン（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 Expert（オンプレミス）との連携	KATAEDR	24	KATAEDR
ウェブコントロール	Web_Control	26	WebControl
サンドボックス統合	Standalone_Sandbox	29	StandaloneSandbox
オブジェクトの実行防止（EDR Expert（オンプレミス））	KATAEDR_Prevention	30	KATAEDRPrevention
Kaspersky Endpoint Detection and Response (KATA) 連携	KATANDR	31	KATANDR
オブジェクトの実行防止（EDR Optimum）	EDRO_Prevention	32	Prevention
KUMA 連携	KUMA	33	KUMA
メール脅威対策	Mail_Monitoring	35	MailMonitoring
有害 USB 攻撃ブロック	Bad_USB	37	BadUSB

タスクに対して次の処理を実行できます：

- *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` – アプリケーションタスクのリストの出力形式です。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：

- `Name` – タスク名
- `ID` – タスク ID
- `Type` – タスク種別
- `State` – タスクの現在の状態

Kaspersky Security Center のポリシーにより、ユーザーによるローカルタスクの表示と編集が禁止されている場合、Scan_My_Computer、Critical_Areas_Scan、Container_Scan、Inventory_Scan、Update（標準モード）、および Rollback（標準モード）タスクに関する情報は利用できません。

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 <タスク種別>
```

説明：

- **<タスク名>** は、新しいタスクに指定する名前です。
- **<タスク種別>** は、作成するタスクの種別を表します。

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。
- **<タスク種別>** は、作成するタスクの種別の識別子です。
- **<ファイルのパス>** は、タスクの作成に使用される設定を含む設定情報ファイルへの完全パスです。
- `--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。`--json` オプション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

License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、InventoryScanタイプのタスクは、一時停止および再開できます。

タスクを開始する

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

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上のタスク名です。
- `[-W]` は、このタスクに関連する現在のイベントの出力を有効にします。
- `[--progress]` は、タスクの進行状況の表示を有効にします。

ID 1 のタスクを実行し、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する例

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

タスクの開始時にエラーが発生し、タスクが開始されない場合は、アプリケーションを再起動した後、タスクを再度開始しようとします。

タスクを停止する

```
kesl-control --stop-task <task ID|name> [-W]
```

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上のタスク名です。
- `[-W]` は、このタスクに関連する現在のイベントの出力を有効にします。

タスクを一時停止する

```
kesl-control --suspend-task <task ID|name>
```

タスクを再開する

```
kesl-control --resume-task <task ID|name>
```

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>
```

ここで、**<タスク ID/名前>** は、タスクの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。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

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/名前> --file <設定情報ファイルのパス> [--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 >** は、タスク設定を書き込む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。**--json** オプションを指定しないと、設定は INI 形式で出力されます。

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*タスクの設定も編集できません。

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。
- コマンドラインオプションを使用して、**< 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のオプション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する場合は、ファイルに次の設定を含む `[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. 次のコマンドを実行します：

   `kesl-control --set-settings <タスク ID/名前> --file <設定情報ファイルのパス> [--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>`** は、タスク設定のインポート元となる設定情報ファイルへの完全パスです。
   - JSON 構成ファイルから設定をインポートする場合は、`--json` オプションを指定します。`--json` オプション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、`--set-settings` オプションを指定して `--accept` コマンドを実行します。

コマンドラインのオプションを使用したタスク設定の編集

`kesl-control --set-settings` コマンドのオプションを使用すると、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

コマンドラインのオプション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、いずれかの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、`--set-settings` オプションを指定して `--accept` コマンドを実行します。

スキャン範囲の追加および削除

コマンドラインのオプション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：

- **<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-path` **<パス>** は、スキャン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。

新しい `[ScanScope.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。

Path設定に指定された値の [ScanScope.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=*
```

コマンドラインのオプションで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 <パス>** は、スキャンするオブジェクトが含まれ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しません。

除外範囲の追加および削除

コマンドラインのオプション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 <パス>**は、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。

  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。

Path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。

コマンドラインのオプション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 <パス>** は、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削除します。

  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
```

ここで、**<タスク ID/名前>** は、タスクの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。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

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/名前> --file <設定情報ファイルのパス> [--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 >** は、タスクスケジュール設定を書き込む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。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

  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、タスクスケジュールの個別設定を **< 設定名 >=< 設定値 >** 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. 次のコマンドを実行します：

   ```
   kesl-control --set-schedule <タスク ID/名前> --file <設定情報ファイルのパス> [--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 >** は、タスクスケジュール設定のインポート元となる設定情報ファイルの完全パスです。
- JSON 構成ファイルから設定をインポートする場合は、**--json** オプションを指定します。**--json** オプション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/名前 > < 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 11 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オプションを使用して、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。
- ファイル操作の読み取りモード（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的な設定の現在の値を、コンソールや設定情報ファイルに出力することができます。この設定情報ファイルを使用して、アプリケーションのパラメータを編集することができます。

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]
```

ここで、`--json` を指定すると、設定が JSON 形式で出力されます。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

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 <設定情報ファイルへのパス> [--json]
```

説明：

- **--file <設定情報ファイルのパス>** は、本製品の全般設定が書き込まれる設定情報ファイルのパスです。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。**--json** オプションを指定しないと、設定は INI 形式で出力されます。

例：
本製品の全般設定を kesl_config.ini という名前のファイルに出力し、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-app-settings --file kesl_config.ini
```

製品の全般設定の編集

コマンドラインで、**kesl-control --set-app-settings** コマンド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。

- コマンドラインオプションを使用して、**<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. 次のコマンドを実行します：

   kesl-control --set-app-settings --file <設定情報ファイルへのパス> [--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完全パスです。設定情報ファイル内のパラメータを削除すると、コマンドの実行後にそのパラメータの既定値が表示されます。

   - JSON 構成ファイルから設定をインポートする場合は、**--json** オプションを指定します。**--json** オプション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。

コマンドラインのオプション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>]

ここで、**<設定名>=<設定値>** は、アプリケーションの全般設定のいずれかの名前と値です。

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
```
ファイル操作の読み取り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 and。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「より小さい」です
  - **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

    > **like** 比較操作は、定義データベースにテキストとして保存されているフィールドでのみ機能します。**like** 操作は、日付、時刻、数値、またはテキスト以外の他のデータ種別のフィールドには適していません。

  - **==** は "対象に等しい"
  - **!=** は "対象に等しくない"
  - **>=** は "対象以上"
  - **<=** は「以下」です

- **< 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。

  日付値は、UNIX™ 時刻（1970 年 1 月 1 日 00:00:00（UTC）から経過した秒数）または YYYY-MM-DD hh:mm:ss 形式で指定できます。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。

- 現在のアプリケーションイベントのうち、特定のイベントに関する情報を出力します（コマンドラインでのイベントの表示、Kaspersky Security Center でのイベントの表示）：

  `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出力します（コマンドラインでのイベントの表示、Kaspersky Security Center でのイベントの表示）：

  `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、すべての製品設定（コンテナスキャンの全般設定、ネットワークトラフィックのスキャン設定、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 <設定情報ファイルへのパス> [--json]
```

説明：

- `--file <設定情報ファイルのパス>` は、アプリケーション設定を保存する設定情報ファイルの完全パスです。
- `--json` を指定すると、設定を JSON 形式で設定情報ファイルにエクスポートします。`--json` オプション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>` は、アプリケーションへの設定のインポート元となる設定情報ファイルの完全パスです。
- `--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。`--json` オプション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。

ファイルから設定をインポートする場合、`UseKSN` と `CloudMode` は `No` に設定され、MDR との連携は無効になります。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。MDR 連携を有効にするには、まず Kaspersky Security Network の拡張モードを有効にし、`UseMDR` を `Yes` に設定する必要があります。

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。

次のポリシー設定は、アプリケーション Web プラグインのバージョン 12.3 からアプリケーションのバージョン 12.4 にインポートできません：

- ファイル脅威対策およびアンチクリプターの保護範囲と除外範囲
- ふるまい分析によるスキャンからのプロセスの除外
- デバイスコントロールの信頼するデバイス
- システム変更監視のスキャン範囲と除外範囲
- ウェブコントロールルール
- プロキシサーバー設定
- プロセスメモリのスキャンからの除外
- グローバル除外（スキャンから除外されるマウントポイント）

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。

デバイスを保護するには、アプリケーションにオペレーティングシステムでのより高い権限が必要です。アプリケーションは、基本的なセキュリティ機能の一部を実行するために root 権限を必要とします。

アプリケーションのロールベースのアクセスモデルには、管理者（admin）ロールが含まれています。場合によっては、管理者ロールを持つユーザーの操作により、オペレーティングシステムのスーパーユーザー（root）の権限で処理が実行される可能性があります。

管理者ロールは、信頼できるユーザーにのみ付与してください。この管理者ロールが侵害または悪用されると、デバイス全体が侵害され、組織のインフラストラクチャのセキュリティ、整合性、パフォーマンス、およびユーザーデータに影響を及ぼす可能性があります。

管理者ロールの付与はシステム所有者の責任であり、組織のアクセスコントロールポリシーおよび該当するユーザーに対する信頼度に従って実施する必要があります。

ユーザーロール

ロール名	製品内のロール	OS のユーザーグループ	権限
Administrator	admin	kesladmin	sudo コマンドを使用せずに、本製品のグラフィカルインターフェイスとコマンドラインで製品設定とタスク設定を管理します。 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 <役割> <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 <役割> <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］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**］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 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、/u

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
```

デバイスの保護ステータスとアプリケーションのパフォーマンス情報の表示

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。

- コマンドラインで次の管理コマンドを使用します：

  - `kesl-control --app-info` コマンドは、本製品のパフォーマンスと、本製品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製品情報を表示します。

  - `kesl-control --supported-tech-info` コマンド：製品機能のリスト、そのステータス（使用中または未使用）に関する情報、およびこれらの製品機能が実装されている Linux テクノロジーを表示します。

  - `kesl-control --get-statistic` コマンドは、アプリケーションのパフォーマンス統計とマウントポイントの一覧を出力します。

  - `kesl-control --export-metrics` コマンドは、OS のステータスメトリックを出力します。

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済みのアプリケーションのリストで、［Kaspersky Endpoint Security］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。

このウィンドウには、Kaspersky Endpoint Security に関する以下の情報も表示されます：

- ［**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** – 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。
- **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）。
- **インストールされた更新プログラム**ブロックには、インストールされているアプリケーションの更新プログラムのバージョンに関する情報が含まれています。
- ［**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**］タブは、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。
- ［**アプリケーション設定**］タブで、次の操作ができます：
  - **Detection and Response** では、デバイスのネットワーク分離を管理できます。
  - ［**アプリケーションコントロール**］セクションでは、指定されたコンポーネント設定とアプリケーションカテゴリをファイルにエクスポートしたり、ファイルからインポートしたりできます。
  - ［**統計**］セクションでは、アプリケーションの統計とマウントポイントのリストを表示できます。

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 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。または、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。

   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。

このウィンドウには、Kaspersky Endpoint Security に関する以下の情報も表示されます：

- ［**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** – 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。
  - **インストール済みアップデート**は、インストールされているアプリケーションのアップデートのバージョンに関する情報です。
  - **製品データベース** – 製品データベースのアップデートがリリースされた日時。
- ［**アプリケーションコントロール**］セクションでは、構成されたコンポーネント設定とアプリケーションカテゴリをファイルにエクスポートしたり、ファイルからインポートしたりできます。
- ［**統計**］セクションには、アプリケーションの統計とマウントポイントに関する情報が表示されます。
- ［**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。
- ［**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

本製品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。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

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。
- デバイスに適用されているポリシーに関する拡張情報：
  - ポリシー名。
  - デバイス上でポリシーが最後に適用または更新された日時。
  - デバイスが属する Kaspersky Security Center 管理グループ。
  - デバイスに適用されているポリシープロファイルのリスト（もしあれば）。

  デバイスにインストールされているネットワークエージェントの［**アプリケーションがデバイス上のポリシーの拡張データを取得することが許可されている**］設定で、Kaspersky Endpoint Security から拡張ポリシーデータを取得することが許可されている場合、拡張ポリシー情報が表示されます。既定で、この設定は有効です。ネットワークエージェント設定についての詳細は、『Kaspersky Security Center のヘルプ』を参照してください。
- 本製品が使用されている主なライセンスに関する情報：
  - **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。
  - **Kaspersky Endpoint Security のライセンスの有効期限**。本製品のライセンスの有効期限の日時 (UTC)。
- 本製品の追加機能を有効にするライセンスに関するライセンス情報。保護対象デバイスに追加機能のライセンスが追加されている場合、次のフィールドが表示されます：
  - **EDR Optimum のライセンス情報**。Endpoint Detection and Response Optimum コンポーネントをアクティベートした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。** ライセンスの有効期限の日時 (UTC)。

- **KUMA ライセンス情報**。Kaspersky Unified Monitoring and Analysis Platform 機能が使用されるライセンスに関する情報、または KUMA ライセンスのステータス。
- **KUMA ライセンスの有効期限日**：ライセンスの有効期限の日時 (UTC)。
- **MDR ライセンス情報**。Managed Detection and Response コンポーネントをアクティベートしたライセンスに関する情報、または MDR ライセンスのステータス。
- **MDR ライセンスの有効期限日**：ライセンスの有効期限の日時 (UTC)。
- **EDR Expert（オンプレミス）のライセンスの情報**。Endpoint Detection and Response Expert（オンプレミス）コンポーネントをアクティベートしたライセンス、および EDR Expert（オンプレミス）のライセンスのステータスに関する情報。
- **EDR Expert（オンプレミス）の ライセンスの有効期限**。ライセンスの有効期限の日時 (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 MDR BLOB ファイルのステータス。
- **MDR BLOB ファイルのライセンスの有効期限**。Kaspersky Managed Detection and Response のライセンスの有効期限の日時 (UTC)。このフィールドは、Kaspersky Managed Detection and Response 連携用に BLOB 設定情報ファイルが読み込まれている場合に表示されます。
- **バックアップのステータス**。バックアップのステータスに関する情報。
- **バックアップ使用量**。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。
- **アップデート可能なカーネルモジュールのステータス**。アップデート可能なカーネルモジュールのステータスに関する情報。
- **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**。
- **仮想環境保護用 Light Agent モード**。アプリケーションが仮想環境保護用 Light Agent モードで使用されていることに関する情報。アプリケーションが標準モードまたは Endpoint Detection and Response Agent モードで使用されている場合、この行は表示されません。
- **Endpoint Detection and Response Agent モード**。本製品が Endpoint Detection and Response Agent モードで使用されていることを示します。本製品が基本モードまたは Light Agent モードで使用されている場合、こ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**。
- **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**。リアルタイムコンテナスキャンのステータス（コンテナスキャン、コンテナ監視）。
- **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。
- **有害 USB 攻撃ブロック**有害 USB 攻撃ブロック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 Expert（オンプレミス）の連携**。Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) との連携のステータス。
- **サンドボックスとの連携**。サンドボックスとの連携ステータス。
- **Kaspersky Unified Monitoring and Analysis Platform との連携**。Kaspersky Unified Monitoring and Analysis Platform との連携ステータス。
- **Kaspersky Network Detection and Response (KATA) の連携** Kaspersky Network Detection and Response (KATA) の連携ステータス。
- **メール脅威対策**メール脅威対策コンポーネントのステータス。
- **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。

製品統計の表示

パフォーマンスを向上させるために、ファイル脅威対策コンポーネントによって最も頻繁にスキャンされるファイル、ふるまい検知コンポーネントによって最も頻繁にスキャンされるアプリケーションへのパス、およびデバイス上で検知されたマウントポイントを除外できます。

fanotify をサポートするオペレーティングシステムを搭載したデバイスでパフォーマンスを向上させる最も効果的な方法は、マウントポイントを除外することです。

最も頻繁にスキャンされたファイルと開始された処理に関する統計情報および検知されたマウントポイントのリストは、次の方法で表示できます：

- Web コンソールで操作
- 管理コンソールで操作
- コマンドラインで

アプリケーションによる統計情報の計算および表示方法のパラメータは、kesl.ini 設定情報ファイルの `[ScannerImpactStats]` セクションで設定できます。

Web コンソールでのアプリケーション統計の表示

Web コンソールでアプリケーション統計を表示します：

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. 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済みのアプリケーションのリストで、［Kaspersky Endpoint Security］をクリックします。

6. 開いたアプリケーションプロパティウィンドウで、［**製品設定**］タブで、［**統計**］→［**スキャン統計**］を選択します。

   ［**スキャン統計**］ウィンドウが表示されます。

［**スキャンの統計**］ウィンドウには、次のアプリケーション統計が表示されます：

- ［**最も頻繁にスキャンされるアプリケーション（ファイル脅威対策）**］ブロックには、ファイル脅威対策コンポーネントが最も頻繁にスキャンするアプリケーションへのパスと、コンポーネントがこれらのアプリケーションにアクセスする回数が表示されます。ファイルはアクセス回数の降順で表示されます。

- ［**最も頻繁に開始される処理**］に、Kaspersky Endpoint Security が最も頻繁に検知する処理へのパスと、開始された回数が表示されます。処理へのパスは、開始された回数の降順で表示されます。

各ブロックの上部にある［**エクスポート**］ボタンを使用すると、そのブロックに表示される統計情報をテキストファイルにエクスポートできます。

管理コンソールでのアプリケーション統計の表示

管理コンソールでアプリケーション統計を表示します：

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、**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 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。または、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。

6. 開いたウィンドウで、［**統計**］→［**スキャン統計**］の順に選択します。

   右側のウィンドウに次のアプリケーション統計が表示されます：

   - ［**最も頻繁にスキャンされるアプリケーション（ファイル脅威対策）**］ブロックには、ファイル脅威対策コンポーネントが最も頻繁にスキャンするアプリケーションへのパスと、コンポーネントがこれらのアプリケーションにアクセスする回数が表示されます。ファイルはアクセス回数の降順で表示されます。

   - ［**最も頻繁に開始される処理**］に、Kaspersky Endpoint Security が最も頻繁に検知する処理へのパスと、開始された回数が表示されます。処理へのパスは、開始された回数の降順で表示されます。

   各ブロックの下にある［**エクスポート**］ボタンを使用すると、そのブロックに表示される統計情報をテキストファイルにエクスポートできます。

Web コンソールでのマウントポイントのリストの表示

Web コンソールでマウントポイントのリストを表示します：

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. 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済みのアプリケーションのリストで、［Kaspersky Endpoint Security］をクリックします。

6. 開いたアプリケーションプロパティウィンドウで、［**製品設定**］タブで、［**統計**］→［**マウントポイント**］を選択します。

   ［**マウントポイント**］ウィンドウが開きます。

   ［**マウントポイント**］ウィンドウには、次の列を含むテーブルが表示されます。

   - **マウントポイントパス**は、デバイス上で検出されたマウントポイントへのパスです。
   - **名前空間**は、マウントポイントが名前空間内に見つかったかどうかを示します。
   - **除外**は、マウントポイントがスキャンの除外リストに追加されているかどうかを示します。

   マウントポイントパスは、次のようにソートされます。

   - 静的、システム、サービス、その他のマウントポイント
   - 名前空間にマウントされたスナップパッケージとマウントポイント
   - Docker コンテナ管理システムによって作成されたマウントポイント

   リストの上にあるウィンドウ上部の［**エクスポート**］ボタンをクリックすると、マウントポイントのリストをテキストファイルにエクスポートできます。ファイルには、マウントポイントパスのリストと、［**名前空間**］タグおよび［**除外**］タグが含まれます。

管理コンソールでのマウントポイントのリストの表示

管理コンソールでマウントポイント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、**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 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。または、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。
6. 開いたウィンドウで、［**統計**］→［**マウントポイント**］の順に選択します。
   ［**マウントポイントのリスト**］テーブルは、ウィンドウの右側に表示され、次の列が含まれます。
   - **マウントポイントパス**は、デバイス上で検出されたマウントポイントへのパスです。
   - **名前空間**は、マウントポイントが名前空間内に見つかったかどうかを示します。
   - **除外**は、マウントポイントがスキャンの除外リストに追加されているかどうかを示します。

   マウントポイントパスは、次のようにソートされます。
   - 静的、システム、サービス、その他のマウントポイント
   - 名前空間にマウントされたスナップパッケージとマウントポイント
   - Docker コンテナ管理システムによって作成されたマウントポイント

   リストの下にある［**エクスポート**］をクリックすると、マウントポイントのリストをテキスト形式のファイルにエクスポートできます。ファイルには、マウントポイントパスのリストと、［**名前空間**］タグおよび［**除外**］タグが含まれます。

コマンドラインでのアプリケーション統計とマウントポイントのリストの表示

アプリケーション統計とマウントポイント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 [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

説明：

- `--files`：ファイル脅威対策コンポーネントによって最も頻繁にスキャンされるファイルに関する統計と、コンポーネントがこれらのファイルにアクセスする回数。
- `--processes`：Kaspersky Endpoint Security によって最も頻繁に検出された開始処理の統計とその開始数。

  ふるまい検知コンポーネントによるスキャンからプロセスを除外しても、これらのプロセスは統計情報から削除されませんが、Kaspersky Endpoint Security アプリケーションのパフォーマンスが向上します。

- `--mountpoints`：マウントポイントのリスト。

  出力には以下の情報が含まれます：

  - `[excluded]`は、マウントポイントがスキャンの除外リストに追加されているかどうかを示します。
  - `[namespace]` はマウントポイントが名前空間で見つかったかどうかを示します。
  - デバイス上で見つかったマウントポイントへのパス。

  マウントポイントパスは、次のようにソートされます。

  - 静的、システム、サービス、その他のマウントポイント
  - 名前空間にマウントされたスナップパッケージとマウントポイント
  - Docker コンテナ管理システムによって作成されたマウントポイント

1つ以上のオプションを任意の組み合わせで指定することも、オプションをまったく指定しないことも選択できます。オプションを指定しない場合、最も頻繁にスキャンされたファイルの統計、最も頻繁に開始された処理の統計、およびデバイス上で見つかったマウントポイントの リストの 3 つを表示します。

システムパフォーマンスメトリックの取得

Kaspersky Endpoint Security は OS に影響します。影響の分析に役立つように、本製品のパフォーマンスに関連するメトリックを取得できます。

Grafana などのデータ可視化ツールでメトリクスを分析できます。エクスポートされたメトリックを Prometheus や Zabbix などの監視システムに公開できます。

本製品が使用するオペレーティングシステムのリソースのメトリックを取得するように設定するには、次のコマンドを実行します：

```
kesl-control [-J] --export-metrics [--period <エクスポート間の間隔（秒）>|--interactive]
```

説明：

- `--period` は結果の定期的な出力を有効にします。
- `--interactive` は、対話型出力を有効にします（**Enter** キーが押されたとき）。

このコマンドは、メトリックのリストをコンソールに出力します。

メトリックのリスト

メトリックの内部名、メトリックのラベルと種別	説明と推奨するしきい値の設定
lfs_system_descriptor_opened_count センサー	kesl プロセスによって現在開かれているディスクリプタの数。 ディスクリプタの数が 1 時間あたり 250 を超える速度で増加する場合は、テクニカルサポートに連絡することを推奨します。
lfs_system_uptime_milliseconds カウンター	オペレーティングシステムの起動から現在までの時間（ミリ秒）。
lfs_system_memory_usage_bytes 「type=virtual」ラベル センサー	kesl プロセスによって現在使用されている仮想化メモリの量。 システム情報に基づいて閾値を設定する手順を実行することを推奨します。この情報は手動で取得することも、スクリプトを使用して取得することもできます。サンプルスクリプトについては、テクニカルサポートにご連絡ください。
lfs_system_memory_usage_bytes 「type=resident」ラベル センサー	kesl プロセスによって現在使用されている常駐メモリの量。 システム情報に基づいて閾値を設定する手順を実行することを推奨します。この情報は手動で取得することも、スクリプトを使用して取得することもできます。サンプルスクリプトについては、テクニカルサポートにご連絡ください。
lfs_system_memory_usage_bytes 「type=swap」ラベル センサー	kesl プロセスによって現在使用されているスワップメモリの量。 システム情報に基づいて閾値を設定する手順を実行することを推奨します。この情報は手動で取得することも、スクリプトを使用して取得することもできます。サンプルスクリプトについては、テクニカルサポートにご連絡ください。
lfs_system_cpu_usage_milliseconds 「type=ユーザー」ラベル カウンター	kesl プロセスの開始から現在までの、ユーザー空間での kesl プロセスによって使用された CPU 時間（ミリ秒）。 システム情報に基づいて閾値を設定する手順を実行することを推奨します。この情報は手動で取得することも、スクリプトを使用して取得することもできます。サンプルスクリプトについては、テクニカルサポートにご連絡ください。
lfs_system_cpu_usage_milliseconds 「type=kernel」ラベル カウンター	kesl プロセスの開始から現在までの、カーネル空間での kesl プロセスによって使用された CPU 時間（ミリ秒）。 システム情報に基づいて閾値を設定する手順を実行することを推奨します。この情報は手動で取得することも、スクリプトを使用して取得することもできます。サンプルスクリプトについては、テクニカルサポートにご連絡ください。
lfs_system_cpu_usage_milliseconds 「type=total」ラベル カウンター	kesl プロセスの開始から現在までの、ユーザー空間とカーネル空間での kesl プロセスによって使用された CPU 時間（ミリ秒）。 kesl プロセスによって使用される CPU 時間が残りの作業を超える場合は、テクニカルサポートに連絡することを推奨します。
lfs_tcpSynInterceptor_connection_hanging_count カウンター	kesl プロセスの開始から現在までの、サーバーとクライアント間の TCP ネットワークのハンドシェイク段階でハングアップしているネットワーク接続の合計数（/proc/sys/net/ipv4/tcp_syn_retries のシステム設定に応じて、1 秒から 2 分間リモートサーバーが接続を許可するのを待機している場合、ネットワーク接続はハングしていると見なされます）。 このメトリックの増加は、リモートサーバーがアクセスできないか、見つからないことが原因で発生する可能性があります。ハングアップしているネットワーク接続の数が 1 分あたり 10 件を超えて増加する場合は、テクニカルサポートに連絡することを推奨します。
lfs_tcpSynInterceptor_connection_count センサー	現在リモートサーバーへの接続を待機しているネットワーク接続数。
lfs_tcpSynInterceptor_verdict_count 「verdict=allow」ラベル カウンター	kesl プロセスの開始から現在までに確立された、読み取った接続の合計数。
lfs_tcpSynInterceptor_verdict_count 「verdict=drop」ラベル カウンター	kesl プロセスの開始から現在までの、確立されていない読み取った接続の合計数。

メトリックの内部名、メトリックのラベルと種別	説明と推奨するしきい値の設定
lfs_tcpSynInterceptor_verdict_count 「verdict=unknown」ラベル カウンター	kesl プロセスの開始から現在までの、リモートサーバーを処理できないソリューションによるネットワーク接続の合計数。
lfs_tcpSynInterceptor_verdict_latency_milliseconds ヒストグラム	SYNパケットがインターセプトされた時点から、そのパケットに対する解決が発行されるまでの間、リモートサーバーが接続の解決を完了するまでに要した時間のヒストグラム。
lfs_tproxy_connection_count 「direction=inbound」ラベル センサー	現在の読み取られた受信ネットワーク接続の数。
lfs_tproxy_connection_count 「direction=outbound」ラベル センサー	現在の読み取られた送信ネットワーク接続の数。
lfs_tproxy_connection_orphaned_count カウンター	読み取りが意図されていなかったにもかかわらず（たとえば、互換性のない iptables 設定や、本製品が新しい読み取り設定を処理する時間がなかったために）、Kaspersky Endpoint Security によって読み取られた接続の合計数（ウェブ脅威対策、ネットワーク脅威対策、およびウェブコントロール保護コンポーネントの開始以降）。このような接続は拒否されます。 このような接続の合計数が 10 を超える場合は、本製品またはシステムが正しく動作していないことを示している可能性があるため、テクニカルサポートに連絡することを推奨します。
lfs_tproxy_threadPool_task_count カウンター	ウェブ脅威対策、ネットワーク脅威対策、およびウェブコントロール保護コンポーネントの開始以降にスレッドプールに追加されたタスク（新しい接続、新しいデータバッチ、送信されたデータなど）の合計数。 作成されたが完了していないタスクの合計数が増え続ける場合は、リソースを追加するか、除外を設定するか、テクニカルサポートに連絡先する必要があります。
lfs_tproxy_threadPool_task_duration_milliseconds ヒストグラム	読み取られた接続を処理するタスクの実行時間のヒストグラム。 タスクの 95% の実行時間が 1 秒を超える場合は、リソースを追加するか、除外を設定するか、テクニカルサポートに連絡する必要があります。
lfs_tproxy_socket_count センサー	現在のソケット数（リスニングソケットと接続ソケット）。読み取られた接続には 2 つの接続ソケットがあります。
lfs_trafficScanning_object_hanging_count センサー	読み取られたトラフィック内のハングアップしているオブジェクトのスキャンの現在の数（1分を超える期間のスキャンはハングしていると見なされます）。 ハングアップしているオブジェクトのスキャンの合計数が 35 を超えると、製品データベースに問題があることを示します。このような場合は、テクニカルサポートに連絡することを推奨します。
lfs_trafficScanning_object_duration_milliseconds ヒストグラム	読み取られたトラフィックオブジェクトのスキャン時間のヒストグラム。 オブジェクトの 95% のスキャン時間が 1 秒を超える場合は、リソースを追加するか、製品データベースをアップデートするか、テクニカルサポートに連絡する必要があります。 読み取られたトラフィック内のパケットスキャンの増加率が 0 であり、lfs_tproxy_threadPool_task_count メトリックの値が 0 でない場合は、製品データベースをアップデートするか、テクニカルサポートに連絡する必要があります。
lfs_fileMonitor_cache_size センサー	ファイルの変更を監視するファイルモニター（ファイル修正キャッシュ）の現在のサイズ。 現在のファイル監視のキャッシュサイズが 50,000 を超える場合は、テクニカルサポートに連絡することを推奨します。
lfs_fileMonitor_cache_hit_count カウンター	ファイルの変更を監視するファイル監視キャッシュ（ファイル修正キャッシュ）のヒットカウント。
lfs_fileMonitor_cache_miss_count カウンター	ファイルの変更を監視するファイル監視キャッシュ（ファイル修正キャッシュ）のミスカウント。

メトリックの内部名、メトリックのラベルと種別	説明と推奨するしきい値の設定
lfs_faCache_file_count センサー	スキャンする必要のない fanotify インターセプターファイルのキャッシュの現在のサイズ。 現在のファイルキャッシュサイズが 100,000 を超える場合は、テクニカルサポートに連絡することを推奨します。
lfs_faCache_file_hit_count カウンター	スキャンする必要のない fanotify インターセプターファイルのキャッシュのヒット数。
lfs_faCache_file_miss_count カウンター	スキャンする必要のない fanotify インターセプターファイルのキャッシュのミス数。
lfs_faCache_volume_count センサー	fanotify 読み取りマウントポイントキャッシュの現在のサイズ。
lfs_oas_cache_file_count センサー	スキャンする必要のないファイル脅威対策ファイルのキャッシュの現在のサイズ。 現在のファイルキャッシュサイズが 100,000 を超える場合は、テクニカルサポートに連絡することを推奨します。
lfs_oas_cache_file_hit_count カウンター	スキャンする必要のないファイル脅威対策ファイルのキャッシュのヒット数。
lfs_oas_cache_file_miss_count カウンター	スキャンする必要のないファイル脅威対策ファイルのキャッシュのミス数。
lfs_oas_cache_volume_count センサー	ファイル脅威対策マウントポイントキャッシュの現在のサイズ。
lfs_processManager_cache_size センサー	システム内でキャッシュされている現在実行中のプロセスの数。
lfs_processManager_cache_hit_count カウンター	システムプロセスキャッシュのヒット数。
lfs_processManager_cache_miss_count カウンター	システムプロセスキャッシュのミス数。
lfs_blockingProcessInterceptor_cache_size センサー	プロセスを開始するために使用できるインタープリターのキャッシュの現在のサイズ。 この数値は、特定のデバイス上でスクリプトがどの程度集中的に実行されるかによって異なります。現在のファイルキャッシュサイズが 10000 を超える場合は、テクニカルサポートに連絡することを推奨します。
lfs_blockingProcessInterceptor_cache_hit_count カウンター	インタープリターキャッシュのヒット数。
lfs_blockingProcessInterceptor_cache_miss_count カウンター	インタプリターキャッシュのミス数。
lfs_prevention_cache_file_count センサー	スキャンが不要なオブジェクトの「オブジェクトの実行防止」タスクのファイルキャッシュの現在のサイズ。
lfs_prevention_cache_file_hit_count カウンター	スキャンが不要なオブジェクトの「オブジェクトの実行防止」タスクのファイルキャッシュのヒット数。
lfs_prevention_cache_file_miss_count カウンター	スキャンが不要なオブジェクトの「オブジェクトの実行防止」タスクのファイルキャッシュのミス数。
lfs_prevention_cache_volume_count センサー	「オブジェクトの実行防止」タスクのマウントポイントキャッシュの現在のサイズ。
eka_telemetry_metrics_registry_callbacks_exec_duration_milliseconds センサー	レジストリに登録されているすべてのクライアントの現在のメトリックのアップデートにかかった時間（ミリ秒単位）。

メトリックの内部名、メトリックのラベルと種別	説明と推奨するしきい値の設定
eka_telemetry_metrics_registry_registered_callbacks センサー	MetricsRegistry が登録済みのすべてのクライアントに対して実行したメトリックアップデートコールバックの現在の数。
eka_telemetry_metrics_registry_scrape_duration_milliseconds センサー	すべてのレジストリメトリックの取得に要した時間（ミリ秒単位）。 このメトリックの値の 99% が 10 分間に 1 秒を超える場合は、テクニカルサポートに連絡することを推奨します。

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

更新機能（アンチウイルスシグネチャの更新およびコードベースの更新を含む）は、米国領土内のアプリケーションでは利用できない場合があります。

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、インターネットトラフィックが最大で数十 MB まで増加することがあります。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 が標準モードまたは Endpoint Detection and Response Agent モードで使用されている場合は、Kaspersky Security Center で、管理 MMC プラグインまたは Kaspersky Endpoint Security 管理 Web 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。

自動的にインストールされる製品アップデート（自動パッチ）を受信することもできます。アップデートタスク設定では、自動パッチのダウンロードおよびインストール方法（ダウンロードとインストール、ダウンロードのみ、ダウンロードなし）を選択できます。

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。

  定義データベースの更新は成功したが、定義データベース自体が破損しており、アプリケーションがエラーで連続して終了した場合、定義データベースは自動的に削除されます。アプリケーションは「定義データベースなし」モードで動作し続け、定義データベースとアプリケーションモジュールの更新機能は引き続き利用できます。

  定義データベースが 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製品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、*製品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、製品データベースをアップデートせずに 7 日間が過ぎると、*製品データベースが完全に未アップデートイベント*が生成されます。

- 製品機能：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、製品機能の動作が変更されたり、新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。

  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。

  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。

アップデート元と更新シナリオ

*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 では、定義データベースと製品機能のアップデート方法として、次の方法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。

  一元的なアップデートでは次の手順を実行します。

  1. 組織ネットワーク内のリポジトリにアップデートパッケージを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 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

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. 表から、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 の 2 つのアップデート元が含まれています。**ステータス**列には、タスクの実行時にアプリケーションがこのアップデート元を使用しているかどうかが示されます。［**追加**］をクリックすると、他のアップデート元をリストに追加できます。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、［**タスクの開始**］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
アップデート元の表	このテーブルには、定義データベースの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**は、アップデート元のアドレスです： • **カスペルスキーのアップデートサーバー** - カスペルスキー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。 • ユーザーによって追加される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。 • **ステータス**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**］）。ステータスを変更するには、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［**このソースを使用する**］切り替えボタンををオンまたはオフにします。 表内で、アップデート元の**追加**、**編集**、削除、**上に移動**、**下に移動**を行うことができます。 ［**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。 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のタイムアウト（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、自動的にインストールされるアップデート（自動パッチ）のダウンロード方法を選択できます。 • **ダウンロードしない**。この項目を選択すると、自動パッチは自動的にダウンロードされません。 • **ダウンロードのみ**。このリスト項目を選択すると、自動パッチは自動的にダウンロードされますが、クライアントデバイスにインストールされません（既定）。 • **ダウンロードしてインストールする**。このリスト項目を選択すると、自動パッチは自動的にダウンロードされ、クライアントデバイスにインストールされます。自動パッチがインストールされると、本製品は自動的に再起動します。

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

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. 表から、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 の 2 つのアップデート元が含まれています。**ステータス**列には、タスクの実行時にアプリケーションがこのアップデート元を使用しているかどうかが示されます。［**追加**］をクリックすると、他のアップデート元をリストに追加できます。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	このテーブルには、定義データベースの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： • **ソースアドレス**はアップデート元のアドレスです： • **カスペルスキーのアップデートサーバー** - カスペルスキー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。 • ユーザーによって追加される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。 • **ステータス**は、そのアップデート元がタスクで使用されるかどうかを示します（**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。 表内で、アップデート元の**追加**、**編集**、削除、**上に移動**、**下に移動**を行うことができます。 ［**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。 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のタイムアウト（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、自動的にインストールされるアップデート（自動パッチ）のダウンロード方法を選択できます。 • **ダウンロードしない**。この項目を選択すると、自動パッチは自動的にダウンロードされません。 • **ダウンロードのみ**。このリスト項目を選択すると、自動パッチは自動的にダウンロードされますが、クライアントデバイスにインストールされません（既定）。 • **ダウンロードしてインストールする**。このリスト項目を選択すると、自動パッチは自動的にダウンロードされ、クライアントデバイスにインストールされます。自動パッチがインストールされると、本製品は自動的に再起動します。

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

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、アップデート設定を管理できます。

- 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。

設定	説明	値
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
ApplicationUpdateMode	自動的にインストールされる製品アップデート（自動パッチ）のダウンロードおよびインストール方法。	Disabled：自動パッチのダウンロードもインストールもしません。 DownloadOnly（既定）：自動パッチをダウンロードしますが、インストールしません。 DownloadAndInstall：自動パッチを自動的にダウンロードしてインストールします。自動パッチがインストールされると、本製品は自動的に再起動します。
[Sources.item_#] セクションには、次の設定が含まれています：		
Enabled	SourceType 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（既定）– アップデート元を使用しています。 No – アップデート元を使用していません。
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。 CustomURL 設定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。
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あるカスタムのアップデート元のアドレス。	既定値は定義されていません。 例： 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。

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定義データベースをアップデートするように Kaspersky Security Center を設定します：

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については、カスペルスキーのナレッジベースを参照してください。

3. 組織のローカルネットワーク内の他のデバイス上の指定された共有ディレクトリから製品データベースと機能のアップデートを設定します。

   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。

   d. 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 の設定で指定されたアドレスと一致する必要があります。

   e. ［**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。

   f. 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。

   g. タスク設定への変更を保存します。

コマンドラインを使用して共有ディレクトリから定義データベースをアップデートするように Kaspersky Security Center を設定します：

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については、カスペルスキーのナレッジベースを参照してください。

3. 組織のローカルネットワーク内の他のデバイスにある指定された共有ディレクトリから、製品データベースとモジュールのアップデートを設定します。Update タスクの設定で、`SourceType=Custom` を設定し、`[Sources.item_#]` セクションで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 の設定で指定されたアドレスと一致する必要があります。

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の読み取り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。

root ユーザーが NFS4 プロトコル経由でデバイスにマウントされたリモートディレクトリにアクセスできない場合、すべてのアプリケーションに対してそのような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（コンテナスキャン、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通りです：
  - 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

  また、本製品は、Watchdog サーバのプロセスなど、一部の内部プロセスを自動的にスキャンから除外します。

- 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。

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アプリケーション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設定を管理できます（**製品設定 → ホスト脅威対策 → ファイル脅威対策**）。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**脅威対策 → ファイル脅威対策**）で、ファイル脅威対策の設定を管理できます。

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。テーブル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
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
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。

テーブル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。

指定された範囲にあるオブジェクトは、範囲のテーブル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。

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、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。 • **All remote mounted** – 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。

設定	説明
	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:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` 説明： `<id>` はコンテナIDです。 `<name>` はコンテナ名です `<path to local directory>` はローカルディレクトリへのパスです。 タグの一意の組み合わせを使用することもできます：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]`、`[image-name:<name>]/path to local directory>`。 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:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` 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。

［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する	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、Kaspersky Endpoint Security によって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ャップする（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、Kaspersky Endpoint Security によって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、Kaspersky Endpoint Security によって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、Kaspersky Endpoint Security によって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する	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、Kaspersky Endpoint Security によって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する	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、Kaspersky Endpoint Security によって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、Kaspersky Endpoint Security によって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利用される場合は、テキストファイルは Kaspersky Endpoint Security によって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。 この設定は、fanotify に基づくシステムイベントインターセプターメカニズムを使用する場合に適用されます。更新可能なカーネルモジュールを使用する場合、スキャン結果のキャッシュを使用してスキャンが最適化されます。
定義データベースのログファイルをスキップ	定義データベースのジャーナルファイルをスキャンすること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、最新のスキャン後 10 分以内に同じプロセスによってジャーナルファイルが再利用されると、本製品は定義データベースのジャーナルファイルをスキャンしません。この設定により、定義データベースのジャーナルファイル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、本製品は定義データベースジャーナルファイルをスキャンします。 既定では、このチェックボックスはオフです。 この設定は、fanotify に基づくシステムイベントインターセプターメカニズムを使用する場合に適用されます。更新可能なカーネルモジュールを使用する場合、スキャン結果のキャッシュを使用してスキャンが最適化されます。
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）	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

設定	説明
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、Kaspersky Endpoint Security は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 Kaspersky Endpoint Security によってスキャンされます。 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 Kaspersky Endpoint Security によってスキャンされます。 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。

［脅威検出］ウィンドウでの処理

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：

ファイル脅威対策の設定

設定	説明
脅威の検知時の処理	本製品が感染を検知したオブジェクトに対して実行する処理を選択できます： • **駆除する。駆除できない場合は削除する**（既定）。この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトは削除されます。 • **駆除する。駆除できない場合はブロックする。**この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトへのアクセスはブロックされます。 • **ブロック**：この処理を選択すると、本製品は感染したオブジェクトへのアクセスをブロックします。 感染したオブジェクトが駆除または削除されると、感染したオブジェクトのコピーがバックアップに配置されます。

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。

管理コンソールでは、ポリシーのプロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**脅威対策 → ファイル脅威対策の除外**）で、ファイル脅威対策の除外を管理できます。

スキャンの除外の設定

設定のグループ	説明
除外リスト	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、［**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。
プロセスによる除外	この設定グループには、**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、**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

このウィンドウには、スキャンの除外範囲が表示されます。テーブル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。

除外範囲の設定

設定	説明
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
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。

既定では、除外範囲のテーブルは空です。テーブル内の項目は、追加、編集、削除できます。

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。

［<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。

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、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。 • **All remote mounted** – 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:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` 説明： `<id>` はコンテナIDです。 `<name>` はコンテナ名です `<path to local directory>` はローカルディレクトリへのパスです。 タグの一意の組み合わせを使用することもできます：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]`、`[image-name:<name>]/path to local directory>`。 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:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` 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がスキャンから除外されます。

設定	説明
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。

［マスクによる除外］ウィンドウ

名前マスクによってオブジェクトのスキャン除外範囲を設定できます。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。

［**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）。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。既定では、このチェックボックスはオフです。

［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。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。既定では、このチェックボックスはオフです。

［プロセスによる除外］ウィンドウ

このウィンドウには、プロセスごとの除外範囲が含まれています。プロセスによる除外の除外範囲を使用すると、指定されたプロセスのアクティビティ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、リスト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
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
除外範囲名	除外範囲名。
パス	除外されるプロセスの完全パス。
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。

テーブル内の項目は、追加、編集、または削除できます。

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。 更新可能なカーネルモジュールがシステムイベント傍受に使用される場合、指定されたプロセスはすべての名前空間での傍受から除外されます。
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。

設定	説明
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。 • **All remote mounted** – 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。 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。
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。

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に指定できるすべての設定について、指定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	値
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。 アーカイブファイルをスキャン中、ファイルが一時ディレクトリに解凍されてスキャンされる間、アーカイブファイルへのアクセスがブロックされ、パフォーマンスに影響を与えるため、この設定を有効にすることは推奨しません。	Yes – アーカイブをスキャンします。 ActionOnThreat が DisinfectDeleteIfNotPossible に設定されていて、駆除が不可能な場合、本製品は圧縮ファイルの種類に応じて、感染したオブジェクトまたは脅威を含む圧縮ファイル全体を削除します。 No（既定値）– アーカイブをスキャンしません。
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 – 自己解凍型アーカイブをスキャンします。 No（既定値）– 自己解凍型アーカイブをスキャンしません。
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 – メールデータベースのファイルをスキャンします。 No（既定値）– メールデータベースのファイルをスキャンしません。
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 – プレーンテキストのメールメッセージをスキャンします。 No（既定値）– プレーンテキストのメールメッセージをスキャンしません。
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。この設定により、製品ログのスキャンを最適化できます。 この設定は、fanotify に基づくシステムイベントインターセプターメカニズムを使用する場合に適用されます。更新可能なカーネルモジュールを使用する場合、スキャン結果のキャッシュを使用してスキャンが最適化されます。	Yes – 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た場合は、テキストファイルをスキャンしません。 No（既定値）– プレーンテキスト形式のファイルをスキャンします。
SkipDatabaseJournals	定義データベースのジャーナルファイルをスキャンすることから一時的に除外します。この設定により、定義データベースのジャーナルファイルのスキャンを最適化できます。 この設定は、fanotify に基づくシステムイベントインターセプターメカニズムを使用する場合に適用されます。更新可能なカーネルモジュールを使用する場合、スキャン結果のキャッシュを使用してスキャンが最適化されます。	Yes – 最後のスキャンから 10 分以内に定義データベースのジャーナルファイルが同じプロセスで再利用された場合は、スキャンしません。 No（既定）– 定義データベースのジャーナルファイルをスキャンします。
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 から 999999 0 – スキャン対象オブジェクトのサイズは無制限です。 既定値：0

設定	説明	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 から 9999 0 – オブジェクトのスキャン時間は無制限です。 既定値：60
ActionOnThreat	感染したオブジェクトに対して実行されるアクションを選択。	DisinfectDeleteIfNotPossible（駆除。不可能な場合は削除）は、本製品がオブジェクトのコピーをバックアップに保存した後、感染したオブジェクトの駆除を試みることを意味します。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトは削除されます。 DisinfectBlockIfNotPossible（駆除。不可能な場合はブロック）は、本製品がオブジェクトのコピーをバックアップに保存した後、感染したオブジェクトの駆除を試みることを意味します。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトへのアクセスはブロックされます。 Block – 感染したオブジェクトへのアクセスをブロックします。 既定値：DisinfectDeleteIfNotPossible。
UseExcludeMasks	ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外します。	Yes – ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外します。 No（既定値）– ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外しません。
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。	既定値は定義されていません。 例： UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外できるようにします。	Yes - ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外します。 No（既定値）：ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外しません。
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。	設定値では大文字と小文字が区別されます。 既定値は定義されていません。 例： UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux

設定	説明	値
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 – 感染していないオブジェクトに関する情報をログに記録します。 No（既定値）– 感染していないオブジェクトに関する情報をログに記録しません。
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 – アーカイブ内のスキャン済みオブジェクトに関する情報をログに記録します。 No（既定値）– アーカイブ内のスキャン済みオブジェクトに関する情報をログに記録しません。
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 – 処理されていないオブジェクトに関する情報をログに記録します。 No（既定値）– 処理されていないオブジェクトに関する情報をログに記録しません。
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（既定値）– ヒューリスティック分析を有効にします。 No – ヒューリスティック分析を無効にします。
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 – 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。 Medium – 中間のヒューリスティック分析レベルで、システムへの負荷ともバランスが取れています。 Deep – 最も徹底的なスキャンを行い、システムへの負荷が最大となります。 Recommended（既定値）– 推奨値。
UseIChecker	iChecker 技術の使用を指定します。	Yes（既定値）– iChecker 技術の使用を有効にします。 No – iChecker 技術の使用を無効にします。
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。	SmartCheck（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。ある処理によってオブジェクトが操作の過程で複数回アクセスされ、変更された場合は、処理によってオブジェクト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。 OpenAndModify – 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。 Open – 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。
[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：All objects。 例： AreaDesc=" Scanning of email databases "
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（既定値）– 指定された範囲をスキャンします。 No – 指定された範囲をスキャンしません。

設定	説明	値
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。 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：*（すべてのオブジェクトをスキャン） 例： AreaMask_item_< 項目番号 >=*doc

設定	説明	値
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へのパス >** – 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。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:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` 説明： `<id>` はコンテナIDです。 `<name>` はコンテナ名です `<path to local directory>` はローカルディレクトリへのパスです。 タグの一意の組み合わせを使用することもできます：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]`、`[image-name:<name>]/path to local directory>`。 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:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` 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`。

設定	説明	値
		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。 `Shared:NFS` – NFSプロトコルによってアクセスできるデバイスのファイルシステムリソースをスキャンします。 `Shared:SMB` – Sambaプロトコルを使用してアクセスできるデバイスのファイルシステムリソースをスキャンします。 `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リモートディレクトリをスキャンします。 `Mounted:SMB` – 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をスキャンします。 `AllRemoteMounted` – Samba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スキャンします。 `AllShared` – SambaプロトコルとNFSプロトコルを使用してアクセス可能なデバイスのすべてのファイルシステムリソースをスキャンします。 `<file system type>` – 指定されたファイルシステムデバイスのすべてのリソースをスキャンします。
[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。	既定値は定義されていません。
`UseScanArea`	指定された範囲のスキャンの除外を指定します。	`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_#`	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：`*`（すべてのオブジェクトをスキャンから除外）

設定	説明	値
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へのパス >** – 指定されたディレクトリ（サブディレクトリを含む）内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**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:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` 説明： `<id>` はコンテナIDです。 `<name>` はコンテナ名です `<path to local directory>` はローカルディレクトリへのパスです。 タグの一意の組み合わせを使用することもできます：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]`、`[image-name:<name>]/path to local directory>`。 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:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` 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`。

設定	説明	値
		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スキャンから除外します。 `Mounted:SMB` – 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をスキャンから除外します。 `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スキャンから除外します。 **<ファイルシステムの種別>** – 指定したデバイスのファイルシステムのすべてのリソースをスキャンから除外します。
[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。 更新可能なカーネルモジュールがシステムイベント傍受に使用される場合、指定されたプロセスはすべての名前空間での傍受から除外されます。	**< プロセスへの完全パス >** – 指定されたローカルディレクトリ内のプロセスをスキャンしません。
`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。
`AreaDesc`	プロセスの除外範囲の説明。	既定値：`All objects`。
`UseExcludedForProgram`	指定された範囲のスキャンの除外を指定します。	`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_#`	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：*（すべてのオブジェクトをスキャンから除外）

設定	説明	値
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。	**< ローカルディレクトリへのパス >** は、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。 `Shared:NFS` – NFSプロトコルによってアクセスできるデバイスのファイルシステムリソースをスキャンから除外します。 `Shared:SMB` – Sambaプロトコルによってアクセスできるデバイスのファイルシステムリソースをスキャンから除外します。 `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スキャンから除外します。 `Mounted:SMB` – 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をスキャンから除外します。 `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スキャンから除外します。 `AllShared` – Sambaプロトコルと NFSプロトコルでアクセス可能なデバイスのすべてのファイルシステムリソースをスキャンから除外します。 `<file system type>` – 指定されたファイルシステムデバイスのすべてのリソースをスキャンから除外します。

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. 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（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 <設定情報ファイルへの完全パス> [--json]`

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. 次のコマンドを実行します：

   `kesl-control --set-settings 1 --file <設定情報ファイルへの完全パス> [--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` オプションを指定します。オプション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

処理するファイルに一つ以上のハードリンクがある場合、本製品は元の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。削除する場合、本製品は処理中のハードリンクを削除しますが、そのファイルへの他のハードリンクは処理しません。

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。

rootユーザーがNFSv4プロトコル経由でデバイスにマウントされたリモートディレクトリにアクセスできない場合、すべてのアプリケーションに対してそのようなファイルへのアクセスがブロックされます。

Kaspersky Security Centerでは、管理MMCプラグインまたはKaspersky Endpoint Security管理Web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

特殊な用途のparsecfsファイルシステム(Astra Linux Special Edition)を使用するオペレーティングシステムで実行する場合は、このファイルシステムのマウントパスをスキャンの除外リストに追加することを推奨します。

- 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する	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する	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する	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

設定	説明
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。
脅威の検知時の処理	本製品が感染を検知したオブジェクトに対して実行する処理を選択できます： • **駆除する。駆除できない場合は削除する**（既定）。この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトは削除されます。 • **駆除する。駆除できない場合は通知する**。この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、ログにレコードが作成されます。 • **通知する**。この処理を選択すると、本製品は感染したオブジェクトに関するレコードをログインに作成します。
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、変更、削除、上に移動、下に移動。 また、[**インポート**] をクリックしてファイルからスキャン範囲のリストをインポートすることも、[**エクスポート**] をクリックしてスキャン範囲のリストを JSON 形式 で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、スキャン範囲のリストを置き換えるか、既存のリストにスキャン範囲を追加するように求められます。

[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。 • **All remote mounted** – 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。

設定	説明
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:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` 説明： `<id>`はコンテナIDです。 `<name>`はコンテナ名です `<path to local directory>`はローカルディレクトリへのパスです。 タグの一意の組み合わせを使用することもできます：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]`、`[image-name:<name>]/path to local directory>`。 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:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` 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。

[スキャン範囲] セクション

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する	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

このテーブルには、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。

テーブル内の項目は、追加、編集、削除できます。

[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	[**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。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。

設定	説明
グローバルの除外リストを使用	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

このウィンドウには、スキャンの除外範囲が表示されます。テーブル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。

除外範囲の設定

設定	説明
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
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。

既定では、除外範囲のテーブルは空です。テーブル内の項目は、追加、編集、削除できます。

インポートボタンを使用してファイルから除外リストをインポートしたり、**エクスポート**ボタンを使用して除外リストをJSONファイルにエクスポートしたり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。

[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。

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。 • **All remote mounted** – 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:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` 説明： `<id>` はコンテナIDです。 `<name>` はコンテナ名です `<path to local directory>` はローカルディレクトリへのパスです。 タグの一意の組み合わせを使用することもできます：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]`、`[image-name:<name>]/path to local directory>`。 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:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` 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。

設定	説明
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。

［マスクによる除外］ウィンドウ

名前マスクによってオブジェクトのスキャン除外範囲を設定できます。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。

［**追加**］または［**編集**］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）。

インポートボタンを使用してファイルから除外リストをインポートしたり、**エクスポート**ボタンを使用して除外リストをJSONファイルにエクスポートしたり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。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。既定では、このチェックボックスはオフです。

［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。

［**追加**］または［**編集**］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。

インポートボタンを使用してファイルから除外リストをインポートしたり、**エクスポート**ボタンを使用して除外リストをJSONファイルにエクスポートしたり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。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。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。

［**除外**］セクションでは、マルウェアのスキャンタスクのプロパティで、除外範囲の設定やマスクの脅威の名前での除外の設定が可能です。

［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。テーブル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
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
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。

テーブル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。

指定された範囲にあるオブジェクトは、範囲のテーブル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。

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、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。 • **All remote mounted** – 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。

設定	説明
	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:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` 説明： `<id>` はコンテナIDです。 `<name>` はコンテナ名です `<path to local directory>` はローカルディレクトリへのパスです。 タグの一意の組み合わせを使用することもできます：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]`、`[image-name:<name>]/path to local directory>`。 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:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` 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。

［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する	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**］ウィンドウが開き、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。
グローバルの除外リストを使用	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

このテーブルには、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。

テーブル内の項目は、追加、編集、削除できます。

［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。

設定	説明
アーカイブをスキャンする	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する	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する	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。

設定	説明
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。

［脅威検出］ウィンドウでの処理

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
脅威の検知時の処理	本製品が感染を検知したオブジェクトに対して実行する処理を選択できます： • **駆除する。駆除できない場合は削除する**（既定）。この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトは削除されます。 • **駆除する。駆除できない場合は通知する**。この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、ログにレコードが作成されます。 • **通知する**。この処理を選択すると、本製品は感染したオブジェクトに関するレコードをログインに作成します。

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

このウィンドウには、スキャンの除外範囲が表示されます。テーブル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。

除外範囲の設定

設定	説明
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
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。

既定では、除外範囲のテーブルは空です。テーブル内の項目は、追加、編集、削除できます。

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。

［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。

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、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。 • **All remote mounted** – 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:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` 説明： `<id>` はコンテナIDです。 `<name>` はコンテナ名です `<path to local directory>` はローカルディレクトリへのパスです。 タグの一意の組み合わせを使用することもできます：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]`、`[image-name:<name>]/path to local directory>`。 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:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` 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がスキャンから除外されます。

設定	説明
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。

［マスクによる除外］ウィンドウ

名前マスクによってオブジェクトのスキャン除外範囲を設定できます。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。

［**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）。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。既定では、このチェックボックスはオフです。

［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。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。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` コマンドを使用して、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に指定できるすべての設定について、指定可能なすべての値と既定値を説明します。

マルウェアのスキャンタスクの設定

設定	説明	値
`ScanFiles`	ファイルのスキャンを指定します。	`Yes`（既定値）– ファイルをスキャンします。 `No` – ファイルをスキャンしません。
`ScanBootSectors`	ブートセクタースキャンを指定します。	`Yes`（既定値）– ブートセクターをスキャンします。 `No` – ブートセクターをスキャンしません。
`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`（既定値）– プロセスメモリとカーネルメモリをスキャンします。 `No` – プロセスメモリとカーネルメモリをスキャンしません。
`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`（既定値）– スタートアップオブジェクトをスキャンします。 `No` – スタートアップオブジェクトをスキャンしません。
`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`（既定値）– アーカイブをスキャンします。 `ActionOnThreat` が `DisinfectDeleteIfNotPossible` に設定されていて、駆除が不可能な場合、本製品は圧縮ファイルの種類に応じて、感染したオブジェクトまたは脅威を含む圧縮ファイル全体を削除します。 `No` – アーカイブをスキャンしません。
`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`（既定値）– 自己解凍アーカイブをスキャンします。 `No` – 自己解凍型アーカイブをスキャンしません。

設定	説明	値
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 – メールデータベースのファイルをスキャンします。 No（既定値）– メールデータベースのファイルをスキャンしません。
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 – プレーンテキストのメールメッセージをスキャンします。 No（既定値）– プレーンテキストのメールメッセージをスキャンしません。
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 から 999999 0 – スキャン対象オブジェクトのサイズは無制限です。 既定値：0
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 から 9999 0 – オブジェクトのスキャン時間は無制限です。 既定値：0
ActionOnThreat	感染したオブジェクトに対して実行されるアクションを選択。	DisinfectDeleteIfNotPossible（駆除。不可能な場合は削除）は、本製品がオブジェクトのコピーをバックアップに保存した後、感染したオブジェクトの駆除を試みることを意味します。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトは削除されます。 DisinfectInformIfNotPossible（駆除。不可能な場合は通知）は、本製品がオブジェクトのコピーをバックアップに保存した後、感染したオブジェクトの駆除を試みることを意味します。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、ログにレコードが作成されます。 Informとは、感染したオブジェクトの駆除または削除を行わないことを意味します。感染したオブジェクトに関する情報は記録されます。 既定値：DisinfectDeleteIfNotPossible。
UseExcludeMasks	ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外します。	Yes – ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外します。 No（既定値）– ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外しません。
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。	既定値は定義されていません。 例： UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外できるようにします。	Yes - ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外します。 No（既定値）：ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外しません。

設定	説明	値
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。	設定値では大文字と小文字が区別されます。 既定値は定義されていません。 例： UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux
UseGlobalExclusions	スキャンのグローバル除外を有効にします。	Yes（既定値）– グローバル除外を使用します。 No – グローバル除外を使用しません。
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。	Yes（既定値）– ファイル脅威対策の除外を使用します。 No – ファイル脅威対策の除外を使用しません。
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 – 感染していないオブジェクトに関する情報をログに記録します。 No（既定値）– 感染していないオブジェクトに関する情報をログに記録しません。
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 – アーカイブ内のスキャン済みオブジェクトに関する情報をログに記録します。 No（既定値）– アーカイブ内のスキャン済みオブジェクトに関する情報をログに記録しません。
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 – 処理されていないオブジェクトに関する情報をログに記録します。 No（既定値）– 処理されていないオブジェクトに関する情報をログに記録しません。
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（既定値）– ヒューリスティック分析を有効にします。 No – ヒューリスティック分析を無効にします。
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 – 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。 Medium – 中間のヒューリスティック分析レベルで、システムへの負荷ともバランスが取れています。 Deep – 最も徹底的なスキャンを行い、システムへの負荷が最大となります。 Recommended（既定値）– 推奨値。
UseIChecker	iChecker 技術の使用を指定します。	Yes（既定値）– iChecker 技術の使用を有効にします。 No – iChecker 技術の使用を無効にします。
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。	AllObjects – すべてのデバイスのブートセクターをスキャンします。 < デバイス名マスク > – 指定したマスクと名前が一致するデバイスのブートセクターをスキャンします。 既定値 – /** – デバイス名にあるすべての文字。「/」も含まれます。

設定	説明	値
[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：`All objects`。 例： `AreaDesc=" Mail bases scan "`
`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`（既定値）– 指定された範囲をスキャンします。 `No` – 指定された範囲をスキャンしません。
`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：`*`（すべてのオブジェクトをスキャン） 例： `AreaMask.item_< 項目番号 >=*doc`
`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へのパス >** – 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。 `Shared:NFS` – NFS プロトコルによってアクセスできるデバイスのファイルシステムリソースをスキャンします。 `Shared:SMB` – Samba プロトコルを使用してアクセスできるデバイスのファイルシステムリソースをスキャンします。 `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リモートディレクトリをスキャンします。 `Mounted:SMB` – 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をスキャンします。 `AllRemoteMounted` – Samba 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スキャンします。 `AllShared` – Samba プロトコルと NFS プロトコルを使用してアクセス可能なデバイスのすべてのファイルシステムリソースをスキャンします。 `<file system type>` – 指定されたファイルシステムデバイスのすべてのリソースをスキャンします。
[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。	既定値は定義されていません。
`UseScanArea`	指定された範囲のスキャンの除外を指定します。	`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_#`	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：`*`（すべてのオブジェクトを除外）

設定	説明	値
Path	除外するオブジェクトを含むディレクトリのパス。	<path to local directory> – 指定されたディレクトリ（サブディレクトリを含む）内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。 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、次の除外を追加できます：/.snapshots/*/snapshot/。 「/」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。 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スキャンから除外します。 Mounted:SMB – 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をスキャンから除外します。 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スキャンから除外します。 <file system type> – 指定されたファイルシステムデバイスのすべてのリソースをスキャンから除外します。 リモートディレクトリは、タスクの開始前にマウントされていた場合にのみ、アプリケーションによるスキャンから除外されます。タスクの開始後にマウントされたリモートディレクトリはスキャンから除外されません。

設定	説明	値

コマンドラインでのファイルとディレクトリのオブジェクトスキャン

次のコマンドを使用して、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：`kesl-control --scan-file`。

オブジェクトスキャンは、事前定義済みタスク *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 <アクション>]
```

説明：

- **<パス>**は、スキャンするファイルまたは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` **<アクション>** は、感染したオブジェクトに対して製品が実行するアクションです。可能な値：`DisinfectDeleteIfNotPossible, DisinfectInformIfNotPossible,Inform`。`--action` オプションを指定しないと、アプリケーションは `DisinfectDeleteIfNotPossible` 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について、指定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_#]` セクションおよび `[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	値
`ScanFiles`	ファイルのスキャンを指定します。	`Yes`（既定値）– ファイルをスキャンします。 `No` – ファイルをスキャンしません。
`ScanBootSectors`	ブートセクタースキャンを指定します。	`Yes` – ブートセクターをスキャンします。 `No` （既定値）– ブートセクターをスキャンしません。
`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` – プロセスメモリとカーネルメモリをスキャンします。 `No`（既定値）– プロセスメモリとカーネルメモリをスキャンしません。

設定	説明	値
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 – スタートアップオブジェクトをスキャンします。 No （既定値）– スタートアップオブジェクトをスキャンしません。
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（既定値）– アーカイブをスキャンします。 ActionOnThreat が DisinfectDeleteIfNotPossible に設定されていて、駆除が不可能な場合、本製品は圧縮ファイルの種類に応じて、感染したオブジェクトまたは脅威を含む圧縮ファイル全体を削除します。 No – アーカイブをスキャンしません。
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 （既定値）– 自己解凍アーカイブをスキャンします。 No – 自己解凍型アーカイブをスキャンしません。
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 – メールデータベースのファイルをスキャンします。 No（既定値）– メールデータベースのファイルをスキャンしません。
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 – プレーンテキストのメールメッセージをスキャンします。 No（既定値）– プレーンテキストのメールメッセージをスキャンしません。
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 から 999999 0 – スキャン対象オブジェクトのサイズは無制限です。 既定値：0
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 から 9999 0 – オブジェクトのスキャン時間は無制限です。 既定値：0
ActionOnThreat	感染したオブジェクトに対して実行されるアクションを選択。	DisinfectDeleteIfNotPossible（駆除。不可能な場合は削除）は、本製品がオブジェクトのコピーをバックアップに保存した後、感染したオブジェクトの駆除を試みることを意味します。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトは削除されます。 DisinfectInformIfNotPossible（駆除。不可能な場合は通知）は、本製品がオブジェクトのコピーをバックアップに保存した後、感染したオブジェクトの駆除を試みることを意味します。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、ログにレコードが作成されます。 Inform とは、感染したオブジェクトの駆除または削除を行わないことを意味します。感染したオブジェクトに関する情報は記録されます。 既定値：DisinfectDeleteIfNotPossible。

設定	説明	値
UseExcludeMasks	ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外します。	Yes – ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外します。 No（既定値）– ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外しません。
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。	既定値は定義されていません。 例： UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外できるようにします。	Yes - ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外します。 No（既定値）：ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外しません。
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。	設定値では大文字と小文字が区別されます。 既定値は定義されていません。 例： UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux
UseGlobalExclusions	スキャンのグローバル除外を有効にします。	Yes（既定値）– グローバル除外を使用します。 No – グローバル除外を使用しません。
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。	Yes（既定値）– ファイル脅威対策の除外を使用します。 No – ファイル脅威対策の除外を使用しません。
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 – 感染していないオブジェクトに関する情報をログに記録します。 No（既定値）– 感染していないオブジェクトに関する情報をログに記録しません。
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 – アーカイブ内のスキャン済みオブジェクトに関する情報をログに記録します。 No（既定値）– アーカイブ内のスキャン済みオブジェクトに関する情報をログに記録しません。
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 – 処理されていないオブジェクトに関する情報をログに記録します。 No（既定値）– 処理されていないオブジェクトに関する情報をログに記録しません。
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（既定値）– ヒューリスティック分析を有効にします。 No – ヒューリスティック分析を無効にします。

設定	説明	値
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 – 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。 Medium – 中間のヒューリスティック分析レベルで、システムへの負荷ともバランスが取れています。 Deep – 最も徹底的なスキャンを行い、システムへの負荷が最大となります。 Recommended（既定値）– 推奨値。
UseIChecker	iChecker 技術の使用を指定します。	Yes（既定値）– iChecker 技術の使用を有効にします。 No – iChecker 技術の使用を無効にします。
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。	AllObjects – すべてのデバイスのブートセクターをスキャンします。 < デバイス名マスク > – 指定したマスクと名前が一致するデバイスのブートセクターをスキャンします。 既定値 – /** – デバイス名にあるすべての文字。「/」も含まれます。
[ScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	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：All objects。 例： AreaDesc=" Scanning of email databases "
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（既定値）– 指定された範囲をスキャンします。 No – 指定された範囲をスキャンしません。
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：*（すべてのオブジェクトをスキャン） 例： AreaMask.item_< 項目番号 >=*doc

設定	説明	値
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へのパス > –** 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。 **Shared:NFS –** NFS プロトコルによってアクセスできるデバイスのファイルシステムリソースをスキャンします。 **Shared:SMB –** Samba プロトコルを使用してアクセスできるデバイスのファイルシステムリソースをスキャンします。 **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リモートディレクトリをスキャンします。 **Mounted:SMB –** 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をスキャンします。 **AllRemoteMounted –** Samba 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スキャンします。 **AllShared –** Samba プロトコルと NFS プロトコルを使用してアクセス可能なデバイスのすべてのファイルシステムリソースをスキャンします。 **<file system type> –** 指定されたファイルシステムデバイスのすべてのリソースをスキャンします。
[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。	既定値は定義されていません。
UseScanArea	指定された範囲のスキャンの除外を指定します。	**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_#	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：*（すべてのオブジェクトを除外）

設定	説明	値
Path	除外するオブジェクトを含むディレクトリのパス。	<path to local directory> – 指定されたディレクトリ（サブディレクトリを含む）内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。 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、次の除外を追加できます：/.snapshots/*/snapshot/。 「/」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。 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スキャンから除外します。 Mounted:SMB – 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をスキャンから除外します。 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スキャンから除外します。 <file system type> – 指定されたファイルシステムデバイスのすべてのリソースをスキャンから除外します。 リモートディレクトリは、タスクの開始前にマウントされていた場合にのみ、アプリケーションによるスキャンから除外されます。タスクの開始後にマウントされたリモートディレクトリはスキャンから除外されません。

設定	説明	値

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。

root ユーザーが NFSv4 プロトコル経由でデバイスにマウントされたリモートディレクトリにアクセスできない場合、すべてのアプリケーションに対してそのようなファイルへのアクセスがブロックされます。

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

  特殊な用途の parsecfs ファイルシステム (Astra Linux Special Edition) を使用するオペレーティングシステムで実行する場合は、このファイルシステムのマウントパスをスキャンの除外リストに追加することを推奨します。
- 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する	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する	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する	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。

設定	説明
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	本製品が感染を検知したオブジェクトに対して実行する処理を選択できます： • **駆除する。駆除できない場合は削除する**（既定）。この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトは削除されます。 • **駆除する。駆除できない場合は通知する**。この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、ログにレコードが作成されます。 • **通知する**。この処理を選択すると、本製品は感染したオブジェクトに関するレコードをログインに作成します。
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、変更、削除、上に移動、下に移動。 また、［**インポート**］をクリックしてファイルからスキャン範囲のリストをインポートすることも、［**エクスポート**］をクリックしてスキャン範囲のリストを JSON 形式 で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、スキャン範囲のリストを置き換えるか、既存のリストにスキャン範囲を追加するように求められます。

［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。 • **All remote mounted** – 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。

設定	説明
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:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` 説明： `<id>` はコンテナIDです。 `<name>` はコンテナ名です `<path to local directory>` はローカルディレクトリへのパスです。 タグの一意の組み合わせを使用することもできます：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]`、`[image-name:<name>]/path to local directory>`。 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:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` 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。

[スキャン範囲] セクション

簡易スキャンタスクのスキャン範囲の設定

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する	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

このテーブルには、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。

テーブル内の項目は、追加、編集、削除できます。

[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	[**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。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。
グローバルの除外リストを使用	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。

設定	説明
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

このウィンドウには、スキャンの除外範囲が表示されます。テーブル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。

除外範囲の設定

設定	説明
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
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。

既定では、除外範囲のテーブルは空です。テーブル内の項目は、追加、編集、削除できます。

インポートボタンを使用してファイルから除外リストをインポートしたり、**エクスポート**ボタンを使用して除外リストをJSONファイルにエクスポートしたり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。

[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。 • **All remote mounted** – 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。

設定	説明
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:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` 説明： `<id>` はコンテナIDです。 `<name>` はコンテナ名です `<path to local directory>` はローカルディレクトリへのパスです。 タグの一意の組み合わせを使用することもできます：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]`、`[image-name:<name>]/path to local directory>`。 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:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` 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。

設定	説明
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。

［マスクによる除外］ウィンドウ

名前マスクによってオブジェクトのスキャン除外範囲を設定できます。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。

［**追加**］または［**編集**］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）。

インポートボタンを使用してファイルから除外リストをインポートしたり、**エクスポート**ボタンを使用して除外リストをJSONファイルにエクスポートしたり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。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。既定では、このチェックボックスはオフです。

［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。

［**追加**］または［**編集**］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。

インポートボタンを使用してファイルから除外リストをインポートしたり、**エクスポート**ボタンを使用して除外リストをJSONファイルにエクスポートしたり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。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。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。テーブル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
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
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。

テーブル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。

指定された範囲にあるオブジェクトは、範囲のテーブル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。

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、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。 • **All remote mounted** – 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。

設定	説明
	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:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` 説明： `<id>` はコンテナIDです。 `<name>` はコンテナ名です `<path to local directory>` はローカルディレクトリへのパスです。 タグの一意の組み合わせを使用することもできます：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]`、`[image-name:<name>]/path to local directory>`。 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:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` 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。

［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、Kaspersky Endpoint Security がファイルをスキャンします。 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、Kaspersky Endpoint Security がブートセクターをスキャンします。 このチェックボックスをオフにすると、Kaspersky Endpoint Security はブートセクター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。
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する	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、Kaspersky Endpoint Security はスタートアップオブジェクトをスキャンします。 このチェックボックスをオフにすると、Kaspersky Endpoint Security はスタートアップ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**］ウィンドウが開き、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。
グローバルの除外リストを使用	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

このテーブルには、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。

テーブル内の項目は、追加、編集、削除できます。

［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。

スキャンの設定

設定	説明
アーカイブをスキャンする	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する	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する	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。

設定	説明
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。

［脅威検出］ウィンドウでの処理

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
脅威の検知時の処理	本製品が感染を検知したオブジェクトに対して実行する処理を選択できます： • **駆除する。駆除できない場合は削除する**（既定）。この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトは削除されます。 • **駆除する。駆除できない場合は通知する**。この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、ログにレコードが作成されます。 • **通知する**。この処理を選択すると、本製品は感染したオブジェクトに関するレコードをログインに作成します。

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

このウィンドウには、スキャンの除外範囲が表示されます。テーブル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。

除外範囲の設定

設定	説明
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
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。

既定では、除外範囲のテーブルは空です。テーブル内の項目は、追加、編集、削除できます。

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。

[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。

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、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。 • **All remote mounted** – 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:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` 説明： `<id>` はコンテナIDです。 `<name>` はコンテナ名です `<path to local directory>` はローカルディレクトリへのパスです。 タグの一意の組み合わせを使用することもできます：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]`、`[image-name:<name>]/path to local directory>`。 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:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` 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がスキャンから除外されます。

設定	説明
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。

［マスクによる除外］ウィンドウ

名前マスクによってオブジェクトのスキャン除外範囲を設定できます。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。

［**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）。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。既定では、このチェックボックスはオフです。

［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。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。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。

設定	説明	値
ScanFiles	ファイルのスキャンを指定します。	Yes – ファイルをスキャンします。 No （既定値）– ファイルをスキャンしません。
ScanBootSectors	ブートセクタースキャンを指定します。	Yes（既定値）– ブートセクターをスキャンします。 No – ブートセクターをスキャンしません。
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 （既定値）– プロセスメモリとカーネルメモリをスキャンします。 No – プロセスメモリとカーネルメモリをスキャンしません。
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（既定値）– スタートアップオブジェクトをスキャンします。 No – スタートアップオブジェクトをスキャンしません。
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（既定値）– アーカイブをスキャンします。 ActionOnThreat が DisinfectDeleteIfNotPossible に設定されていて、駆除が不可能な場合、本製品は圧縮ファイルの種類に応じて、感染したオブジェクトまたは脅威を含む圧縮ファイル全体を削除します。 No – アーカイブをスキャンしません。
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（既定値）– 自己解凍アーカイブをスキャンします。 No – 自己解凍型アーカイブをスキャンしません。
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 – メールデータベースのファイルをスキャンします。 No（既定値）– メールデータベースのファイルをスキャンしません。
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 – プレーンテキストのメールメッセージをスキャンします。 No（既定値）– プレーンテキストのメールメッセージをスキャンしません。
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 から 999999 0 – スキャン対象オブジェクトのサイズは無制限です。 既定値：0
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 から 9999 0 – オブジェクトのスキャン時間は無制限です。 既定値：0

設定	説明	値
ActionOnThreat	感染したオブジェクトに対して実行されるアクションを選択。	DisinfectDeleteIfNotPossible（駆除。不可能な場合は削除）は、本製品がオブジェクトのコピーをバックアップに保存した後、感染したオブジェクトの駆除を試みることを意味します。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトは削除されます。 DisinfectInformIfNotPossible（駆除。不可能な場合は通知）は、本製品がオブジェクトのコピーをバックアップに保存した後、感染したオブジェクトの駆除を試みることを意味します。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、ログにレコードが作成されます。 Informとは、感染したオブジェクトの駆除または削除を行わないことを意味します。感染したオブジェクトに関する情報は記録されます。 既定値：DisinfectDeleteIfNotPossible。
UseExcludeMasks	ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外します。	Yes – ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外します。 No（既定値）– ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外しません。
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。	既定値は定義されていません。 例： UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外できるようにします。	Yes - ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外します。 No（既定値）：ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外しません。
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。	設定値では大文字と小文字が区別されます。 既定値は定義されていません。 例： UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux
UseGlobalExclusions	スキャンのグローバル除外を有効にします。	Yes（既定値）– グローバル除外を使用します。 No – グローバル除外を使用しません。

設定	説明	値
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。	Yes（既定値）– ファイル脅威対策の除外を使用します。 No – ファイル脅威対策の除外を使用しません。
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 – 感染していないオブジェクトに関する情報をログに記録します。 No（既定値）– 感染していないオブジェクトに関する情報をログに記録しません。
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 – アーカイブ内のスキャン済みオブジェクトに関する情報をログに記録します。 No（既定値）– アーカイブ内のスキャン済みオブジェクトに関する情報をログに記録しません。
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 – 処理されていないオブジェクトに関する情報をログに記録します。 No（既定値）– 処理されていないオブジェクトに関する情報をログに記録しません。
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（既定値）– ヒューリスティック分析を有効にします。 No – ヒューリスティック分析を無効にします。
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 – 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。 Medium – 中間のヒューリスティック分析レベルで、システムへの負荷ともバランスが取れています。 Deep – 最も徹底的なスキャンを行い、システムへの負荷が最大となります。 Recommended（既定値）– 推奨値。
UseIChecker	iChecker 技術の使用を指定します。	Yes（既定値）– iChecker 技術の使用を有効にします。 No – iChecker 技術の使用を無効にします。
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。	AllObjects – すべてのデバイスのブートセクターをスキャンします。 < デバイス名マスク > – 指定したマスクと名前が一致するデバイスのブートセクターをスキャンします。 既定値 – /** – デバイス名にあるすべての文字。「/」も含まれます。
[ScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	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：All objects。 例： AreaDesc=" Mail bases scan "
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（既定値）– 指定された範囲をスキャンします。 No – 指定された範囲をスキャンしません。
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：*（すべてのオブジェクトをスキャン） 例： AreaMask.item_< 項目番号 >=*doc

設定	説明	値
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へのパス > –** 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。 **Shared:NFS –** NFS プロトコルによってアクセスできるデバイスのファイルシステムリソースをスキャンします。 **Shared:SMB –** Samba プロトコルを使用してアクセスできるデバイスのファイルシステムリソースをスキャンします。 **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リモートディレクトリをスキャンします。 **Mounted:SMB –** 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をスキャンします。 **AllRemoteMounted –** Samba 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スキャンします。 **AllShared –** Samba プロトコルと NFS プロトコルを使用してアクセス可能なデバイスのすべてのファイルシステムリソースをスキャンします。 **<file system type> –** 指定されたファイルシステムデバイスのすべてのリソースをスキャンします。
[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。	既定値は定義されていません。
UseScanArea	指定された範囲のスキャンの除外を指定します。	**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_#	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：*（すべてのオブジェクトを除外）

設定	説明	値
Path	除外するオブジェクトを含むディレクトリのパス。	<path to local directory> – 指定されたディレクトリ（サブディレクトリを含む）内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。 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、次の除外を追加できます：/.snapshots/*/snapshot/。 「/」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。 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スキャンから除外します。 Mounted:SMB – 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をスキャンから除外します。 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スキャンから除外します。 <file system type> – 指定されたファイルシステムデバイスのすべてのリソースをスキャンから除外します。 リモートディレクトリは、タスクの開始前にマウントされていた場合にのみ、アプリケーションによるスキャンから除外されます。タスクの開始後にマウントされたリモートディレクトリはスキャンから除外されません。

設定	説明	値

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。

Web コンソールでのリムーバブルドライブスキャンの設定

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管理できます（**製品設定 → ホスト脅威対策 → リムーバブルドライブスキャン**）。

管理コンソールでのリムーバブルドライブスキャンの設定

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スキャンの設定を管理できます（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**ローカルタスク → リムーバブルドライブスキャン**）。

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。 リムーバブルメディアでは、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、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、マルウェアスキャンタスクの既定の設定を使用して実行されます。

設定	説明
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。 リムーバブルメディアでは、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、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、マルウェアスキャンタスクの既定の設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、リムーバブルメディア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*を実行しません。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* 種別のタスク）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メディア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` – リムーバブルメディア（CD/DVD、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` – リムーバブルメディア（CD/DVD、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。 リムーバブルメディアでは、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、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`（デフォルト値）- リムーバブルメディアがデバイスに接続されているときにスキャンしません。

設定	説明	値
`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。 リムーバブルメディアでは、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、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、ファイルはブロックされません。	`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。

コンテナスキャン

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*（*コンテナスキャン*、*コンテナ監視*）を使用すると、起動中の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。

コンテナスキャン機能を使用するには、この機能を含むライセンスが必要です。

本製品は、Docker コンテナ管理システム、CRI-O 環境、Podman および runc ユーティリティとの連携をサポートしています。

Docker 28.5.2 以前との連携に対応しています。

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。本製品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適用されます。

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、コマンドラインではコンテナ監視のコンポーネントのステータスが**タスクは使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。

  Docker 28.5.2 以前との連携に対応しています。

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（**アプリケーション設定 → 全般設定 → コンテナスキャン設定**）で、コンテナスキャン設定コンポーネントを管理できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定 → コンテナスキャン設定**）で、アプリケーショントレース設定を管理できます。

コンテナの監視設定

設定	説明
名前空間とコンテナ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、[**コンテナスキャン設定**] ウィンドウが表示されます。

[コンテナスキャン設定] 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 コンテナ管理システム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 28.5.2 以前に対応しています。
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 を使用する	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。

設定	説明
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

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、コマンドラインのオプションを使用して、`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、コンテナスキャンの全般設定をすべて編集できます。コンテナ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。
- コマンドラインオプションを使用して、**< 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]
```

ここで、`--json` を指定すると、設定が JSON 形式で出力されます。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

コンテナ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。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

設定情報ファイルを使用してコンテナ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. 次の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、コンテナスキャンの全般設定が含まれる設定情報ファイルへの完全パスです。
   - JSON 構成ファイルから設定をインポートする場合は、`--json` オプションを指定します。`--json` オプション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。

コマンドラインのオプションを使ってコンテナ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>]`

ここで、**<設定名>=<設定値>** は、コンテナスキャンの全般設定のいずれかの名前と値です。

指定されたコンテナ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、複数のコンテナスキャンタスクを同時実行できます。

この機能を使用するには、コンテナスキャンタスク対象のライセンスが必要です。

本製品は、Docker コンテナ管理システム、CRI-O 環境、Podman および runc ユーティリティとの連携をサポートしています。

Docker 28.5.2 以前との連携に対応しています。

コンテナスキャンを開始し、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。

設定	説明
アーカイブをスキャンする	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する	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する	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。

設定	説明
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	本製品が感染を検知したオブジェクトに対して実行する処理を選択できます： • **駆除する。駆除できない場合は削除する**（既定）。この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトは削除されます。 • **駆除する。駆除できない場合は通知する**。この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、ログにレコードが作成されます。 • **通知する**。この処理を選択すると、本製品は感染したオブジェクトに関するレコードをログインに作成します。
コンテナをスキャン	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**処理を選択することを推奨します。
イメージをスキャンする	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。

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。
グローバルの除外リストを使用	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

名前マスクによってオブジェクトのスキャン除外範囲を設定できます。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。

［**追加**］または［**編集**］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）。

インポートボタンを使用してファイルから除外リストをインポートしたり、**エクスポート**ボタンを使用して除外リストをJSONファイルにエクスポートしたり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。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。既定では、このチェックボックスはオフです。

［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。

［**追加**］または［**編集**］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。

インポートボタンを使用してファイルから除外リストをインポートしたり、**エクスポート**ボタンを使用して除外リストをJSONファイルにエクスポートしたり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。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。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
コンテナをスキャン	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	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、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**処理を選択することを推奨します。
イメージをスキャンする	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。

設定	説明
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。

スキャンの設定

設定	説明
アーカイブをスキャンする	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する	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する	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。

設定	説明
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。

［脅威検出］ウィンドウでの処理

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
脅威の検知時の処理	本製品が感染を検知したオブジェクトに対して実行する処理を選択できます： • **駆除する。駆除できない場合は削除する**（既定）。この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトは削除されます。 • **駆除する。駆除できない場合は通知する**。この処理を選択した場合、本製品はオブジェクトのコピーをバックアップに保存して、感染したオブジェクトの駆除を試みます。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、ログにレコードが作成されます。 • **通知する**。この処理を選択すると、本製品は感染したオブジェクトに関するレコードをログインに作成します。

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
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。

設定のグループ	説明
グローバルの除外リストを使用	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

名前マスクによってオブジェクトのスキャン除外範囲を設定できます。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。

［**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）。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。既定では、このチェックボックスはオフです。

［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。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。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コンテナスキャン

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。

コンテナの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。

コンテナの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 `*` の記号が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。

設定	説明	値
ContainerScanAction	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。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。	StopContainerIfFailed（既定値）– ア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。この値を選択した場合、コンテナで実行される処理は、コンテナとイメージ内のオブジェクトに適用される ActionOnThreat 設定にも依存します（次の表を参照）。ActionOnThreat が DisinfectDeleteIfNotPossible に設定されていて、本製品が処理の実行中に感染したオブジェクトを駆除または削除できない場合、コンテナは停止されます。 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。

コンテナのスキャンタスクの設定

設定	説明	値
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（既定値）– アーカイブをスキャンします。 ActionOnThreat が DisinfectDeleteIfNotPossible に設定されていて、駆除が不可能な場合、本製品は圧縮ファイルの種類に応じて、感染したオブジェクトまたは脅威を含む圧縮ファイル全体を削除します。 No – アーカイブをスキャンしません。
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（既定値）– 自己解凍アーカイブをスキャンします。 No – 自己解凍型アーカイブをスキャンしません。
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 – メールデータベースのファイルをスキャンします。 No（既定値）– メールデータベースのファイルをスキャンしません。
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 – プレーンテキストのメールメッセージをスキャンします。 No（既定値）– プレーンテキストのメールメッセージをスキャンしません。
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 から 9999 0 – オブジェクトのスキャン時間は無制限です。 既定値：0

設定	説明	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 から 999999 0 – スキャン対象オブジェクトのサイズは無制限です。 既定値：0
ActionOnThreat	感染したオブジェクトに対して実行されるアクションを選択。	DisinfectDeleteIfNotPossible（駆除。不可能な場合は削除）は、本製品がオブジェクトのコピーをバックアップに保存した後、感染したオブジェクトの駆除を試みることを意味します。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、感染したオブジェクトは削除されます。 DisinfectInformIfNotPossible（駆除。不可能な場合は通知）は、本製品がオブジェクトのコピーをバックアップに保存した後、感染したオブジェクトの駆除を試みることを意味します。駆除できない場合（オブジェクトの種別またはオブジェクト内の脅威の種別が駆除できない場合など）、ログにレコードが作成されます。 Inform とは、感染したオブジェクトの駆除または削除を行わないことを意味します。感染したオブジェクトに関する情報は記録されます。 既定値：DisinfectDeleteIfNotPossible。
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 – ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外します。 No（既定値）– ExcludeMasks.item_# 設定で指定されたオブジェクトをスキャンから除外しません。
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。	既定値は定義されていません。 例： UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
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 - ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外します。 No（既定値）：ExcludeThreats.item_# 設定で指定された脅威を含むオブジェクトをスキャンから除外しません。
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。	設定値では大文字と小文字が区別されます。 既定値は定義されていません。 例： UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux

設定	説明	値
UseGlobalExclusions	スキャンのグローバル除外を有効にします。	Yes（既定値）– グローバル除外を使用します。 No – グローバル除外を使用しません。
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 – 感染していないオブジェクトに関する情報をログに記録します。 No（既定値）– 感染していないオブジェクトに関する情報をログに記録しません。
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 – アーカイブ内のスキャン済みオブジェクトに関する情報をログに記録します。 No（既定値）– アーカイブ内のスキャン済みオブジェクトに関する情報をログに記録しません。
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 – 処理されていないオブジェクトに関する情報をログに記録します。 No（既定値）– 処理されていないオブジェクトに関する情報をログに記録しません。
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（既定値）– ヒューリスティック分析を有効にします。 No – ヒューリスティック分析を無効にします。
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 – 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。 Medium – 中間のヒューリスティック分析レベルで、システムへの負荷ともバランスが取れています。 Deep – 最も徹底的なスキャンを行い、システムへの負荷が最大となります。 Recommended（既定値）– 推奨値。
UseIChecker	iChecker 技術の使用を指定します。	Yes（既定値）– iChecker 技術の使用を有効にします。 No – iChecker 技術の使用を無効にします。

コンテナとイメージのオブジェクトスキャン

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、**kesl-control --scan-container** コマンドを使用して実行できます。

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 <ID / 名前 [: タグ ]>
```

ここで、**<ID/名前 [: 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。

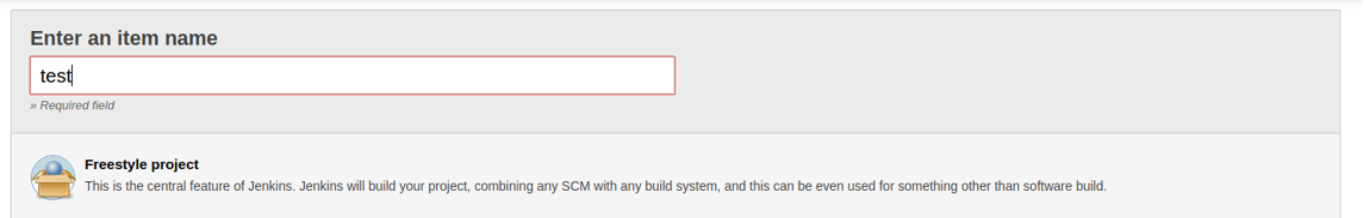
例：
my_container という名前のコンテナをスキャンします：
`kesl-control --scan-container my_container`
my_image（すべてのタグ）という名前のイメージをスキャンします：
`kesl-control --scan-container my_image*`

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：

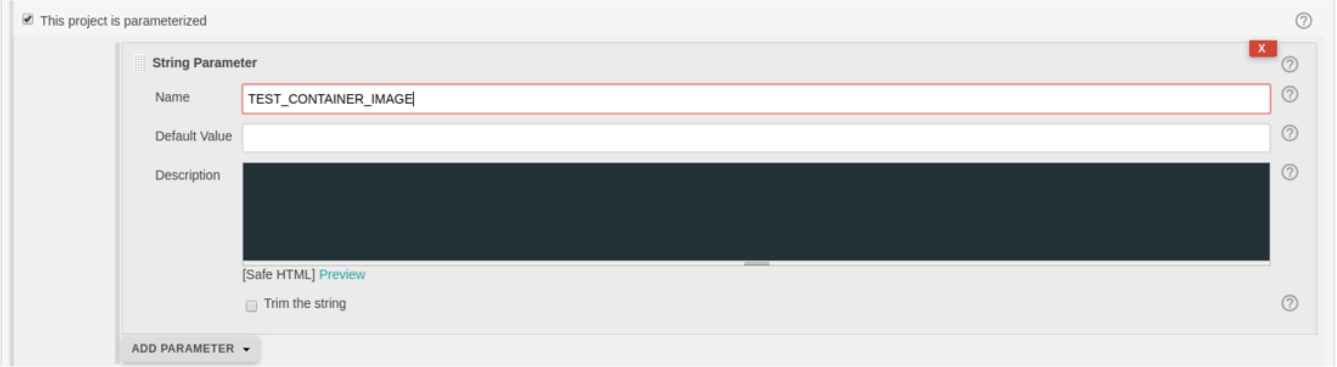
1. Jenkins ノードに Kaspersky Endpoint Security をインストールします。
2. Jenkins ノードに Docker Engine をインストールします。
   詳細は、Docker Engine のガイドを参照してください。
3. Kaspersky Endpoint Security の管理者権限を Jenkins ユーザーに付与します：
   `kesl-control --grant-role admin <ユーザー名 Jenkins>`
4. Jenkins ユーザーを docker グループに追加します：
   `sudo usermod -aG docker <ユーザー名 Jenkins>`
   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では、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。

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コンポーネントを有効にする前に、オペレーティングシステムの他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。

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。

  Red Hat Enterprise Linuxコードベースに基づく一部のOS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（`kesl-control -F --query`）を使用してのみ表示できます。

- 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、事前定義されたネットワークにマッピングします。使用可能なネットワークに IP アドレスやサブネットを追加したり、使用可能なネットワークからアドレスを削除したりすることができます。

- 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。

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。このルールにより、選択したデータプロトコルの、特定のポートを通じた、受信ネットワークトラフィックと送信ネットワークトラフィックが制限されます。

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。

定義済みの使用可能なネットワークについて

*使用可能なネットワーク*とは、定義済みの IP アドレスまたはサブネットのグループです。使用可能なネットワークでは、IP アドレスやサブネットごとに個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することができます。使用可能なネットワークは、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、3 つの定義済みネットワークがあります：

- **パブリック**：ウイルス対策アプリケーション、ファイアウォール、フィルターによって保護されていないネットワーク（インターネットカフェのネットワークなど）。
- **ローカル**：ユーザーがデバイス上のファイルやプリンターにアクセスできる権限を持つネットワーク（企業内LANやホームネットワークなど）。
- **許可**：デバイスが攻撃や不正なデータアクセス試行の対象とされない、安全なネットワークです。

新しい事前定義ネットワークの作成や既存のネットワークの削除はできませんが、ネットワークへの IP アドレスやサブネットの追加や削除は可能です。

Web Console でのファイアウォール管理

Web コンソールでは、ポリシープロパティ（**製品設定 → コミュニケーションと危険サイトブロック → ファイアウォール**）でFirewall 設定を管理できます。

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、ポリシープロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**脅威対策 → Firewall 管理**）で、Firewall 管理設定を管理できます。

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： • ネットワーク接続を**許可**する（既定値）。 • ネットワーク接続を**ブロック**する。

設定	説明
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： • 受信パケットを**許可**する（既定値）。 • 受信パケットを**ブロック**する。
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。

［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
Protocol	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**

設定	説明
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のみを監視します。 • **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接続のみを監視します。 • **送受信**（既定の設定）。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接続と送信接続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のみを監視します。 • **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接続のみを監視します。
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 タイプ**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またはポート範囲を指定します。 **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またはポート範囲を指定します。 **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。 • **指定したアドレスまたはアドレス範囲**。このオプションをオンにすると、次の表で指定された 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。表の上にある **[追加]** ボタンをクリックすると、[**IP アドレスを追加してください**] ウィンドウが開き、デバイスの IP アドレス、ネットワークアドレス、または IP アドレスの範囲を指定できます。 • **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。 • **指定したアドレスまたはアドレス範囲**。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、次のフィールドで指定されます。表の上にある **[追加]** ボタンをクリックすると、[**IP アドレスを追加してください**] ウィンドウが開き、デバイスの IP アドレス、ネットワークアドレス、または IP アドレスの範囲を指定できます。
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。

［IP アドレスを追加してください］ウィンドウ

このウィンドウでは、デバイスの IP アドレス、ネットワークアドレス、または IP アドレスの範囲を指定できます。

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。

［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テーブルは空です。

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。

［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。

ファイアウォール管理の定義済みタスクの設定を編集することで、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。
- 本製品で作成されたファイアウォールルールを表示するには、次のコマンドを使用します：`kesl-control -F --query`

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。

設定	説明	値
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 – 受信接続のみを監視します。 Outgoing または Out – 送信接続のみを監視します。 IncomingPacket または InPacket – 受信パケットのみを監視します。 OutgoingPacket または OutPacket – 送信パケットのみを監視します。 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 – d.d.d.d – IPv4 アドレスの範囲。 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:x:x:x:x – x:x:x:x:x:x:x:x – IPv6 アドレスの範囲。 x:x:x:x:x:x:x:x/p – IPv6 アドレスのサブネット。p は 0 から 128 までの数字です。簡潔にするために :: を使用できます。
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 – d.d.d.d – IPv4 アドレスの範囲。 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:x:x:x:x – x:x:x:x:x:x:x:x – IPv6 アドレスの範囲。 x:x:x:x:x:x:x:x/p – IPv6 アドレスのサブネット。p は 0 から 128 までの数字です。簡潔にするために :: を使用できます。
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）

設定	説明	値
[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）

コマンドラインでの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 <ルール名>] [--action <処理>] [--protocol <プロトコル>] [--direction <方向>] [--remote <リモートアドレス>[:<ポートまたはポート範囲>]] [--local <ローカルアドレス>[:<ポートまたはポート範囲>]] [--at <インデックス>]
```

説明：

- `--name <ルール名>` 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る接続に対して実行する処理です。
- `--protocol <プロトコル>` は、監視するネットワークアクティビティの通信プロトコルの種類です。
- `--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 [:<ポートまたはポート範囲>]>` 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 [:<ポートまたはポート範囲>]>` 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内のルールのインデックスです。`--at` オプション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 <ルール名>` 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内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 <ルール名>` 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内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内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 <ゾーン> --address <アドレス>
```

説明：

- **< ゾーン >** 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`。
- **< アドレス >** 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` **< ゾーン >** `--address` **< アドレス >**
- `kesl-control --del-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。ウェブ脅威対策は、ポート 9879 を使用して接続を傍受します。ポート 9879 が使用中の場合、アプリケーションは利用可能なポートを自動的に選択して接続を傍受します。

本製品またはウェブ脅威対策保護コンポーネントを停止または起動すると、HTTPS などの傍受されたポートへの接続が終了します。

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、ネットワーク攻撃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。

   Kaspersky Endpoint Security のヒューリスティック分析では、オペレーティングシステムにおける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 のトラフィック読み取りの除外リストを設定している場合、ウェブ脅威対策に影響します。

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（**アプリケーション設定 → コミュニケーションと危険サイトブロック → ウェブ脅威対策**）でウェブ脅威対策の設定を管理できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**脅威対策 → ウェブ脅威対策**）で、ウェブ脅威対策の設定を管理できます。

ウェブ脅威対策の設定

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。ウェブ脅威対策により、このオブジェクトをデバイスにダウンロードできます。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 は、追加、編集、削除できます。

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）。

［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。

設定	説明
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。	`Notify` – 検知されたオブジェクトのダウンロードを許可し、ブロックさ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グに記録します。 `Block`（既定値）– 検知されたオブジェクトへのアクセスをブロックし、ブロックさ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グに記録します。
`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ンクのデータベースに存在するかどうかをチェックします。 `No` – リンクが悪意のあるリンクのデータベースに存在するかどうかをチェックしません。
`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リンクのデータベースに存在するかどうかをチェックします。 `No` – リンクがフィッシングリンクのデータベースに存在するかどうかをチェックしません。
`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検知にヒューリスティック分析を使用します。この値を指定すると、ヒューリスティック分析のレベルが `Light` に設定されます（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）。ウェブ脅威対策のヒューリスティック分析のレベルは変更できません。 `No` – 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ータ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クのデータベースに存在するかどうかをチェックしません。
`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含む URL のデータベースにリ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含む URL のデータベースにリンクが登録されているかをチェックしません。

設定	説明	値
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_# 設定を使用して、信頼する URL を指定できます。	Yes（既定値）– 信頼する URL のリストを使用します。 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。

ネットワークトラフィックのスキャン

ネットワークトラフィックスキャンの設定は、ウェブ脅威対策、ネットワーク脅威対策、メール脅威対策、およびウェブコントロールによって使用されます。ウェブ脅威対策コンポーネント、メール脅威対策コンポーネント、およびウェブコントロールコンポーネントは、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。

次のネットワークトラフィックのスキャン設定を管理できます：

- 暗号化された接続のスキャンを有効または無効にします。
- 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。
- ネットワークトラフィック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 root 証明書のリストを構成します。
- トラフィック読み取りの除外リストを設定します。トラフィック読み取りから除外する接続を指定できます。除外される接続は次のパラメータによって定義されます：
  - 通信方向、受信または送信。
  - リモート IP アドレス。読み取りから除外されたトラフィックの送信先または送信元の IP アドレス（通信方向によって異なります）。
  - 宛先ポート、保護対象デバイス上のポート（受信トラフィック読み取りの除外の場合）、またはリモートデバイス上のポート（送信トラフィック読み取りの除外の場合）。

  トラフィック読み取りの除外リストは TCP 接続にのみ適用され、ネットワークパケットルールには影響しません。トラフィック読み取りの除外リストは、ウェブ脅威対策、ネットワーク脅威対策、およびウェブコントロール保護コンポーネントに影響します。

  オペレーティングシステムのツールを使用して、Kaspersky Endpoint Security のトラフィック読み取りの除外リストを設定することもできます。
- 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。

  NFS サーバーへのネットワーク接続を読み取る場合は、NFS サーバーが `insecure` オプション（1～1024 の範囲外のポートからの接続を受け入れる）で起動されていることを確認する必要があります。そうでなければ、NFS サーバーはそのような接続を拒否する可能性があります。
- 本製品が使用するトラフィック傍受モードを選択します。

ネットワークトラフィック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。

ネットワークトラフィック傍受モードについて

本製品は、次の 2 つのネットワークトラフィック傍受モードのいずれかで動作できます：

- *eBPF を使用します*。このオプションを選択すると、eBPF テクノロジーを使用してトラフィックを傍受します。本製品が eBPF テクノロジーを使用してネットワークトラフィックを傍受できない場合は、代わりに iptables ユーティリティが使用されます。
- *iptables を使用する*。このモードを選択すると、iptables テクノロジーを使用してトラフィックを傍受します。既定ではこのモードが選択されます。

eBPF を使用モードでは、本製品は独自の個別のネットワーク名前空間（Linux ネットワーク名前空間）を作成し、その名前空間で、ローカルネットワークインターフェイスの `tc`（Linux トラフィック制御）キューに関連付けられた eBPF プログラムを使用してネットワークパケットをリダイレクトします。リダイレクトされたネットワークトラフィックは、アクティブなネットワーク タスクに従って分析され、元のネットワークインターフェイスに戻されます。

名前空間間の通信には、`veth` 仮想ネットワークインターフェイスのペアが使用されます（ペアの両側は独自のネットワーク名前空間にあります）。

- kesl_in – kesl_worm_in ペアは、着信接続のネットワークトラフィックを送信します。
- kesl_out – kesl_worm_out ペアは、送信接続のネットワークトラフィックを送信します。

これらのインターフェイスのペアを通じて、ネットワークトラフィックは既定の名前空間から本製品によって作成された名前空間にスキャン用に送信され、同じインターフェイスを通じて分析後にトラフィックが返されます。

本製品が実行中で、ネットワーク傍受が有効になっている場合にのみ、ネットワークトラフィックがシステム内の他のネットワークインターフェイスからこれらのインターフェイスに到達します。これらのインターフェイスは、リモートデバイス間のネットワーク経由のデータ転送には使用できません。

デバイスがネットワークポート列挙攻撃の影響を受けやすい場合（ポートフィルタリング付きのオペレーティング システムのファイアウォールがローカルデバイス上で設定されている場合など）は、**eBPF を使用する**モードの選択は推奨しません。また、組織のネットワーク境界にあるデバイスでこのトラフィック傍受モードを使用することも推奨しません。

デバイスが分離されたネットワークセグメント、プライベートネットワーク、または組織のネットワーク境界内にある場合は、ネットワークトラフィック傍受うモードとして **eBPF を使用する**モードを選択できます。

トラフィック傍受モードは、Web コンソール、管理コンソール、またはコマンドラインで選択できます。

トラフィック傍受モードを変更するには、本製品を再起動する必要があります。再起動すると、接続済みのネットワーク接続が切断されます。

Web コンソールでのネットワークトラフィックのスキャン設定

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 → ネットワーク設定**、および **アプリケーション設定 → 信頼ゾーン**）でネットワークトラフィックのスキャン設定を管理できます。

管理コンソールでのネットワークトラフィックのスキャン設定

管理コンソールでは、ポリシーのプロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**セキュリティコントロール → ネットワーク設定**）で、ネットワークトラフィックのスキャン設定を管理できます。

暗号化された接続のスキャンの設定

設定	説明
暗号化された接続のスキャンを有効にする	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。
暗号化された接続の設定	このセクションには、暗号化された接続のスキャンタスクが含まれています。 • **信用できない証明書を持つドメインへの訪問**、信頼していない証明書を持つドメインにアクセスした場合に本製品が実行する必要がある処理が指定されます。 • **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。 • **ネットワークトラフィックスキャンでエラーが発生するドメインへのアクセス**によって、ネットワークトラフィックのスキャンエラーがあるドメインにアクセスした場合に本製品が実行する必要がある処理が指定されます。 • **ドメインを許可および除外リストに追加**（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**検証ポリシーは、本製品が証明書を検証するために使用する方法です： • **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。このボタンをクリックすると、［**信頼する root 証明書**］ウィンドウが表示されます。このウィンドウでは、暗号化された接続をスキャンするときに Kaspersky Endpoint Security が信頼できると見なす root 証明書のリストを設定できます。
トラフィック読み取りの除外リスト	この設定グループには［**設定**］ボタンが含まれており、これをクリックすると［**トラフィック読み取りの除外リスト**］ウィンドウが開きます。このウィンドウでは、本製品がトラフィック読み取りから除外する接続の設定を管理できます。
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。

設定	説明
詳細設定	この設定グループには［**設定**］ボタンが含まれており、これをクリックすると［**トラフィック読み取りモード**］ウィンドウが開きます。このウィンドウでは、トラフィック傍受モードを設定できます： • **eBPF を使用します**。このオプションを選択すると、eBPF テクノロジーを使用してトラフィックを傍受します。 • **iptables を使用します**（既定）。このオプションを選択すると、アプリケーションは iptables テクノロジーを使用してトラフィックを傍受します。 トラフィック傍受モードを変更するには、本製品を再起動する必要があります。再起動すると、接続済みのネットワーク接続が切断されます。

［信頼するドメイン］ウィンドウ

このリストには、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。指定したドメインへのアクセス時に確立された、接続をスキャンしません。

例：`*example.com`たとえば、`*example.com/*`、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、または削除できます。

［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 root 証明書のリストを設定できます。信頼するルート証明書のリストは、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
- 証明書のシリアル番号
- 証明書の発行元
- 証明書の開始日
- 証明書の有効期限
- 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。

証明書を追加または削除できます。

［**追加**］をクリックするとウィンドウが開き、次のいずれかの方法で信頼できる証明書のリストに証明書を追加できます：

- 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。

トラフィック読み取りの除外リストウィンドウ

この表には、本製品がトラフィック読み取りから除外する接続の設定が含まれています：

- **リモート IP アドレス**は、読み取りから除外されたトラフィックの送信先または送信元の IP アドレスです（通信方向によって異なります）。
- **宛先ポート**は、保護対象デバイス上のポート（受信トラフィック読み取りの除外の場合）またはリモートデバイス上のポート（送信トラフィック読み取りの除外の場合）です。
- **通信方向**は、接続における通信方向（受信または送信）です。

除外リストは、追加、編集、削除できます。

トラフィック読み取りの除外リストウィンドウ

このウィンドウでは、トラフィック読み取りの除外を追加できます。そのためには、次の接続設定を指定する必要があります：

- **リモート IP アドレス**は、リモートデバイスの IPv4 または IPv6 アドレスです。通信方向に応じて、指定された IP アドレスからのトラフィック（受信トラフィックの除外）または指定された IP アドレスへのトラフィック（送信トラフィックの除外）が除外されます。
- 通信方向に応じた**宛先ポート**：
  - 保護対象デバイス上のポート（受信トラフィックの除外）。リモートデバイスからこのポートへのトラフィックは読み取りから除外されます。
  - リモートデバイス上のポート（送信トラフィックの除外）。保護対象デバイスからこのポートへのトラフィックは読み取りから除外されます。
- **通信方向**は、除外された接続における通信方向です。受信トラフィックまたは送信トラフィックの除外を設定できます。

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選択されます。

設定	説明
ネットワークポートの設定	この表には、［**選択したネットワークポートのみを監視**］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。 テーブル内の項目は、追加、編集、削除できます。

コマンドラインでのネットワークトラフィックのスキャン設定

コマンドラインでは、特別な管理コマンドを使用して、ネットワークトラフィックのスキャン設定を管理できます。ネットワークトラフィックのスキャン設定管理コマンドを使用すると、次の操作ができます：

- ネットワークトラフィックのスキャン設定を管理します。
- 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。
- 暗号化された接続をスキャンするときにアプリケーションが使用する信頼された root 証明書のリストを設定します。
- トラフィック読み取りの除外リストを設定および表示します。

ネットワークトラフィックおよびスキャンする設定の表示および編集

特別なネットワークトラフィックのスキャン設定管理コマンドを使用して、次の操作ができます：

- ネットワークトラフィックのスキャン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。このファイルを使用して設定を編集できます。
- 設定情報ファイルを使用してネットワークトラフィックのスキャン設定をすべて管理します。ネットワークトラフィックのスキャン設定出力を表示するコマンドを使用して、編集可能な設定情報ファイルを取得できます。
- コマンドラインオプションを使用して、**< 設定名 >=< 設定値 >** の形式で個々の設定を編集します。ネットワークトラフィックのスキャン設定を出力するコマンドを使って設定の現在の値を取得できます。

現在のネットワークトラフィックのスキャン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-net-settings [--json]
```

ここで、`--json` を指定すると、設定が JSON 形式で出力されます。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

現在のネットワークトラフィックのスキャン設定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 <設定情報ファイルへのパス> [--json]
```

説明：

- **--file <設定情報ファイルのパス>**は、ネットワークトラフィックのスキャン設定の保存先となる設定情報ファイルのパスです。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。**--json** オプションを指定しないと、設定は INI 形式で出力されます。

設定情報ファイルを使用してネットワークスキャン設定を管理する場合：

1. 上で説明したように、ネットワークトラフィック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. 次のコマンドを実行します：

   ```
   kesl-control --set-net-settings --file <設定情報ファイルへのパス> [--json]
   ```

   説明：

   - **--file <設定情報ファイルのパス>**は、ネットワークトラフィックのスキャン設定を含む設定情報ファイルへの完全パスです。
   - **--json** を指定すると、設定情報ファイルからアプリケーションに設定が JSON 形式でインポートされます。**--json** オプション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。

   ファイルに設定されているすべてのネットワークトラフィックのスキャン設定がアプリケーションにインポートされます。

コマンドラインでネットワークトラフィックのスキャン設定を編集するには、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>]
```

ここで、**<設定名>=<設定値>**は、ネットワークトラフィックのスキャン設定のいずれか 1 つの名前と値です。

指定された設定の値が変更されます。

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、暗号化された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、暗号化された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、暗号化された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 root 証明書のリストの管理

信頼する root 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 <証明書へのパス>
```

説明：

<証明書へのパス> は、追加する証明書ファイルのパスです（PEM または DER 形式）。

信頼する root 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 <証明書のサブジェクト>
```

信頼する root 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
- 証明書の発行元
- 証明書の開始日
- 証明書の有効期限
- SHA256 証明書のフィンガープリント

トラフィック読み取りの除外リストの設定と表示

トラフィック読み取りの除外リストを追加するには、次のコマンドを実行します：

```
kesl-control --add-bypass-endpoints --direction <in|out> --remote-ip <リモート IP アドレス> --dst-port <宛先ポート>
```

説明：

- **<in|out>** は、除外された接続におけるトラフィックの方向です。受信トラフィックまたは送信トラフィックの除外を設定できます。
- **<リモート IP アドレス>** は、リモートデバイスの IPv4 または IPv6 アドレスです。通信方向に応じて、指定された IP アドレスからのトラフィック（受信トラフィックの除外）または指定された IP アドレスへのトラフィック（送信トラフィックの除外）が除外されます。
- **<宛先ポート>**は、トラフィックの方向に応じて次のようになります：
  - 保護対象デバイス上のポート（受信トラフィックの除外）。リモートデバイスからこのポートへのトラフィックは読み取りから除外されます。
  - リモートデバイス上のポート（送信トラフィックの除外）。保護対象デバイスからこのポートへのトラフィックは読み取りから除外されます。

除外では、ポートなしでリモートデバイスの IP アドレス、または IP アドレスなしで宛先ポートを指定できます。

> 受信トラフィックの除外でリモートデバイスの IP アドレスのみを指定した場合（保護対象デバイスのポートを指定しない）、リモートデバイスからのすべてのトラフィックが読み取りから除外されます。信頼するデバイスからのトラフィックに対してのみこの除外を設定することを推奨します。

設定されたトラフィック読み取り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 --list-bypass-endpoints
```

除外リストごとに次の情報が表示されます：

- 除外リストのシリアル番号
- 通信方向
- リモートデバイスの IP アドレス
- ポート番号

トラフィック読み取りの除外リストを削除するには、次のコマンドを実行します：

```
kesl-control --remove-bypass-endpoints --direction <in|out> --remote-ip <リモート IP アドレス> --dst-port <宛先ポート>
```

説明：

- `<in|out>` は、除外された接続におけるトラフィックの方向です。
- **<リモート IP アドレス>** は、トラフィックがインターセプトから除外されるリモートデバイスの IPv4 または IPv6 アドレスです（トラフィックの方向によって異なります）。
- **<宛先ポート>** は、保護対象デバイス上のポート（受信トラフィックの除外）またはリモートデバイス上のポート（送信トラフィックの除外）です。

オペレーティングシステムのツールを使用したトラフィック読み取りの除外リスト

Kaspersky Endpoint Security 設定では、トラフィックの方向、宛先 IP アドレス、およびポートによって、トラフィック傍受からの除外を設定できます。このような除外設定では Kaspersky Endpoint Security とクライアントアプリケーションの競合を解決できない場合は、特別な許可ルールチェーン kesl_bypass を使用できます。

kesl_bypass チェーンは、Kaspersky Endpoint Security がオペレーティングシステムのファイアウォールのマングルテーブル（iptables/ip6tables）に作成する特別なルールリストです。kesl_bypass チェーンのルールにより、Kaspersky Endpoint Security の傍受からトラフィックを除外できます。kesl_bypass チェーンはネットワークパケット処理プロセスの先頭に追加されるため、kesl_bypass ルールは他のすべての iptables ルールよりも先に処理されます。

本製品が eBPF テクノロジーを使用してトラフィックを傍受する場合、kesl_bypass ルールは適用されません。

Kaspersky Endpoint Security 設定で接続できる除外とは異なり、kesl_bypass チェーンでは、トラフィックの方向、宛先 IP アドレスとポートだけでなく、接続のその他のパラメータによっても除外を設定できます。

kesl_bypass 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。

たとえば、次のコマンドを実行して、kesl_bypass チェーンにルールを追加できます：`iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT`。

このルールにより、任意の IP アドレスのポート 80 での受信および送信の HTTP トラフィックを Kaspersky Endpoint Security による傍受から除外できます。これにより、信頼する Web サービスとの潜在的な競合を回避できます。

チェーン内にトラフィック除外ルールが設定されている場合、これらのルールはウェブ脅威対策、ネットワーク脅威対策、およびウェブコントロールコンポーネントに影響します。

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。

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。ネットワーク脅威対策は、接続を傍受するためにポート 9789 を使用します。

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コンポーネントは製品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、読み取られた 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。

既定では、ネットワーク脅威保護は無効になっています。

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 のトラフィック読み取りの除外リストを設定している場合、ネットワーク脅威対策に影響します。

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（**アプリケーション設定 → コミュニケーションと危険サイトブロック → ネットワーク脅威対策**）で、ネットワーク脅威対策の設定を管理できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**脅威対策 → ネットワーク脅威対策**）で、ネットワーク脅威対策の設定を管理できます。

ネットワーク脅威対策の設定

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フです。
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。 可能な値:1から32768までの整数。 既定値：60
除外リスト	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。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。

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アクティビティが検知された場合に実行される処理。 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、BlockAttackingHosts 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 から 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。

メール脅威対策

メール脅威対策保護コンポーネントは、受信メールおよび送信メールの添付ファイルをスキャンして、ウイルスやその他の脅威となるアプリケーションを検知します。この保護コンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、ヒューリスティック分析を使用してデバイスを保護します。

メール脅威対策は、受信メッセージだけでなく送信メッセージもスキャンすることができます。

本製品は、すべてのメールクライアントで POP3、SMTP、および IMAP プロトコルに対応し、MyOffice Mail および R7-Office Organizer メールクライアントでは拡張プロトコルバージョン（POP3S、SMTPS、および IMAPS）に対応しています。メール脅威対策は、他のプロトコルに対応していません。

メール脅威対策保護コンポーネントが機能するには、ネットワーク設定でネットワークポート 25、465、587、110、995、143、および 993 を監視する必要があります。これらのネットワークポートは、既定で監視対象ポートのリストに追加されます。これらのポートをリストから削除すると、コンポーネントが正しく動作しなくなる可能性があります。

既定では、メール脅威対策保護コンポーネントは有効になっています。Web コンソール、管理コンソール、およびコマンドラインを使用して、メール脅威対策を有効化、無効化、または構成できます。

Web コンソールでのメール脅威対策の設定

Web コンソールでは、ポリシープロパティ（**製品設定 → コミュニケーションと危険サイトブロック → メール脅威対策**）でメール脅威対策の設定を管理できます。

管理コンソールでのメール脅威対策の設定

管理コンソールでは、ポリシープロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）でメール脅威対策設定を管理できます（**脅威対策 → メール脅威対策**）。

メール脅威対策の設定

設定	説明
メール脅威対策	このチェックボックスでは、メール脅威対策を有効または無効にできます。 既定で、このコンポーネントは有効です。
設定 (保護の設定)	このボタンをクリックすると、**メール脅威対策の設定**ウィンドウが開き、メール脅威対策の保護範囲および複合ファイルのスキャン設定を設定できます。
設定 (添付ファイルのフィルター)	このボタンをクリックすると、**添付ファイルのフィルター**ウィンドウが開き、メールの添付ファイルのフィルター処理を設定できます。
ヒューリスティック分析を使用する **ヒューリスティック分析のレベル**	このチェックボックスでは、ヒューリスティック分析を使用するかどうかを選択できます。 悪意のあるコードがファイルに含まれているかどうかをスキャンする場合、ヒューリスティック分析は実行ファイル内の指示を実行します。ヒューリスティック分析が実行する指示の数は、指定されたヒューリスティック分析レベルによって異なります。ヒューリスティック分析レベルは、新しい脅威の検索の徹底性、オペレーティングシステムのリソースへの負荷、およびヒューリスティック分析の期間の間のバランスを設定します。 既定では、ヒューリスティック分析は有効になっており、ヒューリスティック分析レベルが中に選択されています。

設定	説明
脅威の検知時の処理	メールメッセージで脅威が検知された時にメール脅威対策が実行する処理： • **駆除する。駆除できない場合は削除する**受信メッセージで感染したオブジェクトが検知された時は、検知されたオブジェクトの駆除を試行します。その後、安全な添付ファイル付きのメッセージがユーザーに提供されます。駆除に失敗した場合、本製品は感染したオブジェクトを削除します。本製品は、実行された処理に関する情報をメッセージの件名に追加します（例：*[メッセージが処理されました]* <*メッセージの件名*>）。既定では、この処理が選択されています。 • **駆除する。駆除できない場合はブロックする**受信メッセージで感染したオブジェクトが検知された時は、検知されたオブジェクトの駆除を試行します。その後、安全な添付ファイル付きのメッセージがユーザーに提供されます。駆除に失敗した場合は、メッセージの件名に警告が追加されます。その後、元の添付ファイルのあるメッセージがユーザーに提供されます。 • **ブロック**受信メッセージで感染したオブジェクトが検出されると、本製品はメッセージの件名に警告を追加します。その後、元の添付ファイルのあるメッセージがユーザーに提供されます。

メール脅威対策の設定ウィンドウ

このウィンドウでは、メール脅威対策の保護範囲および複合ファイルスキャンの設定ができます。

メール脅威対策の設定

設定	説明
保護範囲	*保護範囲*は、コンポーネントがスキャンする必要があるオブジェクト（受信メッセージと送信メッセージ、または受信メッセージのみ）を指定します。 既定では、［**受信メッセージと送信メッセージ**］オプションが選択されています。
アーカイブの添付ファイルをスキャン	添付圧縮ファイルのスキャンを有効または無効にします。 これには、ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE およびその他の種類の圧縮ファイルのスキャンが含まれます。本製品は、拡張子だけでなく、形式によっても圧縮ファイルを識別します。圧縮ファイルをスキャンする際、本製品は再帰的な解凍を実行します。これにより、ネストされた圧縮ファイル（圧縮ファイル内の圧縮ファイル）内の脅威を検知できるようになります。 既定では、このチェックボックスはオンです。
Office アプリケーション形式の添付ファイルをスキャン	オフィス形式の添付ファイルのスキャンを有効または無効にします。本製品は、このチェックボックスが選択されているかどうかに関係なく、1MB 未満のオフィス形式の添付ファイルをスキャンします。 既定では、このチェックボックスはオンです。
次のサイズを超えるアーカイブをスキャンしない（MB）	このチェックボックスをオンにすると、メール脅威対策では、指定された制限を超える添付圧縮ファイルがスキャン対象から除外されます。このチェックボックスをオフにすると、メール脅威対策はあらゆるサイズの添付圧縮ファイルをスキャンします。 既定では、このチェックボックスはオフです。
アーカイブのスキャン時間を次の時間制限する（秒）	このチェックボックスをオンにすると、メールに添付ファイルとして送信された圧縮ファイルのスキャン期間が制限されます。 既定では、このチェックボックスはオフです。

添付ファイルフィルターウィンドウ

このウィンドウでは、メールの添付ファイルのフィルター処理を設定できます。

添付ファイルのフィルター処理設定

設定	説明
フィルターを適用しない	このオプションを選択すると、メール脅威対策はメールメッセージに添付ファイルをフィルターしません。
指定した種別の添付ファイルの名前を変更する	このオプションを選択すると、メール脅威対策は、指定されたファイルの種別（添付ファイル.doc_ など）の拡張子の最後の文字をアンダースコア文字に置き換えます。したがって、ファイルを開くには、ユーザーはファイルの名前を変更する必要があります。 既定ではオンです。

設定	説明
指定した種別の添付ファイルを削除する	このオプションを選択すると、メール脅威対策は指定された種別の添付ファイルをメールメッセージから削除します。 ファイルマスクのリストで、メールメッセージから名前を変更したり削除したりする添付ファイルの種別を指定できます。
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
添付ファイル種別のテーブル	このテーブルには、メールメッセージから名前を変更したり削除したりする添付ファイルの種別がリストされています。 対応するボタンを使用して、添付ファイルの種類を追加、編集、または削除できます。

コマンドラインでのメール脅威対策の設定

コマンドラインでは、メール脅威対策の事前定義済みタスク（*Mail_Monitoring*）を使用してメール脅威対策を管理できます。

メー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。

メー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、管理者ロール権限が必要です。

メール脅威対策の管理は、メー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。

次の表は、メール脅威対策タスクに指定できる設定の使用可能な値と既定値を示しています。

メール脅威対策タスクの設定

設定	説明	値
`CheckIncomingMessagesOnly`	*保護範囲*は、コンポーネントがスキャンする必要があるオブジェクト（受信メッセージと送信メッセージ、または受信メッセージのみ）を指定します。	`Yes` は、本製品が受信メッセージのみをスキャンすることを意味します。 `No`（既定）は、本製品が受信メッセージと送信メッセージの両方をスキャンすることを意味します。
`ScanFileArchive`	添付圧縮ファイルのスキャンを有効または無効にします。 これには、ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE およびその他の種類の圧縮ファイルのスキャンが含まれます。本製品は、拡張子だけでなく、形式によっても圧縮ファイルを識別します。圧縮ファイルをスキャンする際、本製品は再帰的な解凍を実行します。これにより、ネストされた圧縮ファイル（圧縮ファイル内の圧縮ファイル）内の脅威を検知できるようになります。	`Yes`（既定）は、本製品が添付されたアーカイブをスキャンすることを意味します。 `No` は、本製品が添付されたアーカイブをスキャンしないことを意味します。
`ScanFileOffice`	オフィス形式の添付ファイルのスキャンを有効または無効にします。	`Yes`（既定）は、本製品が添付された Office 形式のファイルをスキャンすることを意味します。 `No` は、本製品が Office 形式の添付ファイルをスキャンしないことを意味します。
`UseSizeLimit`	スキャンする圧縮ファイルのサイズを制限します。	`Yes` は、本製品が `SizeLimit` より大きい添付アーカイブをスキャン対象から除外することを意味します。 `No`（既定）は、本製品がメールメッセージに添付されたあらゆるサイズのアーカイブをスキャンすることを意味します。

設定	説明	値
SizeLimit	スキャンできる圧縮ファイルの最大サイズを設定します。	1～9999（MB）。
UseTimeLimit	添付ファイルの圧縮ファイルの最大スキャン期間を制限します。	Yes は、TimeLimit に達した後に本製品が添付されたアーカイブのスキャンを停止することを意味します。 No（既定）は、添付されたアーカイブのスキャン時間が制限されないことを意味します。
TimeLimit	添付圧縮ファイルの最大スキャンする期間を設定します。	1～9999（秒）。
ExtensionFilter	メールの添付ファイルのフィルター処理を設定します。	Disable は、本製品がメールメッセージに添付されたファイルをフィルタリングしないことを意味します。 Rename（既定）は、本製品が指定されたファイル種別の拡張子の最後の文字をアンダースコア文字に置き換えることを意味します（例：attachment.doc_）。したがって、ファイルを開くには、ユーザーはファイルの名前を変更する必要があります。 Delete は、本製品がメールメッセージから指定された種別の添付ファイルを削除することを意味します。
ExtensionMasks	メールメッセージから名前を変更したり削除したりする添付ファイルの種別の拡張子を指定します。	複数の拡張子のリストは次のように指定できます： [ExtensionMasks.item_0000] UseExtensionMask=Yes ExtensionMask=*.txt [ExtensionMasks.item_0001] UseExtensionMask=Yes ExtensionMask=*.run [ExtensionMasks.item_0002] UseExtensionMask=Yes ExtensionMask=*.exe ... 既定では、TXT、RUN、EXE、JS、JSE、MSI、SCR、VBE、VBS、SH 拡張子のファイルが処理されます。 拡張子のリストを変更するには、タスク設定を INI ファイルにエクスポートし、ファイル内のリストを編集して、INI ファイルを本製品にインポートする必要があります。
UseAnalyzer	ヒューリスティック分析を有効または無効にします。	Yes（既定）は、ヒューリスティック分析が有効であることを意味します。 No は、ヒューリスティック分析が無効であることを意味します。
AnalyzerLevel	悪意のあるコードがファイルに含まれているかどうかをスキャンする場合、ヒューリスティック分析は実行ファイル内の指示を実行します。ヒューリスティック分析が実行する指示の数は、指定されたヒューリスティック分析レベルによって異なります。ヒューリスティック分析レベルは、新しい脅威の検索の徹底性、オペレーティングシステムのリソースへの負荷、およびヒューリスティック分析の期間の間のバランスを設定します。	Light—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。 Medium（既定）– スキャンの詳細レベルが中程度で、システム負荷のバランスがとれています。 Deep—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。

設定	説明	値
`ActionOnThreat`	受信メールメッセージで脅威が検知された時にメール脅威対策が実行する処理です。 `ActionOnThreat` 設定は、送信メッセージには適用されません。送信メッセージで感染したオブジェクトが検知されると、本製品はメッセージの送信をブロックします。	`DisinfectDeleteIfNotPossible`（既定）– 駆除します。駆除に失敗した場合は削除します。受信メッセージで感染したオブジェクトが検知された時は、検知されたオブジェクトの駆除を試行します。その後、安全な添付ファイル付きのメッセージがユーザーに提供されます。駆除に失敗した場合、本製品は感染したオブジェクトを削除します。本製品は、実行された処理に関する情報をメッセージの件名に追加します（例：*[メッセージが処理されました]* <*メッセージの件名*>）。既定では、この処理が選択されています。 `DisinfectBlockIfNotPossible` – 駆除します。駆除に失敗した場合はブロックします。受信メッセージで感染したオブジェクトが検知された時は、検知されたオブジェクトの駆除を試行します。その後、安全な添付ファイル付きのメッセージがユーザーに提供されます。駆除に失敗した場合は、メッセージの件名に警告が追加されます。その後、元の添付ファイルのあるメッセージがユーザーに提供されます。 `Block` – ブロックします。受信メッセージで感染したオブジェクトが検出されると、本製品はメッセージの件名に警告を追加します。その後、元の添付ファイルのあるメッセージがユーザーに提供されます。

有害 USB 攻撃ブロック

ウイルスの中には、オペレーティングシステムで USB デバイスがキーボードとして検知されるように、USB デバイスのファームウェアを改竄するものがあります。その結果、ウイルスはユーザーアカウントでコマンドを実行し、マルウェアなどをダウンロードできるようになります。

BadUSB 攻撃ブロック保護コンポーネントを使用すると、キーボードを模倣した感染した USB デバイスがコンピューターに接続されるのを防止できます。

オペレーティングシステムによってキーボードとして識別される USB デバイスがデバイスに接続されると、本製品は、新たに接続されたキーボードから、またはオンスクリーンキーボード（使用可能な場合）を使用して、本製品によって生成された数値コードをユーザーに入力するように要求します。この手順をキーボード承認と呼びます。

コードが正しく入力されると、本製品は識別パラメータ（キーボードの VID/ PID および接続されているポート番号）を、承認済みキーボードの一覧に保存します。キーボードが再度接続されたときやオペレーティングシステムの再起動後に、認証が繰り返されることはありません。

認証済みのキーボードがデバイスの別の USB ポートに接続された時、本製品は再度承認を要求します。

数値コードが正しく入力されなかった場合、本製品は新しいコードを生成します。承認コードの入力試行回数を設定できます。数値コードが複数回間違って入力された場合、またはキーボード承認ウィンドウが閉じられた場合、本製品はこのキーボードからの入力をブロックします。USB デバイスのブロック時間の経過後もしくはオペレーティングシステムの再起動後に、キーボード認証を再度実行するようユーザーに要求します。

承認されたキーボードの使用は許可され、承認されなかったキーボードの使用はブロックされます。

既定では、BadUSB 攻撃者ブロック保護コンポーネントは無効になっています。Web コンソール、管理コンソール、およびコマンドラインを使用して、BadUSB 攻撃ブロックを有効化、無効化、または構成できます。

Web コンソールでの BadUSB 攻撃ブロックの設定

Web コンソールでは、ポリシープロパティ（**製品設定 → ホスト脅威対策 → 有害 USB 攻撃ブロック**）で有害 USB 攻撃ブロックの設定を管理できます。

管理コンソールでの BadUSB 攻撃ブロックの設定

管理コンソールでは、ポリシープロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）でウェブ脅威対策設定を管理できます（**脅威対策 → 有害 USB 攻撃ブロック**）。

有害 USB 攻撃ブロックの設定

設定	説明
BadUSB 脅威対策の有効化	このチェックボックスでは、BadUSB 脅威対策を有効または無効にするかを選択します。 コンポーネントは、既定で無効になっています。
USB デバイス承認の最大試行回数：	承認コードを指定回数間違って入力すると、USB デバイスを自動的にブロックします。有効な値は 1～10 です。たとえば、認証コードを 5 回まで許可する設定にすると、認証コードの入力を 5 回目に失敗すると本製品は USB デバイスをブロックします。Kaspersky Endpoint Security は、USB デバイスがブロックされている時間を表示します。その時間が経過すると、また認証コードを 5 回まで入力できます。 既定値：5
承認試行の最大回数に達した場合のブロック期間（分）：	認証コードの入力に指定回数失敗した後の USB デバイスのブロック期間。可能な値：1～180（分） 既定値：5
USB デバイスの承認時にオンスクリーンキーボードの使用を許可しない	このチェックボックスをオンにすると、認証コードを入力できない USB デバイスの認証時に、本製品はスクリーンキーボードの使用をブロックします。 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 BadUSB 攻撃ブロックの設定

コマンドラインでは、BadUSB 攻撃ブロックの事前定義済みタスク（*Bad_USB*）を使用してBadUSB 攻撃ブロックを管理することもできます。

既定では、BadUSB 攻撃ブロックタスクが開始されません。このタスクは、手動で開始および停止できます。

BadUSB 攻撃ブロックタスクをコマンドラインから開始または停止するには、管理者ロール権限が必要です。

BadUSB 攻撃ブロック事前定義済みタスクの設定を編集することにより、BadUSB 攻撃ブロック設定を管理できます。

次のテーブルは、有害 USB 攻撃ブロックタスクに指定できる設定の使用可能な値と既定値を示しています。

BadUSB 攻撃ブロックタスク設定

設定	説明	値
`MaxAuthAttempts`	USB デバイス承認の最大試行回数です。この回数を超えると本製品は USB デバイスをブロックし、`TimeoutAfterAttempts` パラメータで指定した期間、さらに USB デバイスの承認を試行します。	可能な値：1～10 既定値：5
`TimeoutAfterAttempts`	`MaxAuthAttempts` の回数分認証コードの入力に失敗した後の USB デバイスのブロック期間です。	可能な値：1～180（分）既定値：5 分。
`ProhibitOnScreenKeyboard`	USB デバイスの承認にオンスクリーンキーボードを使用することを禁止または許可します。	`Yes` の場合、本製品では、承認コードの入力に使用できない USB デバイスのキーボード認証にオンスクリーンキーボードを使用することは許可されません。 `No` の場合、本製品では、承認コードの入力に使用できない USB デバイスのキーボード認証にオンスクリーンキーボードを使用することは許可します。

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。

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、ポリシープロパティ（**製品設定 → ホスト脅威対策 → ふるまい分析 → アンチクリプター**）でアンチクリプター設定を管理できます。

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、ポリシープロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**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管理できます。

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。
除外リスト	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、［**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。テーブル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
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
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。

テーブル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。

指定された範囲にあるオブジェクトは、範囲のテーブル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。

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、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、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。

[保護の設定] ウィンドウ

保護設定

設定	説明
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、信頼しないホスト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。 可能な値:1 から 2147483647 までの整数。 既定値：30

[除外範囲] ウィンドウ

このウィンドウには、スキャンの除外範囲が表示されます。テーブル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。

除外範囲の設定

設定	説明
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
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。

既定では、除外範囲のテーブルは空です。テーブル内の項目は、追加、編集、削除できます。

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。

［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。

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、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。 • **All remote mounted** – 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:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` 説明： `<id>` はコンテナIDです。 `<name>` はコンテナ名です `<path to local directory>` はローカルディレクトリへのパスです。 タグの一意の組み合わせを使用することもできます：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]`、`[image-name:<name>]/path to local directory>`。 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:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` 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。

設定	説明
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。

［マスクによる除外］ウィンドウ

名前マスクによってオブジェクトのスキャン除外範囲を設定できます。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。

［**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）。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。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。

アンチクリプタータスクの設定

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を保護範囲から除外できるようにします。 この設定は、`ExcludeMasks.item_#` 設定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。

設定	説明	値
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します。	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。 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保護）
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 経由でアクセス可能なリソースを保護します。 Shared:NFS – NFS 経由でアクセス可能な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。

設定	説明	値
`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内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。

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>
```

ここで、**<アドレス>** 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。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。

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。

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。
- ルールと一致する、アプリケーションの実行試行を検知した場合に Kaspersky Endpoint Security が開始する処理を選択します。Kaspersky Endpoint Security は、*ルールを適用して*ルールで指定された処理を実行したり、*ルールをテストして*ルールに一致するアプリケーションの実行試行についてのみ通知したりできます。
- アプリケーションコントロール設定のエクスポートとインポート。

アプリケーションコントロールは、Snap、Flatpak、または AppImage の起動を制御しません。

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（ユーザーによるアプリケーションの起動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、 共通点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。

- 選択したユーザーおよびユーザーグループがアプリケーションを実行できるようにしたり、できないようにしたりします。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。

- ルールを適用する条件。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 のみ使用できます。

  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、? 文字を使用して任意の文字（/ 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適用されません。
- *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。

アプリケーションコントロールルールのテストモード

アプリケーションコントロールルールが業務に必要なアプリケーションをブロックしないように、*アプリケーションコントロールルールのテスト*を有効にすることを推奨します。このモードでは、Kaspersky Endpoint Securityはサードパーティ製アプリケーションの実行をブロックせず、それらの起動に関する通知を管理サーバーに送信します。

既定では、アプリケーションコントロールは、ルールで禁止されているものを除き、すべてのサードパーティ製アプリケーションの実行を許可します。

アプリケーションコントロールルールのテスト

1. **アプリケーションコントロールルールの作成**

   テストするアプリケーションコントロールルールを設定して有効にします。たとえば、「ゴールデンイメージ」カテゴリおよび「業務アプリケーション」カテゴリのアプリケーションを除き、すべてのサードパーティ製アプリケーションの実行を防止するルールを作成できます。

2. **テストモードでアプリケーションコントロールを有効にする**

   Web コンソールでアプリケーションコントロールのテストモードを有効にする方法

   1. Web コンソールのメインウィンドウで、［**資産管理**］→［**ポリシー**］の順に選択します。
   2. Kaspersky Endpoint Security の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。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**アプリ管理**］に移動します。

5. コンポーネントのトグルスイッチが **アプリ管理は有効です** の位置にあることを確認します。

6. **アプリケーションの開始時の処理** で、アプリケーションコントロールに対して **通知する** 処理を選択します。

7. ポリシーをコンピューターに適用するには、南京錠のアイコンを閉じて変更を保存します。

コマンドラインでアプリケーションコントロールのテストモードを有効にする方法

アプリケーションコントロールのテストモードを選択するには、次のコマンドを実行します：

```
kesl-control --set-settings 21 AppControlRulesAction=TestRules
```

3 テスト結果の確認

アプリケーションコントロールレポートと、Kaspersky Security Centerに送信されるコンポーネントのイベントを確認します。

Web コンソールでアプリケーションコントロールレポートを表示する方法

1. Web コンソールのメインウィンドウで、［**資産管理**］→［**ポリシー**］の順に選択します。

2. Kaspersky Endpoint Security の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。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**セキュリティコントロール**］→［**アプリ管理**］に移動します。

5. コンポーネントのトグルスイッチが **アプリ管理は有効です** の位置にあることを確認します。

6. アプリケーションコントロールルールのテーブルで、［**レポートの表示**］をクリックします。

7. ［**テストモードでのブロック対象アプリケーションのレポート**］ウィンドウが表示されます。

8. テストモードで起動した禁止対象アプリケーションに関する情報を確認します。

アプリケーションコントロールのテスト実行で発生したイベントを表示する方法

1. Web コンソールのメインウィンドウで、［**監視**］→［**イベントの抽出**］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**新規のイベントの抽出**ウィンドウで、イベント抽出の名前を指定します。たとえば、「アプリケーションコントロールルールのテスト」です。

4. **イベント**セクションに移動して、次の設定を管理します：

   - **アプリケーション名** – Kaspersky Endpoint Security for Linux。
   - **深刻度** – **情報**。

- ［**選択した一般イベントを含める**］を選択します。
- **アプリケーションの起動がテストモードでブロックされています**イベントおよび**アプリケーションの起動がテストモードで許可されています**イベントの横にあるチェックボックスをオンにします。

5. 必要に応じて、残りの設定を構成します。
6. 変更内容を保存します。
7. イベント抽出の結果を表示するには、イベント抽出の名前をクリックします。

4 **ルールを調整する**

テストモードの結果、コンピューターのユーザーの業務に必要なすべてのアプリケーションについて起動ブロックイベントがなければ、適切なルールが作成されています。

そうでない場合は、作成したルールの設定を編集するか、追加のルールを作成するか、既存のルールを削除してください。

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、ポリシープロパティ（**製品設定 → セキュリティコントロール → アプリ管理**）でアプリケーションコントロール設定を管理できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**セキュリティコントロール → アプリケーションコントロール**）で、デバイスコントロールの設定を管理できます。

アプリケーションコントロールの設定

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。

設定	説明
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）。このオプションを選択した場合、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、ポリシーで設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、［**新規ルールを追加**］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、変更、または削除できます。

［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。
Category	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、または削除できます。

［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。 カテゴリの作成についての詳細は、Kaspersky Security Center のヘルプを参照してください。
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。［**ゴールデンイメージ（ローカル）**］カテゴリは編集できません。

［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。
Access	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ケーションコントロールの設定

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。

許可するアプリケーションのリストを変更する場合、またはすべてのアプリケーションや Kaspersky Endpoint Security の動作に影響するアプリケーションの起動を禁止する場合、設定情報ファイルを使用してタスクの設定を変更する場合、またはコマンドラインオプションを使用する場合は、`--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について、指定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、? 文字を使用して任意の文字（/ を含む）を表示できます。

設定	説明	値
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、? 文字を使用して任意の文字（/ 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 のみ使用できます。
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、? 文字を使用して任意の文字（/ 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、? 文字を使用して任意の文字（/ 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 のみ使用できます。
[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：		
Description	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。

設定	説明	値
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。 **< ユーザー名 >** は、ルールを適用するユーザーの名前です。 **@< グループ名 >** は、ルールを適用するユーザーグループの名前です。
[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：		
Description	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。 **< ユーザー名 >** は、ルールを適用するユーザーの名前です。 **@< グループ名 >** は、ルールを適用するユーザーグループの名前です。

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 > は、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 < アプリケーションの実行ファイルへの完全パス >)", "
(FileHash == < 実行ファイルのハッシュ >)" ],
```

```
        "GUID" : "<一意のカテゴリ ID>",
        "Include" : [ "(FilePath like <アプリケーションの実行ファイルへの完全パス>)", "
   (FileHash == <実行ファイルのハッシュ>)" ],
        "Name" : "<カテゴリ 1 の名前>"
     },
   {
        "Exclude" : [ "(FilePath like <アプリケーションの実行ファイルへの完全パス>)", "
   (FileHash == <実行ファイルのハッシュ>)" ],
        "GUID" : "<一意のカテゴリ ID>",
        "Include" : [ "(FilePath like <アプリケーションの実行ファイルへの完全パス>)", "
   (FileHash == <実行ファイルのハッシュ>)" ],
        "Name" : "<カテゴリ 2 の名前>"
     }
]
```

［Exclude］フィールドと［Include］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、? 文字を使用して任意の文字（/ を含む）を表示できます。

> Name 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>**は、情報を変更するカテゴリの名前です。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>**は、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コマンド、kesl-control --get-categories 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 <設定情報ファイルへのパス>] [--json]
```

説明：

- **--file <設定情報ファイルへのパス>** は、設定の書き込み先となる JSON 設定情報ファイルへの完全パスです。
- **--json** を指定すると、設定は JSON 形式で出力されます。--json オプションを省略すると、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

別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 [--names <カテゴリ名 1> <カテゴリ名 2> ... <カテゴリ名 N>] [--file <設定情報ファイルへのパス>] [--json]
```

説明：

- **<カテゴリ名 1> <カテゴリ名 2> ... <カテゴリ名 N>** は、情報を表示するカテゴリの名前です。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 <設定情報ファイルへのパス>** – 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完全パス。
- **--json** を指定すると、設定は JSON 形式で出力されます。--json オプションを省略すると、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 <path to configuration file>] [--json]
```

説明：

- `--file <path to configuration file>` は、設定の出力先となる設定情報ファイルの完全パスです。
- `--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。
- 設定済みルールに一致するアプリケーションの起動の試行を検知したとき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）。
- アプリケーションコントロールルールの動作ステータス。
- 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 <path to configuration file>] [--json]
```

説明：

- `--file <path to configuration file>` は、設定のインポート元となる設定情報ファイルの完全パスです。
- `--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
```

アプリケーションコントロール設定のエクスポートとインポート

ユーザーデバイス上の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簡素化するために、アプリケーションコントロール設定およびアプリケーションカテゴリのリストをエクスポートおよびインポートできます。

Web コンソールでのアプリケーションコントロール設定のエクスポートとインポート

Web コンソールでは、管理対象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→［**アプリケーション**］タブ→<Kaspersky Endpoint Security アプリケーション名>リンク→［**製品設定**］タブ→［**アプリケーションコントロール**］セクション））で、アプリケーションコントロール設定とアプリケーションカテゴリのタブをエクスポートまたはインポートできます。

アプリケーションコントロール設定の［**エクスポート**］をクリックすると、設定を保存するファイルを指定できるウィンドウが開きます。**アプリケーションコントロール設定**の［**インポート**］をクリックすると、設定のインポート元ファイルを指定できるウィンドウが開きます。

アプリケーションカテゴリの［**エクスポート**］をクリックすると、追加したアプリケーションカテゴリを保存するファイルを指定できるウィンドウが開きます。**アプリケーションカテゴリ**の［**インポート**］をクリックすると、アプリケーションカテゴリのインポート元ファイルを指定できるウィンドウが開きます。

管理コンソールでのアプリケーションコントロール設定のエクスポートとインポート

管理コンソールでは、管理対象デバイスのプロパティで、アプリケーションコントロール設定とアプリケーションカテゴリのリストをエクスポートおよびインポートできます（［**管理対象デバイス**］→［**デバイス**］タブ→デバイスのプロパティウィンドウ→［**アプリケーション**］セクション→<アプリケーション名>→［**プロパティ**］ボタン→［**<アプリケーション名> 設定**］ウィンドウ→［**アプリケーションコントロール**］セクション）。

アプリケーションコントロール設定の［**エクスポート**］をクリックすると、設定を保存するファイルを指定できるウィンドウが開きます。**アプリケーションコントロール設定**の［**インポート**］をクリックすると、設定のインポート元ファイルを指定できるウィンドウが開きます。

アプリケーションカテゴリの［**エクスポート**］をクリックすると、追加したアプリケーションカテゴリを保存するファイルを指定できるウィンドウが開きます。**アプリケーションカテゴリ**の［**インポート**］をクリックすると、アプリケーションカテゴリのインポート元ファイルを指定できるウィンドウが開きます。

コマンドラインでのアプリケーションコントロール設定のエクスポートとインポート

コマンドラインでは、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、アプリケーションコントロールおよびアプリケーションカテゴリのリストをエクスポートまたはインポートできます。

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。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。

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。
- インベントリの範囲（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。
- インベントリタスクの完了時に Kaspersky Endpoint Security が「ゴールデンイメージ」アプリケーションカテゴリで実行する必要がある処理を選択します。タスクがデバイス上で検出したアプリケーションをカテゴリに追加したり、カテゴリを変更せずにそのままにしたり、削除したりすることができます。
- インベントリタスクがデバイス上で検出したアプリケーションに関する情報を Kaspersky Security Center 管理サーバーに送信するかどうかを有効または無効にします。デバイス上のアプリケーションに関する情報が管理サーバーに送信された場合、その情報を使用して、Kaspersky Security Center を使用してアプリケーションコントロールルールのアプリケーションカテゴリを設定できます。

Web コンソールでのインベントリの設定

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
タスク完了後に「ゴールデンイメージ」カテゴリに実行する処理	ドロップダウンリストで、インベントリタスクの完了時に Kaspersky Endpoint Security が「ゴールデンイメージ」アプリケーションカテゴリで実行する必要がある処理を選択できます。 • **変更なし** - インベントリの完了後に「ゴールデンイメージ」アプリケーションカテゴリを変更しません。これが既定です。 • **アップデートまたは作成（存在しない場合）** - インベントリタスクがデバイス上で検出し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。カテゴリが存在しない場合は作成されます。カテゴリが存在する場合、カテゴリ内のアプリケーションのリストが更新されます。 • **Remove** – インベントリを完了した後、「ゴールデンイメージ」カテゴリを削除します。 アプリケーションコントロールルールで「ゴールデンイメージ」カテゴリを使用できます。
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。
インベントリの範囲	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の範囲を示す表。テーブル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つのインベントリの範囲（/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、編集、削除、上に移動、下に移動。 また、［**インポート**］をクリックしてファイルからインベントリの範囲のリストをインポートすることも、［**エクスポート**］をクリックしてインベントリの範囲のリストを JSON 形式 で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、インベントリの範囲のリストを置き換えるか、既存のリストにインベントリの範囲を追加するように求められます。

［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の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の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。「**/**」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。

[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

このウィンドウには、スキャンの除外範囲が表示されます。テーブル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。

除外範囲の設定

設定	説明
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
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。

既定では、除外範囲のテーブルは空です。テーブル内の項目は、追加、編集、削除できます。

インポートボタンを使用してファイルから除外リストをインポートしたり、**エクスポート**ボタンを使用して除外リストをJSONファイルにエクスポートしたり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。

[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。

設定	説明
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。

管理コンソールでのインベントリの設定

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
タスク完了後に「ゴールデンイメージ」カテゴリに実行する処理	ドロップダウンリストで、インベントリタスクの完了時に Kaspersky Endpoint Security が「ゴールデンイメージ」アプリケーションカテゴリで実行する必要がある処理を選択できます。 • **変更なし** - インベントリの完了後に「ゴールデンイメージ」アプリケーションカテゴリを変更しません。これが既定です。 • **アップデートまたは作成（存在しない場合）** - インベントリタスクがデバイス上で検出し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。カテゴリが存在しない場合は作成されます。カテゴリが存在する場合、カテゴリ内のアプリケーションのリストが更新されます。 • **Remove** – インベントリを完了した後、「ゴールデンイメージ」カテゴリを削除します。 アプリケーションコントロールルールで「ゴールデンイメージ」カテゴリを使用できます。
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。
インベントリの範囲	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**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。テーブル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。

テーブル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。

指定された範囲にあるオブジェクトは、範囲のテーブル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。

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

このウィンドウには、スキャンの除外範囲が表示されます。テーブル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。

除外範囲の設定

設定	説明
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
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。

既定では、除外範囲のテーブルは空です。テーブル内の項目は、追加、編集、削除できます。

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。

［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。

設定	説明
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。

コマンドラインでのインベントリの設定

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。

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に指定できるすべての設定について、指定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。

設定	説明	値
GoldenImageAction	インベントリタスクの完了時に Kaspersky Endpoint Security が「ゴールデンイメージ」アプリケーションカテゴリで実行する必要がある処理： アプリケーションコントロールルールで「ゴールデンイメージ」カテゴリを使用できます。	DoNothing（既定）- インベントリの完了後に「ゴールデンイメージ」アプリケーションカテゴリを変更しません。 Create – 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。カテゴリが存在しない場合は作成されます。カテゴリが存在する場合、カテゴリ内のアプリケーションのリストが更新されます。 Remove – インベントリを完了した後、「ゴールデンイメージ」カテゴリを削除します。
[ScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	インベントリの範囲の説明。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の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 つのインベントリの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の範囲をスキャンします。 No – 指定されたインベントリの範囲をスキャンしません。
AreaMask.item_#	インベントリスキャン範囲の制限。インベントリスキャン範囲で、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。 この設定が指定されていない場合、インベントリの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：*（すべてのオブジェクトをスキャン）
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へのパス >** – 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。	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、インベントリの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へのパス >** は、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。
  - **Type**。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。

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への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。このアクセスモードは、ストレージデバイス（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ドライブ、CD/DVD ドライブ）に対してのみ指定できます。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。
  - *読み取り専用*：選択した種別のデバイスへの読み取り専用アクセスを許可し、書き込みアクセスをブロックします。このアクセスモードは、ストレージデバイス（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ドライブ、CD/DVD ドライブ）に対してのみ指定できます。デバイスのアクセスタイプが「読み取り専用」の場合、信頼するデバイスが特定のユーザーに割り当てられると、割り当てられたユーザーは無視され、デバイスはすべてのユーザーが書き込み可能になります。
- **接続バス**。*接続バス*は、USB や FireWire など、デバイスが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。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。

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はシステムドライブをブロックしません。アプリケーションがシステムドライブを自動的に検出できない場合、デバイスコントロールコンポーネントはエラーで終了します。

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、6.8 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。

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。
- デバイスが接続されているバスに応じて、デバイス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。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。さらに、どのデバイスを信頼するユーザーまたはグループを指定することもできます。

  信頼するデバイスのリストは、コマンドラインまたは Kaspersky Security Center を使用して管理できます。

  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。クライアントデバイス上のコマンドラインまたは Kaspersky Security Center を使用して、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や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を取得できます。Kaspersky Security Center 管理サーバーとの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）。

  Kaspersky Security Center を使用してアプリケーションを管理している場合は、以下の方法でデバイスを信頼済みリストに追加することもできます。

  - 管理対象クライアントデバイスで検出されたデバイスのリスト。リストは、Web コンソールまたは管理コンソールのポリシープロパティに表示されます。
  - Kaspersky Security Center のデバイスコントロールイベントに基づいて生成されたデバイスのリスト。このリストは、Web コンソールまたは管理コンソールのポリシーのプロパティで作成できます。

  管理コンソールでは、設定済みの信頼するデバイスのリストをファイルにエクスポートしたり、ファイルから信頼するデバイスのリストをインポートしたりすることもできます。

- ストレージデバイス（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ドライブ、および CD/DVD ドライブ）のアクセススケジュールを設定します。

  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。

- ブロックされたデバイスへの一時アクセスをユーザーが要求し、デバイスへのアクセス権の付与を許可します。

  ブロックされたデバイスへのアクセスを許可できるのは、組織内に Kaspersky Security Center 16.2 が導入されており、クライアントデバイスが管理サーバーとの接続を確立できる場合のみです。

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管理できます（**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**）。

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、ポリシープロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**セキュリティコントロール → デバイスコントロール**）で、デバイスコントロール設定を管理できます。

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効にする	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。
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できます。
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が検知されるとイベントを生成します。 • **ブロック**（既定値）：このオプションをオンにすると、Kaspersky Endpoint Security はデバイスまたはバスに設定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。
一時的なアクセス要求の許可	このチェックボックスをオンにすると、ユーザーはアプリケーションのグラフィカルインターフェイスまたはコマンドラインで、ブロックされたデバイスへの一時アクセスを要求できます。
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。

［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	信頼するデバイスが接続されているクライアントデバイスの名前。
ユーザーまたはグループ名	デバイスが信頼されるユーザーまたはグループの名前。
コメント	信頼するデバイスに関するコメント。

次のように、［**追加**］をクリックして、信頼するデバイスリストにデバイスを追加できます。

- デバイス ID または デバイス ID マスクを指定します（［**追加**］→［**ID またはマスクでデバイスを追加**］）。
- 管理対象デバイスで検出されたデバイスのリストから目的のデバイスを選択します（［**追加**］→ **コンピューターで検知されたデバイスのリストからデバイスを選択**）。
- Kaspersky Security Center のデバイスコントロールイベントで検出されたデバイスのリストから目的のデバイスを選択します（［**追加**］→**イベントに基づいてデバイスを追加**）。

表内の信頼するデバイスを編集および削除できます。

また、［**詳細**］→［**選択した項目をエクスポート**］または［**詳細**］→［**すべてエクスポート**］の順にクリックして、追加されたデバイスのリストをファイルにエクスポートしたり、［**詳細**］→［**インポート**］の順にクリックして JSON ファイルからデバイスのリストをインポートしたりすることもできます。

3 つのインポートモードを利用できます：

- **既存のものと組み合わせて**、インポート時に信頼するデバイスのリストをマージします。ファイルにこのデバイス ID のエントリが既に存在する場合は、既存のエントリの設定がアップデートされます。以前リストになかったデバイスについては、エントリが追加されます。
- インポート時に信頼するデバイスをリストに追加するには、 ［**既存に追加**］をクリックします。以前にデバイスリストになかったデバイスのエントリのみがリストに追加されます。
- 信頼するデバイスのリストを置き換えるには、**既存のものを置き換えます**。信頼するデバイスの既存のリストは、ファイルからのリストに置き換えられます。

［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	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）。
ユーザーまたはユーザーグループのアクセスを許可する	このフィールドには、信頼するデバイスが信頼されているユーザーおよび/またはグループの名前が表示されます。既定値：**/Everyone**（全ユーザー）
設定	ボタンをクリックすると、［**信頼するデバイスへのアクセス**］ウィンドウが表示されます。

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、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、現在のポリシーが作成され、ネットワークエージェントとの同期が実行されている場合にのみ利用できます（同期間隔はネットワークエージェントポリシーで指定されており、既定は 15 分です）。

新しく非アクティブポリシーを作成すると、リストは空になります。

管理対象デバイスで検出されたデバイスのリストからのデバイスの追加

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、指定したパラメータのデバイスを検索します。検索結果を下のテーブルに示します。
検出されたデバイスのリスト	表には次の列があります： • **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。 • **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。 • **デバイス名** – 検出されたデバイスの名前。 • **デバイス ID** – 検出されたデバイスの ID。

デバイスコントロールイベントウィンドウに基づくデバイスのリスト

このウインドウでは、Kaspersky Security Center のデバイスコントロールイベントで検出されたデバイスのリストを作成できます。このリストからデバイスを信頼するデバイスのリストに追加できます。

信頼するデバイスのリストに追加するデバイスを1つ以上選択できます。

デバイスコントロールが有効になっていて、アクティブなポリシーがあり、ネットワークエージェントとの同期が実行されている場合は、デバイスに関する情報を利用できます（同期はネットワークエージェントポリシーで指定された頻度で実行されます。既定では 15 分ごと）。

新しく非アクティブポリシーを作成すると、リストは空になります。

Kaspersky Security Center のイベントで検出されたデバイスのリストからデバイスを追加する

設定	説明
イベント種別	チェックボックスを使用して、Kaspersky Security Center に送信されるデバイスコントロールイベントの種別を選択できます。リストには、指定された種別のイベントで検出されたデバイスが含まれます。 既定では、すべてのチェックボックスがオンになっています。
管理グループ	検出されたデバイスが接続済みのクライアントデバイスを含む管理グループの名前を入力するフィールドです。指定された管理グループのクライアントデバイスに接続済みのデバイスのみがリストに含まれます。 グループ名の一部を指定できます。 既定では、リストには任意の管理グループ内のクライアントデバイスに接続済みのデバイスが含まれます。
期間のイベント	ドロップダウンリストでは、イベントが発生した期間を選択できます。リストには、指定された期間中に Kaspersky Security Center に送信されたイベントで検出されたデバイスが含まれます。 既定では、リストには過去1か月間のイベントで検出されたデバイスが含まれます。
デバイスを検索	このボタンをクリックすると、指定したパラメータのデバイスを検索します。検索結果を下のテーブルに示します。
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。 • **接続日**は、見つかったデバイスが接続済みになった日付です。 • **管理グループ**は、検出されたデバイスが接続済みのクライアントデバイスを含む管理グループの名前です。
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）。
ユーザーまたはユーザーグループのアクセスを許可する	このフィールドには、信頼するデバイスが信頼されているユーザーおよび/またはグループの名前が表示されます。既定値：**/Everyone**（全ユーザー）
設定	ボタンをクリックすると、［**信頼するデバイスへのアクセス**］ウィンドウが表示されます。

［信頼するデバイスへのアクセス］ウィンドウ

このウィンドウでは、選択した信頼するデバイスへのユーザーまたはユーザー グループのアクセスを設定できます。

信頼するデバイスへのアクセス

設定	説明
ユーザーまたはユーザーグループのいずれかまたは両方	追加したデバイスを信頼させたいユーザーとグループのリスト。 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、または削除できます。

［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、デバイスを信頼させたいユーザーまたはユーザーグループを指定できます。

信頼するデバイスの設定

設定	説明
種別	デバイスを信頼させたい**ユーザー**または**グループ**。
ユーザーまたはグループ名	ローカルユーザーまたはドメインユーザーの名前（システム上でこの形式でのユーザー名の入力が許可されている場合はドメインを含むフルネームを指定しないか、**<ドメイン名>\<ユーザー名>**または**<ユーザー名>@<ドメイン名>**の形式で）、またはデバイスを信頼させたいユーザーグループの名前。

［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、次のいずれかの項目を選択します： • **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。 • **パスに依存**（既定値）– 接続パ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。このメニューコマンドは、ストレージデバイス（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ドライブ、CD/DVD ドライブ）でのみ使用できます。 • **読み取り専用**– 選択した種別のデバイスへの読み取り専用アクセスを許可します。このメニューコマンドは、ストレージデバイス（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ドライブ、CD/DVD ドライブ）でのみ使用できます。

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
ユーザーまたはユーザーグループのいずれかまたは両方	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、または削除できます。
デバイスアクセスルール	この表には、ユーザーまたはユーザーグループのいずれかまたは両方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）。 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。**接続パス**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、または削除できます。**既定の**スケジュールは、編集や削除はできません。

［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	ローカルユーザーまたはドメインユーザーの名前（システム上でこの形式でのユーザー名の入力が許可されている場合はドメインを含むフルネームを指定しないか、**<ドメイン名>\<ユーザー名>** または **<ユーザー名>@<ドメイン名>** の形式で）、またはルールが適用される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	このテーブルでは、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、次のいずれかの項目を選択します： • **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。

デバイスコントロールメッセージテンプレートの設定

ユーザーがブロックされたデバイスにアクセスしようとすると、本製品はアクセス拒否またはデバイスでの操作のブロックに関するメッセージを表示します。

アクセス拒否メッセージは、ブロックの理由を説明するテンプレートに基づいています。メッセージテンプレートでは、特殊変数（%USER_NAME% など）を使用できます。このような変数を使用すると、異なるデバイスで同じメッセージテンプレートを使用できます。メッセージを生成するときに、本製品は特定のデバイス、ユーザー、およびイベントに対応する値変数をメッセージに挿入します。

メッセージテンプレートは編集できます。

Web コンソールでメッセージテンプレートを変更する方法：

1. 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**］→［**デバイスコントロール**］の順に選択します。

2. ［**メッセージテンプレート**］セクションで、［**メッセージのブロック**］をクリックします。

3. 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［**ユーザーへのメッセージ**］タブでデバイスコントロールのメッセージテンプレートを設定します：

   ［**変数の追加**］および［**リンクの追加**］をクリックすると、ユーザーへのメッセージの本文に変数とリンクを追加できます。テンプレートに変数を追加するには、テキスト内の必要な場所にカーソルを置き、［**変数の追加**］をクリック、ドロップダウンリストから変数を選択します。テンプレートにリンクを追加するには、テキスト内の必要な場所にカーソルを置き、［**リンクの追加**］をクリックします。

   ［**既定にリセット**］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することもできます。

4. ［OK］をクリックします。

5. ［**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**］→［**デバイスコントロール**］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**］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［**ブロックメッセージ**］タブでデバイスコントロールのメッセージテンプレートを設定します：

   ［**変数**］および［**リンク**］をクリックすると、ユーザーへのメッセージの本文に変数とリンクを追加できます。テンプレートに変数を追加するには、テキスト内の必要な場所にカーソルを置き、［**変数**］をクリック、ドロップダウンリストから変数を選択します。テンプレートにリンクを追加するには、テキスト内の必要な場所にカーソルを置き、［**リンク**］をクリックします。

   ［**既定**］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することもできます。

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

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タスクは既定では開始されません。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。

次のようにデバイスコントロール管理コマンドも使用できます：

- 接続済みのデバイスリストを表示し、ファイルにエクスポートする
- 信頼するデバイスのリストを表示および変更する

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について、設定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）– アプリケーション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。 `Notify` – 選択されたアクセスモードがテストされ、デバイスへのアクセスの試みの検知に関するイベントを生成します。
`AllowToRequestTemporaryAccess`	ブロックされたデバイスへの一時アクセス要求の許可。 ブロックされたデバイスへのアクセスを許可できるのは、組織内に Kaspersky Security Center 16.1 が導入されており、クライアントデバイスが管理サーバーとの接続を確立できる場合のみです。	`Yes` - ユーザーがアプリケーションのグラフィカルインターフェイスまたはコマンドラインで、ブロックされたデバイスへの一時アクセスを要求することを許可します。 `No`（既定）- ブロックされたデバイスへの一時アクセスをユーザーが要求することを許可しません。
［**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` – ハードディスクへのアクセスをユーザーに許可します。 `DependsOnBus`（既定）：ハードドライブへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 `Block` – すべてのハードディスクへのアクセスをユーザーに対してブロックします。ただし、システムハードディスクは、デバイスコントロールでブロックされないので含まれません。 `ByRule` – ハードディスクへのアクセス可否は、アクセスルールに応じて決まります。 `ReadOnly` - ユーザーはハードドライブの読み取りのみが可能で、書き込みはできません。

設定	説明	値
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 – リムーバブルドライブへのアクセスをユーザーに対して許可します。 DependsOnBus（既定）：リムーバブルドライブへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 Block – リムーバブルドライブへのアクセスをユーザーに対してブロックします。 ByRule – リムーバブルドライブへのアクセス可否は、アクセスルールに応じて決まります。 ReadOnly - ユーザーはリムーバブルドライブの読み取りのみが可能で、書き込みはできません。
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ドライブ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ドライブをブロックしません。	Allow — フロッピーディスクドライブへのアクセスをユーザーに許可します。 DependsOnBus（既定）：フロッピーディスクドライブへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 Block — フロッピーディスクドライブへのアクセスをユーザーに対してブロックします。 ByRule — フロッピーディスクドライブへのアクセス可否は、アクセスルールに応じて決まります。 ReadOnly — ユーザーはフロッピーディスクドライブの読み取りのみが可能で、書き込みはできません。
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 ドライブへのアクセスをユーザーに許可します。 DependsOnBus（既定）：CD / DVD へのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 Block – CD/DVD ドライブへのアクセスをユーザーに対してブロックします。 ByRule – CD/DVD ドライブへのアクセス可否は、アクセスルールに応じて決まります。 ReadOnly - ユーザーは CD/DVD ドライブの読み取りのみが可能で、書き込みはできません。
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 – シリアルポートで接続されたデバイスへのアクセスをユーザーに許可します。 DependsOnBus（既定）：シリアルポート経由で接続されたデバイスへのアクセスは、バスアクセスモードに依存します。 Block – シリアルポートで接続されたデバイスへのアクセスをユーザーに対してブロックします。
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 – パラレルポートで接続されたデバイスへのアクセスをユーザーに許可します。 DependsOnBus（既定）：パラレルポート経由で接続されたデバイスへのアクセスは、バスアクセスモードに依存します。 Block – パラレルポートで接続されたデバイスへのアクセスをユーザーに対してブロックします。
Printer	クライアントデバイスに接続されたプリンターに対するアクセスモード。	Allow – プリンターへのアクセスをユーザーに許可します。 DependsOnBus（既定）：プリンターへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 Block – プリンターへのアクセスをユーザーに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 – モデムへのアクセスをユーザーに許可します。 DependsOnBus（既定）：モデムへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 Block – モデムへのアクセスをユーザーに対してブロックします。

設定	説明	値
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 – テープデバイスへのアクセスをユーザーに許可します。 DependsOnBus（既定）：テープデバイスへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 Block – テープデバイスへのアクセスをユーザ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 – 多機能デバイスへのアクセスをユーザーに許可します。 DependsOnBus（既定）：多機能デバイスへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 Block – 多機能デバイスへのアクセスをユーザ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 – スマートカードリーダーへのアクセスをユーザーに対して許可します。 DependsOnBus（既定）：スマートカードリーダーへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 Block – スマートカードリーダーへのアクセスをユーザーに対してブロックします。
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 アダプターへのアクセスをユーザーに許可します。 DependsOnBus（既定）：Wi-Fiアダプターへのアクセスは、接続バスのアクセスモードに依存します。 Block – Wi-Fi アダプターへのアクセスをユーザーに対してブロックします。
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 – 外部ネットワークアダプターへのアクセスをユーザーに許可します。 DependsOnBus（既定）：外部ネットワークアダプターへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 デバイスコントロールでは、クライアントデバイスをネットワークから切り離すことを避けるため、外部ネットワークアダプターへのアクセスを拒否することはできません。
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 – ポータブルデバイスへのアクセスをユーザーに許可します。 DependsOnBus（既定）：ポータブルデバイスへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 Block – ポータブルデバイスへのアクセスをユーザーに対してブロックします。
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 デバイスへのアクセスをユーザーに許可します。 DependsOnBus（既定）：Bluetooth デバイスへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 Block – Bluetooth デバイスへのアクセスをユーザーに対してブロックします。
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 – すべてのイメージングデバイスへのアクセスをユーザーに対して許可します。 DependsOnBus（既定）：イメージングデバイスへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 Block – すべてのイメージングデバイスへのアクセスをユーザーに対してブロックします。

設定	説明	値
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 – すべてのサウンドアダプターへのアクセスをユーザーに対して許可します。 DependsOnBus（既定）：サウンドアダプターへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 Block – すべてのサウンドアダプターへのアクセスをユーザーに対してブロックします。
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 – 入力デバイスへのアクセスをユーザーに許可します。 DependsOnBus（既定）：入力デバイスへのアクセスは、接続されているバスに定義されているアクセスモードに依存します。 Block – 入力デバイスへのアクセスをユーザー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 デバイスへのアクセスをユーザーに許可します。 Block – USB デバイスへのアクセスをユーザー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続されたデバイスのアクセスモード。	Allow（既定値）– FireWire インターフェイスで接続されたデバイスへのアクセスをユーザーに許可します。 Block – FireWire インターフェイスで接続されたデバイスへのアクセスをユーザーに対してブロックします。
[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）または「?」（任意の 1 文字）のマスクを、デバイス ID を示すマスクとして使用できます。 例： *指定した USB デバイス以外のすべての USB デバイスへのアクセスを拒否するには、次の設定を指定します：* [DeviceBus] セクションで、USB=Block を指定します [TrustedDevices.item_#] セクションで、DeviceId=< **デバイス ID** > を指定します *すべての USB デバイスへのアクセスを拒否し、すべての USB ドライブへのアクセスを許可するには、次の設定を指定します：* [DeviceBus] セクションで、USB=Block を指定します [TrustedDevices.item_#] セクションで、DeviceId=USBSTOR* を指定します
Comment	指定された信頼するデバイスへコメントします。	–
[TrustedDevices.item_#.Principals.item_#] セクションには、信頼するデバイスにアクセスするためのルールが含まれています。		
Principal	デバイスが信頼されるユーザーまたはグループ。 デバイスのアクセスタイプが「読み取り専用」の場合、信頼するデバイスが特定のユーザーに割り当てられると、割り当てられたユーザーは無視され、デバイスはすべてのユーザーが書き込み可能になります。	\Everyone（既定）：デバイスはすべてのユーザーに対して信頼されます。 < **ユーザー名** > は、デバイスが信頼されるローカルユーザーまたはドメインユーザーの名前です（システム上でこの形式でのユーザー名の入力が許可されている場合はドメインを含むフルネームを指定しないか、< **ドメイン名** >\< **ユーザー名** > または < **ユーザー名** >@< **ドメイン名** > の形式で指定します）。 @< **グループ名** > は、デバイスが信頼される（ローカルまたはドメイン）ユーザーグループの名前です。
[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、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ドライブ、および CD/DVD ドライブに対してのみ設定できます。		

設定	説明	値
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 のスケジュールでは、対応するデバイス種別へのアクセスが接続バスに許可されている場合、ユーザーはいつでもデバイスにフルアクセスできます。 Default のスケジュールを削除することはできません。
DaysHours	スケジュールの時間を指定します。	All（既定値）– 24 時間 365 日有効なスケジュールです（時間制限なし）。 **< 曜日 >** は曜日です。完全な曜日名または省略形のいずれかを使用できます（たとえば、月曜日の場合は、Mo、Mon、Monday で指定できます）。平日には、間隔または特定の日を指定できます。週は日曜日から始まります。 **< 時 >** は時間 [0:24] です。時間の場合は、間隔による指定のみ可能です。 例： *Schedule_1 は、日曜日から土曜日の午前 0 時から午前 11 時、午後 12 時から午後 3 時、および午後 4 時から午前 12 時まで有効です：* [Schedules.item_0001] ScheduleName=schedule_1 DaysHours=Su-Sa:0..11,12..15,16..24 *Schedule_2 は、木曜日の午後 12 時から午後 2 時、金曜日の午前 2 時から午後 3 時、および午後 4 時から午前 12 時まで有効です：* [Schedules.item_0002] ScheduleName=schedule_2 DaysHours=Th:12..14;Fr:2..15,16..24 *Schedule_3 は 週 7 日 24 時間有効です：* [Schedules.item_0003] ScheduleName=schedule_3 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。複数のアクセスルールをハード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を指定できます。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）では、アクセスルールがすべてのユーザーに適用されます。 **< ユーザー名 >** は、アクセスルールが適用されるローカルユーザーまたはドメインユーザーの名前です（システム上でこの形式でのユーザー名の入力が許可されている場合はドメインを含むフルネームを指定しないか、**< ドメイン名 >\< ユーザー名 >** または **< ユーザー名 >@< ドメイン名 >** の形式で指定します）。 **@< グループ名 >** は、アクセスルールが適用される（ローカルまたはドメイン）ユーザーグループの名前です。
[HardDrivePrincipals.item_#.AccessRules.item_#] には、アクセスルールの設定が含まれています。		
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）– アクセスルールは有効です。 No – アクセスルールは無効です。
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）– ハードディスクへのアクセスを許可します。 Block – ハードディスクへのアクセスをブロックします。
[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。複数のアクセスルールをリ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ュールを指定できます。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ます。		

設定	説明	値
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）では、アクセスルールがすべてのユーザーに適用されます。 **< ユーザー名 >** は、アクセスルールが適用されるローカルユーザーまたはドメインユーザーの名前です（システム上でこの形式でのユーザー名の入力が許可されている場合はドメインを含むフルネームを指定しないか、**<ドメイン名>\<ユーザー名>** または **<ユーザー名>@< ドメイン名>** の形式で指定します）。 **@< グループ名 >** は、アクセスルールが適用される（ローカルまたはドメイン）ユーザーグループの名前です。
[RemovableDrivePrincipals.item_#.AccessRules.item_#] には、アクセスルールの設定が含まれています。		
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）– アクセスルールは有効です。 No – アクセスルールは無効です。
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）– リムーバブルドライブへのアクセスを許可します。 Block – リムーバブルドライブへのアクセスをブロックします。
[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。複数のアクセスルールをフロ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を指定できます。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）では、アクセスルールがすべてのユーザーに適用されます。 **< ユーザー名 >** は、アクセスルールが適用されるローカルユーザーまたはドメインユーザーの名前です（システム上でこの形式でのユーザー名の入力が許可されている場合はドメインを含むフルネームを指定しないか、**<ドメイン名>\<ユーザー名>** または **<ユーザー名>@< ドメイン名>** の形式で指定します）。 **@< グループ名 >** は、アクセスルールが適用される（ローカルまたはドメイン）ユーザーグループの名前です。
[FloppyDrivePrincipals.item_#.AccessRules.item_#] には、アクセスルールの設定が含まれています。		
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）– アクセスルールは有効です。 No – アクセスルールは無効です。
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）– フロッピーディスクへのアクセスを許可します。 Block – フロッピーディスクへのアクセスをブロックします。
[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。複数のアクセスルールを 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ルを指定できます。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）では、アクセスルールがすべてのユーザーに適用されます。 **< ユーザー名 >** は、アクセスルールが適用されるローカルユーザーまたはドメインユーザーの名前です（システム上でこの形式でのユーザー名の入力が許可されている場合はドメインを含むフルネームを指定しないか、**<ドメイン名>\<ユーザー名>** または **<ユーザー名>@< ドメイン名>** の形式で指定します）。 **@< グループ名 >** は、アクセスルールが適用される（ローカルまたはドメイン）ユーザーグループの名前です。
[OpticalDrivePrincipals.item_#.AccessRules.item_#] には、アクセスルールの設定が含まれています。		

設定	説明	値
`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）– アクセスルールは有効です。 `No` – アクセスルールは無効です。
`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/DVD ドライブへのアクセスを許可します。 `Block` – CD/DVD ドライブへのアクセスをブロックします。

コマンドラインでの接続デバイスリストの表示とエクスポート

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 --get-device-list [--all] [--json]
```

説明：

- `--all` は接続済みのすべてのデバイスを一覧表示します。
- `--json` は、接続済みのデバイスをJSON形式で一覧表示します。

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。
- **Name**。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）。
- **Bus**。接続バス。指定可能な値：`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。

接続されたデバイスのリスト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 --get-device-list --export <file>
```

<ファイル>は、接続されているデバイスのリストを保存する JSON ファイルの完全パスです。

信頼するデバイスの一覧がエクスポートされます。

コマンドラインでの信頼するデバイスリストの管理

信頼するデバイスのリストには、アクセスが許可されているデバイス（特定のユーザーまたはグループ）に関する情報が含まれています。

コマンドラインでは、信頼するデバイスのリストを表示したり、リストにデバイスを追加または削除したり、ファイルから信頼するデバイスのリストをインポートしたりできます。

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 --trusted-devices --list
```

信頼するデバイスのリストにデバイスを追加するには、次のコマンドを実行します：

```
kesl-control --trusted-devices --add <ID>
```

ここで、**<識別子>** はデバイス ID またはデバイス ID マスクです。

信頼するデバイスのリストからデバイスを削除するには、次のコマンドを実行します：

```
kesl-control --trusted-devices --delete <ID>
```

ここで、**<識別子>** はデバイス ID またはデバイス ID マスクです。

ファイルから信頼するデバイスのリストをインポートするには、次のコマンドを実行します：

```
kesl-control --trusted-devices --merge|--add|--replace --file <file>
```

説明：

- `--merge` は、信頼するデバイスのリストをマージします。現在のリストおよびインポートされたリストに同じ ID を持つデバイスのエントリが含まれている場合、既存のエントリがアップデートされます。現在のリストにないデバイスの場合、エントリが追加されます。
- `--add` は、インポート時に現在の信頼するデバイスのリストを追加します。以前にデバイスリストになかったデバイスのエントリのみがリストに追加されます。
- `--replace` は、現在の信頼するデバイスのリストを置き換えます。信頼するデバイスの既存のリストは、インポートされたリストに置き換えられます。
- `--file` **<ファイル>** は、信頼するデバイスのリストのインポート元となる JSON ファイルへの完全パスです。

デバイスへの一時的なアクセスの許可

デバイスコントロールを設定する際に、管理ユーザーが誤って、ユーザーの作業に必要なデバイスへのアクセスをブロックしてしまうことがあります。ユーザへのアクセスまたはデバイスコンテンツの操作が誤ってブロックされたと思われる場合は、企業のプライベートネットワークのオペレーターに、ブロックされたデバイスへの一時アクセスを要求できます。

管理者がユーザーに許可している場合、ユーザーは一時アクセスを要求できます。管理者は、Web コンソール、管理コンソール、またはデバイスコントロールタスクの設定のポリシーのプロパティでこの権限を設定できます。

ブロックされたデバイスへのアクセスを許可するには、次の手順を実行します：

1. ユーザーは*アクセス要求ファイル*を作成し、メールや利用可能な任意の方法で管理者に送信します（管理者はブロックメッセージテンプレートでこれを設定できます）。ユーザーはアプリケーションのグラフィカルインターフェイスまたはコマンドラインで、ブロックされたデバイスへの一時アクセスを要求することを許可できます。

2. 管理者はアクセス要求ファイルに基づいて*アクセスキー*を作成し、メールなどの方法でユーザーに渡します。ブロックされたデバイスへのアクセスは、Web コンソールで許可されます。

3. ユーザーはアクセスキーをアップロードし、ブロックされたデバイスへの一時的なアクセス権を取得します。ユーザーは、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またはコマンドラインでアクセスキーをアップロードできます。

ブロックされたデバイスへのアクセスを許可できるのは、組織内に Kaspersky Security Center 16.1 が導入されており、クライアントデバイスが管理サーバーとの接続を確立できる場合のみです。

Web コンソールでのブロックされたデバイスへのアクセスの許可

ブロックされたデバイスへのアクセスを許可できるのは、組織内に Kaspersky Security Center 16.1 が導入されており、クライアントデバイスが管理サーバーとの接続を確立できる場合のみです。

管理者は、ユーザーから一時アクセス要求を受け取った場合、Web コンソールでアクセス要求ファイルからアクセスキーを作成できます。

デバイスへの一時的なアクセスを提供するには、管理者は**データ暗号化**機能に対する読み取り、書き込み、および実行権限を持っている必要があります（［**ユーザーとロール**］→［**ロール**］→<ユーザーロール>→ユーザーロールのプロパティウィンドウ→［**アクセス権**］タブ→<アプリケーション名>→［**データ暗号化**］→**読み取り / 書き込み / 実行**）。

ブロックされたデバイスのアクセスキーを作成する場合：

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. 該当するデバイスを含む管理グループを選択し、デバイス名の横にあるチェックボックスをオンにします。

3. 管理対象デバイスのリストの上にある［**オフラインモードでデバイスへのアクセスを許可する**］をクリックします。このボタンがデバイスリストの上に表示されない場合は、三点リーダーをクリックし、メニューから［**オフラインモードでデバイスへのアクセスを許可する**］コマンドを選択します。

4. これにより、［**アプリケーション設定**］ウィンドウが開きます。そのウィンドウの**デバイスコントロール**セクションで［**参照**］をクリックし、ユーザーから受信したアクセス要求ファイルをダウンロードします。

   ユーザーがアクセスを要求したブロックされたデバイスに関する情報が表示されます。

5. 必要に応じて、［**アクセス期間**］フィールドで期間（時間単位）を変更します。

   既定では、**アクセス期間**は、アクセス要求ファイルを生成するときにユーザーが指定した値に設定されます。

6. 必要に応じて、［**クライアントデバイスでアクセスキーを使用できる期間を指定する（時間単位）**］フィールドの値を変更します。

   このフィールドには、ユーザーがアクセスキーをアップロードできる期間が含まれます。

7. ［**キーの作成**］をクリックします。

8. アクセスキーファイルを *.acode 拡張子で保存します。

コマンドラインでのデバイスへの一時アクセス

ユーザーが、デバイスへのアクセスが誤ってブロックされた、またはデバイスの内容に対する操作が誤って禁止されたと考える場合、次のデバイスコントロール管理コマンドを使用して、組織のローカルネットワークの管理者にブロックされたデバイスへの一時アクセスを要求できます：`kesl-control --request-temporary-device-access`。

ブロックされたデバイスへの一時的なアクセスを要求するには、次のコマンドを実行します：

```
kesl-control --request-temporary-device-access --device-id <デバイス ID> --access-duration <アクセス期間> --path <アクセス要求ファイルへのパス>
```

説明：

`--device-id <デバイス ID>` は、アクセスする対象のブロックされたデバイスの ID を指定します。

`--access-duration <アクセス期間>` は、デバイスにアクセスできるようにする期間（時間単位）を指定します。可能な値：1 ～ 100

`--path <アクセス要求ファイルへのパス>` は、.akey 拡張子のアクセス要求ファイルを保存するディレクトリへのパスを指定します。

このコマンドはアクセス要求ファイルを作成し、メールなどの方法で管理者に送信する必要があります（管理者は、ブロックメッセージテンプレート内で推奨される方法を記述できます）。

管理者からアクセスキーを取得したら、デバイスへの一時アクセスを取得するため、コマンド `kesl-control --upload-temporary-device-access-key` を使用してアクセスキーをアップロードする必要があります。

ブロックされたデバイスに一時的にアクセスするには、次のコマンドを実行します：

```
kesl-control --upload-temporary-device-access-key --path <アクセスキーを含むファイルへのパス>
```

説明：

`--path <アクセスキーを含むファイルへのパス>` は、デバイスへのアクセスキーを含むファイル（.acode 拡張子のファイル）へのパスです。

このコマンドは、デバイスに許可されたアクセスおよびアクセス期間に関する情報を出力します。

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、トラフィック消費量を削減し、業務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、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。

> Kaspersky Endpoint Security のトラフィック読み取りの除外リストを設定している場合、ウェブコントロールに影響します。

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。ブラウザーによるインターネットアクセスを制限するときに、IT 部門以外の社内ユーザーを対象にするような使い方ができます。

- **ルールのスケジュール**：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。ブラウザーによるインターネットアクセスを制限するときに、対象時間を就業時間中のみに限定するような使い方ができます。

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ことで、ユーザーは誤ったブロックについて企業 LAN の管理者に問い合わせのメッセージを送信し、ブロックされた Web リソースへのアクセスをリクエストできます。

- *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ことで、ユーザーは誤った警告について企業 LAN の管理者に問い合わせのメッセージを送信できます。その間、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。

それぞれのルールには優先順位が割り当てられています。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（**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**）でウェブコントロール設定を設定できます。

管理コンソールでの ウェブ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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**セキュリティコントロール → ウェブコントロール**）で、ウェブコントロール設定を管理できます。

ウェブコントロールの設定

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、追加、編集、削除、**上に移動**、**下に移動**を実行できます。 ［**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。 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。

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。ルール名は一意である必要があります。
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の選択**］ウィンドウが表示されます。 • **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、［**アドレスを選択**］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、［**アドレスを選択**］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、［**ユーザーを選択**］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、［**ユーザーを選択**］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、［**アクセススケジュール**］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。
ルールの処理	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。 • **Allow**（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。

このためには、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。

ネストされたすべてのコンテンツカテゴリのチェックボックスを選択しても、親コンテンツカテゴリのチェックボックスは自動的には選択されません。

［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。

このためには、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。

［アドレスを選択］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。

［**アドレスを選択**］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。

テーブル内の項目は、追加、編集、または削除できます。

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［**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。

［ユーザーを選択］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またはユーザーグループのいずれかまたは両方の名前が含まれます。

テーブル内の項目は、追加、編集、または削除できます

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	このテーブルでは、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。

  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する方法：

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. ポリシーのプロパティウィンドウで、**製品設定 → Security Controls → Web Control**を選択します。

5. ［**メッセージのテンプレート**］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。
   - **ブロックに関するメッセージ**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適用される際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**［**ブロックに関するメッセージ**］**タブ**では、［**変数を追加**］ボタンと［**リンクを追加**］ボタンをクリックして、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。

   ［**既定を復元**］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**］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適用される際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 管理コンソールの［**ユーザのリクエスト**］を選択して表示できます。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**］と［**リンク**］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。

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。	Allow（既定値）– Web リソースへのアクセスを許可します。 Block – 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：		
Name	Web リソースアクセスルール名。ルール名は一意である必要があります。	
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。	Allow（既定値）– Web リソースへのアクセスを許可します。 Block – Web リソースへのアクセスをブロックします。 Notify – 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。
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、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。 No（既定値）– 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。
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ルールを適用します。
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にマ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。	None（既定）– Web リソースコンテンツフィルターを使用しません。 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ます。 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。	–

設定	説明	値
ContentCategory	コンテンツカテゴリ。	AdultContent, AlcoholTobaccoNarcotics, Violence, Profanity, Weapons, ChatForum, WebMail, OnlineShops, SocialNets, Recruitment, HttpQueryRedirection, CreditCards, PoliceDecision, SoftwareAudioVideo, TechnologyElectronics, GamblingLotteriesSweepstakes, InternetCommunicationMedia, CryptocurAndMining, LegislationBE, ECommerce, ComputerGames, Religions, News, Torrents, FileSharing, AudioAndVideo, BankSites, Blogs, DatingSites, LegislationRF, LegislationGlobal, SexuallyExplicit, Sexuality, GenerativeAITools
[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 アプリケーションファイル 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ルターを使用します。 No（既定値）– ユーザーフィルターを使用せず、すべてのユーザーにルールを適用します。
[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。	
Name	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。	< **ユーザー名** > は、ルールを適用するユーザーの名前です。 **@< グループ名 >** は、ルールを適用するユーザーグループの名前です。 既定値：Web リソースアクセスルールはすべてのユーザーに適用されます。
[UrlCategories.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にマ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 – 999999 0 が Default のスケジュールの ID であり、ルールは時間制限なしで、常に機能します。

設定	説明	値
Name	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。	< **曜日** > は曜日です。完全な曜日名または省略形のいずれかを使用できます（たとえば、月曜日の場合は、Mo、Mon、Monday で指定できます）。平日には、間隔または特定の日を指定できます。週は日曜日から始まります。 < **時** > は時間 [0:24] です。指定できる間隔の単位は時間のみです。

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 <設定情報ファイルへのパス>] [--json]
```

説明：

--file <設定情報ファイルへのパス>は、設定が書き込まれる設定情報ファイルへの完全パスです。

--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 <設定情報ファイルへのパス>] [--json]
```

説明：

--file <設定情報ファイルへのパス>は、設定のインポート元となる設定情報ファイルへの完全パスです。

--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 `*.`。

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`、 `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にある文字シーケンス `/*` は、`/*` または空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

番号	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	含まれない	ルール 1 を参照
2	*.example.com	http://www.123.example.com	含まれる	ルール 2 を参照

番号	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
3	*example.com	http://www.123example.com	含まれる	ルール 1 を参照
4	*example.com	http://www.123.example.com	含まれる	ルール 1 を参照
5	http://www.*.example.com	http://www.123example.com	含まれない	ルール 1 を参照
6	www.example.com	http://www.example.com	含まれる	ルール 3、2、1 を参照してください。
7	www.example.com	https://www.example.com	含まれる	ルール 3、2、1 を参照してください。
8	http://www.*.example.com	http://123.example.com	含まれる	ルール 3、4、1 を参照してください。
9	www.example.com	http://www.example.com/abc	含まれる	ルール 3、5、1 を参照してください。
10	example.com	http://www.example.com	含まれる	ルール 3 と 1 を参照してください。
11	http://example.com/	http://example.com/abc	含まれる	ルール 6 を参照
12	http://example.com/*	http://example.com	含まれる	ルール 7 を参照
13	http://example.com	https://example.com	含まれない	ルール 8 を参照
14	"example.com"	http://www.example.com	含まれない	ルール 9 を参照
15	"http://www.example.com"	http://www.example.com/abc	含まれない	ルール 9 を参照
16	"*.example.com"	http://www.example.com	含まれる	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	含まれる	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	含まれる	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	含まれない	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。

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読み取ることにより、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管理できます。

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、ポリシープロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**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の設定を管理できます。

システム変更監視設定の設定

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
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
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。

テーブル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。

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。

[除外範囲] ウィンドウ

このウィンドウには、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。テーブル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。

監視除外範囲の設定

設定	説明
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
除外範囲名	除外範囲名。

設定	説明
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。

既定では、除外範囲のテーブルは空です。テーブル内の項目は、追加、編集、または削除できます。

また、[**インポート**]をクリックしてファイルから除外範囲のリストをインポートすることも、[**エクスポート**]をクリックして除外範囲のリストを JSON 形式 で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、除外範囲のリストを置き換えるか、既存のリストに除外範囲を追加するように求められます。

[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。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。 [**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、監視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。

[**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、監視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）。

インポートボタンを使用してファイルから除外リストをインポートしたり、**エクスポート**ボタンを使用して除外リストをJSONファイルにエクスポートしたり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。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。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。

オンアクセスシステム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`	監視範囲の説明。監視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。

設定	説明	値
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_#] 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）

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。

ベースラインは、タスク設定が変更された場合（たとえば、新しい監視範囲が追加された場合）だけでなく、タスクを `RebuildBaseline=Yes` 設定を指定して開始した場合（または Kaspersky Security Center のタスクのプロパティで［**タスク開始ごとにベースラインを再構築する**］チェックボックスがオンになっている場合）にも更新されます。

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 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みなされません）。 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、システム変更チェック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、編集、削除、上に移動、下に移動。 また、［**インポート**］をクリックしてファイルから監視範囲のリストをインポートすることも、［**エクスポート**］をクリックして監視範囲のリストを JSON 形式 で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、監視範囲のリストを置き換えるか、既存のリストに監視範囲を追加するように求められます。

［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。

設定	説明
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。

[除外範囲]セクション

システム変更チェックタスクの[**除外リスト**]では、スキャンの除外リストと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、システム変更チェックコンポーネントの監視除外範囲が表示されます。テーブル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。

テーブル内の項目は、追加、編集、または削除できます。

インポートボタンを使用してファイルから除外リストをインポートしたり、**エクスポート**ボタンを使用して除外リストをJSONファイルにエクスポートしたり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。

[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。

設定	説明
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。

［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。

［**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）。

インポートボタンを使用してファイルから除外リストをインポートしたり、**エクスポート**ボタンを使用して除外リストをJSONファイルにエクスポートしたり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。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。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では、システム変更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構築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みなされません）。 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、システム変更チェック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。

テーブル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。

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。

設定	説明
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。

[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、システム変更チェックコンポーネントのスキャン除外範囲が表示されます。テーブル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。

システム変更チェックタスクのスキャン除外範囲の設定

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。

テーブル内の項目は、追加、編集、または削除できます。

[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。

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。 ［**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。

［**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）。

インポートボタンを使用してファイルから除外リストをインポートしたり、**エクスポート**ボタンを使用して除外リストをJSONファイルにエクスポートしたり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。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージする場合は、[**継承した値を統合する**]チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。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システム変更チェックの設定

ユーザー *システム変更チェックタスク*（*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変更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：*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 – ファイルの最終アクセス日時を追跡します。 No（既定値）– ファイルの最終アクセス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	監視範囲の説明。監視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。

設定	説明	値
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。

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。

脆弱性攻撃ブロックコンポーネントを最適に動作させるには、ふるまい検知コンポーネントを有効にすることをお勧めします。

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。
- ふるまい検知コンポーネントと MDR および EDR Expert（オンプレミス）コンポーネントによるスキャンからプロセスアクティビティを除外します。

  本製品は、Watchdog サーバープロセスのアクティビティをスキャンから自動的に除外します。この除外は削除できません。

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。

root ユーザーが NFSv4 プロトコル経由でデバイスにマウントされたリモートディレクトリにアクセスできない場合、すべてのアプリケーションに対してそのようなファイルへのアクセスがブロックされます。

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、ポリシープロパティ（**製品設定 → ホスト脅威対策 → ふるまい分析 → ふるまい検知**）でふるまい検知の設定を管理できます。

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、ポリシープロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**先進の脅威対策 → ふるまい検知**）で、ふるまい検知設定を管理できます。

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。 • 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

このウィンドウには、プロセスごとの除外範囲が含まれています。プロセスによる除外の除外範囲を使用すると、指定されたプロセスのアクティビティを除外できます。

プロセスによる除外範囲の設定

設定	説明
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 既定では、このチェックボックスはオフです。
除外範囲名	除外範囲名。
パス	除外されるプロセスの完全パス。
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。

既定では、除外範囲のテーブルは空です。テーブル内の項目は、追加、編集、または削除できます。

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。
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。
ふるまい検知のスキャンからプロセスを除外する	このチェックボックスは、ふるまい検知によるスキャンからプロセスの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。
MDR および EDR Expert（オンプレミス）テレメトリからプロセスを除外	このチェックボックスは、 MDR および EDR Expert（オンプレミス）コンポーネントによって収集されたテレメトリからのプロセスの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。

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
`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。
`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。
[TrustedPrograms.item_#] セクションには、ふるまい検知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。		

設定	説明	値
ProgramPath	除外するプロセスのパス。	< **プロセスへの完全パス** > – 指定されたローカルディレクトリ内のプロセスをスキャンしません。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のアクティビティをスキャンから除外します。	Yes（既定値）– 指定されたプロセスのアクティビティをスキャンから除外します。 No – 指定されたプロセスのアクティビティをスキャンから除外しません。
UseTrustedProgramForDetects	ふるまい検知によるスキャンからプロセスのアクティビティを除外します。	Yes に設定すると、指定されたプロセスのアクティビティはふるまい検知によるスキャンから除外されます。 No（既定）に設定すると、指定されたプロセスのアクティビティはふるまい検知によるスキャンから除外されません。
UseTrustedProgramForMDRAndEDR	MDR および EDR Expert（オンプレミス）コンポーネントによって収集されるテレメトリからプロセスを除外します。	Yes – MDR および EDR Expert（オンプレミス）コンポーネントによって収集されるテレメトリから、このプロセスのアクティビティを除外します。 No（既定）– テレメトリからこのプロセスのアクティビティを除外しません。
TelemetrySource	Detection and Response ソリューションと連携されている場合に、それらのソリューションに送信されるテレメトリを収集するための追加設定。 UseTelemetryMonopolyMode 設定は、TelemetrySource が Default に設定されている場合にのみ適用されます。	Default（既定）は、テレメトリを収集するために eBPF 技術と auditd サービスが使用されることを意味します。 OnlyEBPF は、テレメトリの収集に eBPF 技術のみが使用されることを意味します。
UseTelemetryMonopolyMode		True（既定）は、Kaspersky Endpoint Security が auditd サービスを排他モードで使用することを意味します。 False は、auditd サービスが非排他モードで使用されることを意味します。

脆弱性攻撃ブロック

脆弱性攻撃ブロックは、デバイスの脆弱性を悪用して管理者権限を取得したり悪意のある処理を実行したりするコードを監視します。たとえば、脆弱性を悪用した攻撃の例としては、バッファーオーバーフロー攻撃などがあります。この攻撃では、脆弱性のあるアプリケーションに大量のデータが送信され、このデータの処理中に、悪意のあるコードが脆弱性のあるアプリケーションによって実行されてしまいます。この攻撃により、不正にマルウェアをインストールされてしまう可能性があります。脆弱なアプリケーションから実行ファイルを実行しようとしたのがユーザーではなかった場合、Kaspersky Endpoint Security はこのファイルの実行をブロックするか、ユーザーに通知します。既定では、脆弱性攻撃ブロックは無効になっています。

脆弱性攻撃グロックには、ふるまい検知と更新可能なカーネルモジュールの有効化が必要です。脆弱性攻撃ブロックコンポーネントを最適に動作させるには、 ウェブ脅威対策コンポーネントも有効にすることを推奨します。

脆弱性攻撃ブロックおよび管理コンポーネントの設定を有効または無効にできます。

- エクスプロイトが検知されたときにアプリケーションが実行す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。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通りです：
  - オブジェクト内で検知された脅威の名前
  - 指定されたパスにあるファイルとディレクトリ
  - 指定されたハッシュを持つファイル

Web コンソールでの脆弱性攻撃ブロックの設定

Web コンソールでは、ポリシーのプロパティ（**[製品設定] → ホスト脅威対策 → ふるまい分析 → 脆弱性攻撃ブロック**）で、ぜい弱性攻撃ブロック設定を管理できます。

管理コンソールでの脆弱性攻撃ブロックの設定

管理コンソールでは、ポリシーのプロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**[先進の脅威対策] → [ふるまい検知]**）で、ぜい弱性攻撃ブロック設定を管理できます。

脆弱性攻撃ブロックの設定

設定	説明
脆弱性攻撃ブロックを有効にする	このチェックボックスでは、脆弱性攻撃ブロック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。
脆弱性攻撃ブロックセクション。	**[設定]** をクリックすると、**[ぜい弱性攻撃ブロックの除外]** ウィンドウが開き、ぜい弱性攻撃ブロックコンポーネントのスキャンからの除外を設定できます。

設定	説明
脆弱性の検知時の処理	エクスプロイトが検知されたときに本製品が実行する処理 • **ブロック**（既定値）：本製品は、エクスプロイトの悪意のあるアクティビティをブロックし、その情報をイベントログに記録します。 • **通知する**。本製品はエクスプロイトのアクティビティをブロックするのではなく、エクスプロイトの検知に関する情報をイベントログに記録するだけです。

脆弱性攻撃ブロック除外ウィンドウ

このウィンドウでは、脆弱性攻撃ブロックのスキャンからオブジェクトの除外を設定できます。指定されたオブジェクトはスキャンされません。既定では、オブジェクトのリストは空です。

脆弱性攻撃ブロック除外の設定

設定	説明
継承した値を統合する	このチェックボックスは、子ポリシーに継承されるときにリストのマージ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、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。 チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。 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。
脅威の名前。	スキャンから除外される脅威の名前です。
ファイルまたはディレクトリのパス	スキャンから除外するファイルまたはディレクトリへの完全パスです。
ファイルハッシュ	スキャン対象から除外されたファイルのハッシュです。
コメント	スキャンの除外に関するコメントです。

既定では、除外の表は空です。テーブル内の項目は、追加、編集、または削除できます。

脆弱性攻撃ブロック除外ウィンドウ

このウィンドウでは、脆弱性攻撃ブロックスキャンから除外するオブジェクトを追加または設定できます。

脆弱性攻撃ブロック除外の設定

設定	説明
脅威の名前を使用する	このチェックボックスは、オブジェクトで検知された脅威の名前によるスキャンからの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ンです。
脅威の名前。	このフィールドには、オブジェクトで検知された脅威の名前を入力できます。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。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。 このフィールドは、［**脅威の名前を使用する**］チェックボックスがオンの場合に使用できます。
ファイルハッシュを使用する	このチェックボックスは、ファイルのハッシュによるスキャンからの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ンです。
ファイルのハッシュサム種別	このドロップダウンリストでは、スキャンからファイルを除外するために使用するファイルのハッシュ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、［**ファイルのハッシュを使用する**］チェックボックスが選択されている場合に使用できます。

設定	説明
ファイルのハッシュサム	このフィールドには、スキャンする際に除外するファイルのハッシュを入力できます。 このフィールドは、［**ファイルのハッシュを使用する**］チェックボックスが選択されている場合に使用できます。
ファイルまたはディレクトリのパスを使用する	このチェックボックスは、パスによって脅威が検知されたファイルの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ンです。
ファイルまたはディレクトリのパス	スキャンから除外するファイルまたはディレクトリのパスを指定する入力フィールドです。パスには * および ? 文字を使用できます。 このフィールドは、［**ファイルまたはディレクトリのパスを使用する**］チェックボックスが選択されている場合に使用できます。
コメント	コメントの入力フィールド（任意）。
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除外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。

コマンドラインでの脆弱性攻撃ブロックの設定

コマンドラインでは、ふるまい検知 (*Behavior_Detection*) 事前定義済みタスクの設定を使用して、脆弱性攻撃ブロックを管理できます。

脆弱性攻撃ブロック は、ふるまい検知の事前定義タスクの設定を編集することで設定できます（下のテーブルを参照してください）。

脆弱性攻撃ブロックの設定

設定	説明	値
`UseAEP`	脆弱性攻撃ブロックコンポーネントを有効にします。	`Yes` を選択すると、脆弱性攻撃ブロックが有効になります。 `No`（既定）の場合、脆弱性攻撃ブロックが無効になります。
`AEPMode`	脆弱性攻撃が検知されたときに行うべき処理です。	`Block`（既定）に設定すると、脆弱性攻撃の悪意のあるアクティビティがブロックされ、イベントがログに記録されます。 `Notify` に設定すると、脆弱性攻撃のアクティビティはブロックされず、検知された脆弱性攻撃に関する情報のみがイベントログに記録されます。
[AEPExclusions.item_#] セクションには、脆弱性攻撃ブロックコンポーネントのスキャンからの除外が含まれています。		
`Enabled`	脆弱性攻撃ブロックコンポーネントのスキャンからの除外を有効にします。	`Yes` （既定値） – 脆弱性攻撃ブロックの除外を使用します。 `No` ー ぜい弱性攻撃ブロック除外を使用しません。
`DetectName`	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、`UseDetectName` 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。 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。
`Hash`	ハッシュによって脅威が検知された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、`UseHash` 設定が有効になっていることを確認します。	
`HashType`	`Hash` パラメータを使用したスキャンからファイルを除外するために使用するファイルのハッシュのタイプ。	`Md5` ー MD5 ハッシュ `Sha256` ー SHA256 ハッシュ
`Path`	パスによって脅威が検知された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、`UsePath` 設定が有効になっていることを確認します。	**< ファイルまたはローカルディレクトリへの完全パス >** – 指定したディレクトリ（サブディレクトリを含む）内のファイルまたはオブジェクトをスキャンから除外します。パスには * および ? 文字を使用できます。

設定	説明	値
UseDetectName	DetectName 設定で指定された脅威を含むオブジェクトをスキャンから除外できるようにします。	Yes（既定）ー DetectName 設定で指定された脅威を含むオブジェクトをスキャンから除外します。 No ー DetectName 設定を使用して指定した脅威を含むオブジェクトをスキャンから除外しません。
UseHash	ハッシュによって脅威が検知されたファイルを除外します。ファイルのハッシュは Hash パラメーターで指定します。	Yes（既定値）－ハッシュによって脅威が検知されたファイルを除外します。 No ーハッシュによって脅威が検知されたファイルを除外しません。
UsePath	パスによって脅威が検知されたファイルを除外します。ファイルへのパスはPathパラメーターを使用して指定します。	Yes（既定）ーパスによって脅威として検知されたファイルを除外します。 No ーパスによって脅威が検知されたファイルを除外しません。

Kaspersky Security Network の使用

KSN 機能は、米国領土内のアプリケーションでは利用できない場合があります。

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。

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

新しいライセンスでアプリケーションをアクティベートした後に 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。

Kaspersky Security Network は、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使用できます。

個人データの収集、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対策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、管理サーバーの 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。

Kaspersky Endpoint Security を標準モードで使用する場合は、Kaspersky Security Center Web コンソールまたは管理コンソールを使用して次の KSN プロキシサーバー設定を設定できます：

KSN プロキシ設定はコマンドラインでは管理できません。

Kaspersky Security Center では、Kaspersky Endpoint Security による KSN プロキシサーバーの使用に関して次の設定を行うことができます：

- 管理サーバーの KSN プロキシサーバーとしての使用を有効または無効にします。
- KSN プロキシサービスが利用できない場合に、KSN サーバーとの直接のやり取りを許可または拒否します。

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（**アプリケーション設定 → 全般設定 → Kaspersky Security Network**）で、アプリケーションによる Kaspersky Security Network の使用を設定できます。

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。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**先進の脅威対策 → Kaspersky Security Network**）で、Kaspersky Endpoint Security による 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 プロキシサーバーとして管理サーバーを使用する	このチェックボックスをオンにすると、Kaspersky Endpoint Security は管理サーバー上の KSN プロキシサービスを使用して KSN サーバーと通信します。 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。仮想環境保護用 Light Agent モードでは、本製品は KSN プロキシサーバー経由でのみ KSN インフラストラクチャと通信できます。
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をオンにすると、Kaspersky Endpoint Security は管理サーバー上の KSN プロキシサービスを使用できない場合に、直接 KSN サーバーと通信します。 既定では、このチェックボックスはオンです。 このチェックボックスは、［**KSN プロキシサーバーとして管理サーバーを使用する**］が選択されている場合に使用できます。 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。

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。カスペルスキー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。カスペルスキー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 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。 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 Private 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 の使用の設定

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オプション。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 の利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 <設定情報ファイルへのパス> [--json] [--accept-ksn]
```

説明：

- --file <設定情報ファイルのパス> は、必要な UseKSN の値が設定されている全般的なアプリケーション設定を含む設定情報ファイルの完全パスです。
- JSON 構成ファイルから設定をインポートする場合は、--json オプションを指定します。--json オプション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オプション。Kaspersky Security Network の使用を有効にする場合は、オプション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 の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。

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、コマンドラインのオプションを使用して、 `CloudMode` 設定の値を編集できます。

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。

アプリケーションの詳細設定

次の追加アプリケーション設定を行うことができます：

- 本製品用のプロキシサーバー。
- 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の読み取り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。
- ファイル操作の読み取りモード。
- 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の検出。
- アプリケーションの安定性監視。
- アプリケーションの起動設定。
- 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 の保管領域へのデータ転送の設定。
- タスク管理許可。
- バッテリー電源で動作しているデバイスでスケジュールされたタスクをキャンセル。
- システムイベントインターセプターの設定。
- テレメトリの追加設定。

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、カスペルスキーアクティベーションサーバーに接続したり、定義データベースと機能のソースをアップデートしたり、Kaspersky Security Network に接続したり、ウェブ脅威対策コンポーネントを使用して Web サイトの証明書を検証したりするときに、プロキシサーバーを使用できます。

プロキシサーバーは、既定で無効になっています。

アクティベーションコードを使用して、インターネットにアクセスできない隔離されたネットワークセグメント内のデバイスをアクティベートする場合は、カスペルスキーアクティベーションサーバーにアクセスするためのプロキシサーバーとして Kaspersky Security Center 管理サーバーを使用できます。Web コンソールまたは管理コンソールで、管理サーバーをアクティベーションサーバーにアクセスするためのプロキシサーバーとして使用できるようにできます。

Web コンソール、管理コンソール、またはコマンドラインで、プロキシサーバーの次の除外を設定できます：

- Detection and Response ソリューションとの連携を提供する EDR Expert（オンプレミス）、NDR (KATA)、およびサンドボックスのコンポーネントの場合。プロキシサーバーをバイパスする必要があるコンポーネントを指定できます。
- URL 用。プロキシサーバーをバイパスして接続するアドレスのリストを指定できます。

Kaspersky Endpoint Security を Light Agent モードで使用する場合、Kaspersky Security Network、SVM、および Integration Server へ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ていません。Kaspersky Security Center 管理サーバーをカスペルスキーアクティベーションサーバーにアクセスするためのプロキシサーバーとして使用することにも対応していません。

Web コンソールでのプロキシサーバーの設定

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**] → [**ネットワーク設定**]）でプロキシサーバーの設定を指定できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定 → プロキシサーバー設定**）で、プロキシ設定を管理できます。

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。
指定したプロキシサーバー設定を使用する	このオプションを選択すると、アプリケーションは指定されたプロキシサーバー設定を使用して、カスペルスキーアクティベーションサーバーに接続し、定義データベースと機能のソースをアップデートし、Kaspersky Security Networkに接続し、ウェブ脅威対策コンポーネントを使用して Web サイトの証明書を検証します。
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。

設定	説明
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	カスペルスキーアクティベーションサーバーにアクセスするためのプロキシサーバーとして Kaspersky Security Center 管理サーバーの使用を有効または無効にします。これは、アクティベーションコードを使用して、インターネットにアクセスできない分離されたネットワークセグメントでアプリケーションをアクティベートする場合に必要です。 このチェックボックスをオンにすると、インターネットにアクセスできる管理サーバー経由でアクティベーションサーバーにアクセスできるようになります。 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。
プロキシサーバーの除外リスト	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、［**プロキシサーバーの除外**］ウィンドウが表示されます。

プロキシサーバーの除外ウィンドウ

このウィンドウでは、Kaspersky Anti Targeted Attack Platform ソリューションのコンポーネントとIntegration Server を連携している場合のプロキシ サーバーの使用と、プロキシサーバーをバイパスするアドレスのリストを設定できます。

プロキシサーバーの除外リスト

設定	説明
コンポーネントにプロキシサーバーを使用しない	プロキシサーバーを使用しない製品コンポーネントの横にあるチェックボックスをオンにします。 • **Endpoint Detection and Response Expert（オンプレミス）**ー Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) との連携を提供するサーバーへの接続時に、プロキシサーバーを使用しません。 • **サンドボックス**ーサンドボックスとの対話を提供するサーバーに接続するときにプロキシサーバーを使用しません。 • **Kaspersky Detection and Response (KATA)**ー Kaspersky Network Detection and Response (KATA)との連携サーバーに接続する時は、プロキシサーバを使用しません。
アドレスにプロキシサーバーを使用しない	この表には、プロキシサーバーをバイパスして接続するアドレスのリストが含まれています。 • **IP アドレス/DNS 名**は、プロキシサーバーを使用せずに接続する IP アドレスまたは DNS 名です。アドレスの指定にマスク（* と ?）が使用できます。 • オプションで、［**コメント**］フィールドにコメントを入力できます。 表内のアドレスは、**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。

コマンドラインでのプロキシサーバー設定の構成

コマンドラインでは、UseProxy、ProxyServer、ProxyBypass、ProxyBypassEdr、ProxyBypassNdr、および ProxyBypassSandbox の全般設定を使用して、製品コンポーネントのプロキシサーバー設定を管理できます。

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。

［UseProxy］パラメータが取り得る値は、次のとおりです：

- 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設定では、プロキシサーバー設定を次の形式で指定できます：**<接続プロトコル>://[<ユーザー>[:<パスワード>]@]<プロキシサーバーのアドレス**<code class="programcharacter">a:<</code>**ポート番号>**、ここで：

- **<ユーザー>**は、プロキシサーバーでの認証に使用するユーザー名です。
- **<パスワード>**は、プロキシサーバーでの認証に使用するユーザーパスワードです。
- **<プロキシサーバーのアドレス>**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。
- **<ポート番号>**は、プロキシサーバーのポート番号です。

HTTPS 経由のプロキシサーバーへの接続には対応していません。

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。

ProxyBypass 設定を使用すると、プロキシサーバーを使用せずに接続されるアドレスのリストを指定できます。アドレスは、**<アドレス>[:<ポート番号>]** 形式で指定します。アドレスを指定するには、マスク（*記号）とコメント（\ 記号の後）を使用できます。

次の設定により、Detection and Response ソリューションとの連携を提供する EDR Expert（オンプレミス）、NDR（KATA）およびサンドボックスコンポーネントによるプロキシサーバの使用を設定できます。

- ProxyBypassEdr 設定は、Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) との統合を提供するサーバーへの接続時に、プロキシサーバーの使用を有効または無効にします。
- ProxyBypassNdr 設定は、Kaspersky Network Detection and Response (KATA) との連携を提供するサーバーへの接続時に、プロキシサーバーの使用を有効または無効にします。
- ProxyBypassSandbox 設定は、サンドボックスとの対話を提供するサーバーに接続するときにプロキシサーバーの使用を有効または無効にします。

この設定で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。

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の読み取り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読み取りから除外できます。さらに、グローバル除外は、コンテナ監視コンポーネント（コンテナスキャン、コンテナ監視）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（**製品設定 → 信頼ゾーン → 信頼するマウントポイント**）で、グローバル除外を設定できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定 → グローバル除外**）で、グローバル除外を管理できます。

除外する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、除外する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。リストの項目は、追加、編集、削除できます。

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。 • **All remote mounted** – 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、ファイル操作の読み取り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、`?` 文字を使用して任意の文字を表示できます。 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。
ファイルシステム名	ファイル操作の読み取り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。

［ExcludedMountPoint.item_#］パラメータが取り得る値は、次のとおりです：

- 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読み取りから除外します。
- 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読み取りから除外します。
- 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読み取りから除外します。
- Mounted:<**ファイルシステム種別**> — 指定したファイルシステム種別のマウント済みディレクトリをすべて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の読み取りから除外します。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。
- <**次を含むパス**： /mnt/user* **または** /mnt/**/user_share> マスク — 名前に指定した**マスク**を含むマウントポイント内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、? 文字を使用して任意の文字を表示できます。

> 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。

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。

プロセスメモリのスキャンからの除外

プロセスメモリのスキャンの除外リストを設定できます。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 → パフォーマンス**）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。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定 → プロセスメモリを除外**）で、プロセスメモリの除外を管理できます。

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、`?` 文字を使用して任意の文字を表示できます。

子ポリシーに継承されるときに除外リストのマージを有効にできます。リスト項目をマージするには、［**スキャンからプロセスメモリを除外**］ウィンドウで［**継承した値を統合する**］チェックボックスをオンにします。チェックボックスをオンにすると、親ポリシーのリストにある項目が子ポリシーに表示され、子ポリシーのリストに項目を追加できるようになります。チェックボックスをオフにすると、ポリシー設定を継承するときにリスト項目はマージされません。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。

`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。

ファイル操作の読み取りモードの選択

ファイル操作の読み取りモードは、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。感染した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コンポーネントの **脅威の検知時の処理**（`ActionOnThreat`）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。

ファイル操作傍受のブロックモードが有効になっていない場合、ファイル脅威対策、デバイスコントロール、および実行防止保護コンポーネントは、設定されているモードに関係なく、通知モードで動作します。

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**］→［**検知の設定**］）でファイル操作の読み取りモードを設定できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定** → **アプリケーション設定** → **ファイル操作インターセプトモード**セクション）で、アプリケーショントレース設定を管理できます。

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

`FileBlockDuringScan` のFileBlockDuringScan 設定を使用して、コマンドラインでファイル操作の読み取りモードを設定できます。

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。

［`FileBlockDuringScan`］パラメータが取り得る値は、次のとおりです：

- `Yes`（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`No`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。

  このファイル操作の読み取り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。こうしたアプリケーションは必ずしも悪意のある目的を持っているわけではありませんが、ハッカーによって悪用される可能性があります。侵入者がデバイスやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションに関する詳細情報は、カスペルスキー百科事典の Web サイトを参照してください。

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 → 検知の設定**）で、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の検知設定を管理できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定 → 製品設定**、**スキャン設定**セクション）で、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の検知を有効または無効にできます。

［**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**］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、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の検知を有効または無効にできます。

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。

［`DetectOtherObjects`］パラメータが取り得る値は、次のとおりです：

- `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したり監視の設定管理をすることができる 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 → **パフォーマンス**）で、アプリケーションの安定性監視を有効または無効にできます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定** → **製品設定**、**アプリケーションの詳細設定**）で、アプリケーションの安定性監視を有効または無効にできます。

［**アプリケーションの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。

この設定を適用するには、本製品とネットワークエージェント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 Kaspersky Endpoint Security の安定性監視を構成できます。

`TrackProductCrashes` を使用すると、本製品が不安定な場合に、 Kaspersky Endpoint Security から Kaspersky Security Center にデバイスのステータス情報を送信できるようになります。この設定は次の値を使用できます：

- `Yes/true` にすると、Kaspersky Endpoint Security からKaspersky Security Centerへのデバイスステータス情報の送信が有効になります。
- `No/false` の場合、Kaspersky Endpoint Security から Kaspersky Security Center へのデバイスステータス情報の送信が無効になります。

`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` 設定を使用すると、本製品の不安定性に関する製品情報が表示されるまで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。

アプリケーションの起動設定の構成

次のアプリケーションの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 → ユーザーインターフェイス**）でアプリケーションの起動設定を管理できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定 → 製品設定**、**アプリケーションの起動設定**）で、アプリケーションの起動設定を管理できます。

［**アプリケーションの起動設定**］で［**設定**］ボタンをクリックすると、［**アプリケーションの起動設定**］ウィンドウが開き、アプリケーションの起動設定を編集できます（次の表を参照）。

アプリケーションの起動設定

設定	説明
アプリケーション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
アプリケーションの起動を待つ時間	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` 設定および `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` 設定を使用すると、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

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使用量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（**製品設定 → 全般設定 → パフォーマンス**）で常駐メモリ使用量の制限を管理できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定 → 製品設定**）で、常駐メモリ使用量の制限を設定できます。

［**アプリケーションの詳細設定**］セクションで［**設定**］ボタンをクリックすると［**詳細設定**］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）。

変更を適用するには、ポリシーが適用された後、管理対象デバイスで Kaspersky Endpoint Security アプリケーションを再起動してください。

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**。このオプションを選択すると、常駐メモリの使用量は制限されません。 • **自動で制限（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（%）で制限**。この項目を選択すると、［**メモリ使用量の制限（%）**］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。 • **サイズ（MB）で制限**。この項目を選択すると、［**メモリ使用量の制限（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。 • **割合、サイズのどちらか低い方で制限**。この項目を選択すると、［**メモリ使用量の制限（%）**］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。 • **割合、サイズのどちらか高い方で制限**。この項目を選択すると、［**メモリ使用量の制限（%）**］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。
メモリ使用量の制限（%）	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
メモリ使用量の制限（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、常駐メモリ使用量の制限を設定できます。

［MaxMemory］パラメータが取り得る値は、次のとおりです：

- off – 常駐設定のサイズは制限されません。
- < 値 >% – RAM の 1 ～ 100 パーセントの値。
- < 値 >MB – メガバイト単位の値。
- lowest/< 値 >%/< 値 >MB – パーセンテージ値とメガバイト単位の絶対値のうち小さい方。
- highest/< 値 >%/< 値 >MB – パーセンテージ値とメガバイト単位の絶対値のうち大きい方。
- 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。

メモリーとプロセッサリソースの使用の制限

スキャンタスクのメモリ使用量制限を設定できます。既定の制限は 8192 メガバイトです。

> スキャンタスクに使用可能なメモリがすべて使い果たされ、本製品が再起動されることを回避するために、スキャンタスクのメモリ使用量制限を常駐メモリ使用量制限より低く指定することを推奨します。

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。制限を設定する場合、すべての CPU コアのリソースの合計が 100% になる点に留意するようにしてください。top のユーティリティの出力では、100% は単一コアの完全使用率に相当します。したがって、10 コアの CPU（top のユーティリティでは合計 1000% とレポートされます）の場合、400% の値は CPU 全体（すべてのコアを合わせた）の使用率が 40% であることを意味します。同じ 10 コア CPU で、top のユーティリティによってレポートされる値を 150% 未満に抑えたい場合は、CPU 使用率制限として 15 を指定する必要があります。CPU 使用率の制限は 10 から 100 までの整数にする必要があります。さらに、CPU 使用率の制限はすべてのアプリケーションタスクに適用されるのではなく、*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*コンテナスキャン*のタスクにのみ適用されるため、CPU 使用率が設定された値を超える可能性があります。

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**］→［**パフォーマンス**］）でスキャンタスクの CPU およびメモリ使用量を制限する設定を管理できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定 → アプリケーション設定**、**パフォーマンス**セクション）で、CPU 使用率の制限を有効または無効にし、スキャンタスクに対する RAM の制限を設定できます。

[**パフォーマンス**] の下にある [**設定**] をクリックすると、[**スキャンタスクのパフォーマンス設定**] ウィンドウが開き、**CPU およびメモリの使用率**セクションで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。 チェックボックスがオンの場合、これらのタスクによるすべての CPU コアへの最大負荷は、右側のフィールドで指定したパーセント値未満に維持されます（すべての CPU コアへの最大合計負荷を 100% とみなします）。フィールドの値は 10 から 100 までの整数である必要があります。 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、全般的なアプリケーション設定の `UseOnDemandCPULimit` および `OnDemandCPULimit` 設定を使用して、*ODS*、*ContainerScan*、および *InventoryScan* タスクの CPU 使用率の制限を設定できます。

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。

［`UseOnDemandCPULimit`］パラメータが取り得る値は、次のとおりです：

- `Yes`：*ODS*、*ContainerScan*、および *InventoryScan* タスクの種別の 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。設定の値は 10 から 100 までの整数である必要があります。既定値：100

コマンドラインでは、kesl.ini 設定情報ファイルの `ScanMemoryLimit` 設定を使用して、*ODS*、*ContainerScan*、および *InventoryScan* タスクのメモリ使用量の制限を設定できます。既定値：8192

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カスタム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。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定 → アプリケーション設定**、**パフォーマンス**セクション）で、非特権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の上限を設定できます。

［**パフォーマンス**］セクションの［**設定**］ボタンをクリックすると、［**スキャンタスクのパフォーマンス設定**］ウィンドウが開きます。このウィンドウでは、［**カスタムスキャンタスクの数**］セクションの［**カスタムスキャンタスクの最大数**］フィールドに 0 から 100,000 の値を指定できます。既定値：00 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。

コマンドラインでの制限の設定

`LimitNumberOfScanFileTasks` の LimitNumberOfScanFileTasks 設定を使用して、コマンドラインで同時カスタムスキャンタスクの数の制限を設定できます。

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。

`LimitNumberOfScanFileTasks` は 0 から 100000 までの値を受け入れます。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。既定値：5

Kaspersky Security Center ストレージへのデータ転送の設定

Kaspersky Security Center では、バックアップのファイル、隔離ファイル、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データの 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。

クライアントデバイス上のカスペルスキーアプリケーションによって隔離されたファイルの一般的なリストは、Kaspersky Security Center に保存され、Web コンソール（**[操作] → [リポジトリ] → [隔離]**）および管理コンソール（**[詳細] → [リポジトリ] → [隔離]**）で利用できます。

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 で保管され、Web コンソール（**詳細設定 → リポジトリ → バックアップ**）および Web コンソール（**動作 → リポジトリ → バックアップ**）で利用できます。

未処理のファイルに関する情報は、Web コンソール（**操作 → リポジトリ → アクティブな脅威**）および管理コンソール（**詳細設定 → リポジトリ → 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 → リポジトリ → ハードウェア**）および管理コンソール（**詳細設定 → リポジトリ → 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、データが転送されます。

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に関する情報は、Web コンソール（[**操作**] → [**サードパーティアプリケーション**] → [**アプリケーションレジストリ**]）および管理コンソール（[**製品情報**] → [**アプリケーション管理**] → [**アプリケーションレジストリ**]）のアプリケーションリストに表示されます。アプリケーションコントロールが有効な場合、データが転送されます。

Web コンソールでのデータ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** → **KSC Integration**、管理サーバーへのデータ転送セクション、詳細設定リンク）と管理対象デバイスのプロパティ（**資産（デバイス）** → **管理対象デバイス** → <デバイス名> リンク → **アプリケーション**タブ → <Kaspersky Endpoint Security アプリケーション名> リンク → **製品設定**タブ → **ストレージ設定**セクション、**管理サーバーへのデータ転送設定**セクション）で管理サーバーの連携設定を管理できます。

Web コンソールのポリシーのプロパティでの管理サーバーへのデータ転送設定については、付録 5 で説明しています。

管理対象デバイスのプロパティでの管理サーバーへのデータ転送設定については、次の表で説明しています。

デバイスのプロパティでの管理サーバーへのデータ転送設定

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、バックアップされているファイルについてのデータ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フです。
隔離にあ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、隔離されているファイルについてのデータ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、スキャン中に処理されなかった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フです。
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データ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フです。
デバイスで見つかったアプリケーションについて通知する	このチェックボックスは、インベントリタスクがクライアントデバイス上で検出したアプリケーションのリストを管理サーバーに送信するかどうか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データ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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定** → **ストレージ設定**、**管理サーバーへのデータ転送**）または管理対象デバイスのプロパティ（**管理対象デバイス** → **デバイス**タブ → デバイスのプロパティウィンドウ → **アプリケーション**セクション → アプリケーションのプロパティウィンドウ → **ストレージ設定**、**管理サーバーへのデータ転送**セクション）で、管理サーバーへのデータ転送を有効または無効にできます。

[**管理サーバーへのデータ転送**] セクションで [**設定**] をクリックすると、**データ転送設定**が開き、管理サーバーへのデータ転送を有効または無効にすることができます。

設定	説明
隔離にあるファイルについて	このチェックボックスでは、隔離されているファイルについてのデータ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。
バックアップにあるファイルについて	このチェックボックスでは、バックアップされているファイルについてのデータ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。
処理されていないファイルについて	このチェックボックスでは、スキャン中に処理されなかった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	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データ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。
デバイスで見つかったアプリケーションについて	このチェックボックスは、インベントリタスクがクライアントデバイス上で検出したアプリケーションのリストを管理サーバーに送信するかどうか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 で作成されたローカルタスクの使用。Kaspersky Security Center のポリシーにより、ユーザーによるローカルタスクの表示と編集が禁止されている場合、Scan_My_Computer、Critical_Areas_Scan、Container_Scan、Inventory_Scan、Update（標準モード）、および Rollback（標準モード）タスクに関する情報は利用できません。
- 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および管理。

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 → ユーザーインターフェイス**）でタスクを表示および管理する権限設定を管理できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**ローカルタスク → タスク管理**）で、タスクの表示および管理の権限を管理できます。

設定	説明
ローカルタスクを許可する	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。 このチェックボックスをオンにすると、ユーザーは本製品のグラフィカルインターフェイスとコマンドラインでタスクを設定および実行できます。 このチェックボックスをオフにすると、ローカルタスクは使用されません。スケジュールされたローカルタスクは実行されません。タスクは、本製品のグラフィカルインターフェイスまたはコマンドラインでは実行または設定できません。 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、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。 このチェックボックスをオンにすると、Kaspersky Security Center で作成されたタスクが本製品のグラフィカルインターフェイスに表示されます。ユーザーは、本製品のグラフィカルインターフェイスおよびコマンドラインからこれらのタスクを開始および停止できます。 このチェックボックスをオフにすると、Kaspersky Security Center で作成されたタスクは、本製品のグラフィカルインターフェイスまたはコマンドラインで表示または管理できなくなります。 既定では、このチェックボックスはオフです。

バッテリー駆動時のタスクのキャンセル

バッテリー電源で実行しているときに、スケジュールされたタスクのキャンセルを有効または無効にすることができます。スケジュールされたタスクをキャンセルすると、リソースの消費量が削減され、バッテリー寿命が延びます。

スケジュールされたタスクのキャンセルが有効になっていて、デバイスがバッテリー電源で動作している場合、Kaspersky Endpoint Security は次のスケジュールされたタスクをキャンセルします：

- すべてのスキャンタスク（オブジェクトスキャン、カスタムコンテナスキャン、簡易スキャン、マルウェアのスキャン）
- インベントリ
- 定義データベースと機能のアップデート
- IOC スキャン
- システム整合性チェック

必要に応じてタスクを手動で実行できます。

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 → Performance**）で、スケジュールされたタスクのキャンセルを設定できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（[**全般設定**] → [**製品設定**]、[**パフォーマンス**]）で、スケジュールされたタスクのキャンセルを管理できます。

[**バッテリー駆動時にスケジュールされたタスクをスキップする**]チェックボックスは、スケジュールされたタスクのキャンセル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。

このチェックボックスをオフにすると、デバイスがバッテリー電源で動作しているかどうかに関係なく、すべてのタスクがスケジュールどおりに実行されます。

コマンドラインでの設定

全般設定の `PowerSaveMode` 設定を使用して、コマンドラインでスケジュールされたタスクのキャンセルを設定できます。

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。

[`PowerSaveMode`]パラメータが取り得る値は、次のとおりです：

- `Yes`（既定値）の場合、デバイスがバッテリ電源で動作しているときにスケジュールされたタスクをスキップします。
- `No` は、デバイスがバッテリー電源で動作しているかどうかに関係なく、スケジュールされたタスクを実行します。

システムイベントインターセプターの設定

本製品が適切に機能するには、システムイベント、つまりファイル操作とプロセスの開始を読み取る必要があります。本製品がシステムイベントインターセプターを使用しない場合、リアルタイムスキャンは実行されず、デバイスの保護レベルが低下します。

デバイスの OS が fanotify に対応している場合は、本製品がシステムイベントを読み取るために使用するメカニズムを選択できます。

- fanotify に基づくシステムインターセプターメカニズム。このメカニズムは既定で使用されます。
- *アップデート可能なカーネルモジュール*に基づくインターセプターメカニズム。アップデート可能なカーネルモジュールを使用すると、Kaspersky Endpoint Security によるファイル操作および起動プロセスの傍受を最適化できます。更新可能なカーネルモジュールは、ファイルが開かれたり、名前が変更されたり、ファイルに変更を加えられたときにファイル操作を傍受します。スキャンする必要のないファイルとプロセスのキャッシュを使用することで、本製品のパフォーマンスが向上します。

更新可能なカーネルモジュールを使用することで、グローバル除外リストをより細かく設定できます。fanotify テクノロジに基づくインターセプトメカニズムを使用している場合、指定されたマウントポイント全体が、ファイル操作のインターセプトから除外されます。更新可能なカーネルモジュールを使用すると、デバイスにマウントされた特定のローカルディレクトリまたはリモートディレクトリを除外できます。

アップデート可能なカーネルモジュールは、本製品の配布キットに含まれています。

fanotify に対応していない OS では、インターセプターメカニズムを選択することはできません。本製品は特別なカーネルモジュールを使用してシステムイベントを読み取り、ファイル脅威対策を提供します。すべての依存関係とビルドツールが利用可能であれば、ファイル脅威対策の起動時にこのモジュールは自動的にコンパイルされます。

OS がアップデート可能なカーネルモジュールのインストール要件を満たしている場合、本製品はアップデート可能なカーネルモジュールに基づくインターセプターメカニズムを使用できます。

更新可能なカーネルモジュールのインストール要件

アップデート可能なカーネルモジュールをインストールして使用するには、デバイスに次のいずれかの 64 ビット OS がインストールされている必要があります。

- 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.10015-01 (operational update 1.8)

  Kaspersky Endpoint Security を基本モードで使用する場合、更新可能なカーネルモジュールは、Astra Linux オペレーティングシステムを搭載したデバイスの閉鎖ソフトウェア環境モードで使用できます。

- CentOS 7.x
- CentOS Stream 8
- Debian GNU/Linux 12.0
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 8.10
- SberLinux 8.10
- SberLinux 9.1
- SberLinux 9.6
- SberLinux 9.7
- SberOS 3.4
- SberOS 3.5
- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS

- ALT SP Workstation リリース 10
- ALT SP Server リリース 10
- ALT Education 10
- ALT Workstation リリース 11
- ALT Server リリース 11
- ALT Education 11
- RED OS 7.3
- RED OS 8
- ROSA「Cobalt」7.9 ワークステーション
- ROSA「Cobalt」7.9 サーバー
- ROSA「Chrome」12 ワークステーション
- ROSA "Chrome" 12 サーバー

32 ビット OS および Arm アーキテクチャの OS には対応していません。

アップデート可能なカーネルモジュールは、一部の Linux カーネルバージョンおよび一部のサードパーティアプリケーションと競合する可能性があります。

Kaspersky ULKM ツールを使用して、デバイスがアップデート可能なカーネルモジュールのインストール要件を満たしているかどうかを確認できます。

オペレーティングシステムが要件を満たしている場合は、更新可能なカーネルモジュールに基づく読み取り方法を、本製品のインストール中に選択できます。これにより、更新可能なカーネルモジュールがインストールされます。また、使用しているオペレーティングシステムがサポート対象になった場合は、更新可能なカーネルモジュールを後からインストールすることも可能です。次の手順に従います：

1. 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更新可能なカーネルモジュールは、通常のアップデート手順の一環としてインストールされます。
2. 更新可能なカーネルモジュールに基づいてインターセプターのメカニズムを選択します。**Web コンソール**、管理コンソール、または**コマンドライン**から、システムイベントインターセプターのメカニズムを選択できます。

   コマンドラインでは、`InterceptorMode`、`InterceptorFallbackStrategy`、および `InterceptorApplyStrategy` の全般設定を使用して、システムイベントインターセプターを設定できます。

   設定は、オペレーティングシステムが fanotify 技術に対応しているデバイスでのみ表示され、編集が可能です。

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。

`InterceptorMode` を使用すると、本製品で使用されるシステムイベントインターセプターメカニズムを選択できます。この設定は次の値を使用できます：

- `UseFanotify` fanotify テクノロジーを使用してシステムイベントをインターセプトします。
- `UseUpdatableKernelModule` – 更新可能なカーネルモジュールを使用してシステムイベントを遮断します。

アップデート可能なカーネルモジュールを選択した場合、`InterceptorFallbackStrategy` 設定が適用されます。この設定では、アップデート可能なカーネルモジュールの起動に失敗した場合の本製品の動作を指定できます。この設定は次の値を使用できます：

- `FallbackToFanotify` は、アップデート可能なカーネルモジュールの起動に失敗した場合に備えて、システムイベントインターセプターメカニズムを fanotify に切り替えます。
- `FallbackToLimitedMode` は、アップデート可能なカーネルモジュールの起動に失敗した場合に備えて、システムイベントインターセプターをオフにします。本製品がシステムイベントインターセプターを使用しない場合、リアルタイムスキャンは実行されず、デバイスの保護レベルが低下します。

アップデート可能なカーネルモジュールを選択した場合、`InterceptorApplyStrategy` 設定が適用されます。本製品がアップデート可能なカーネルモジュールの使用に切り替えた場合、モジュールを起動するには本製品を再起動する必要があります。この設定では、本製品を自動的に再起動するか、手動で再起動するかを指定できます。

- `RestartServiceAutomatically` は、アップデート可能なカーネルモジュールを起動するために本製品を自動的に再起動します。
- `RestartServiceManually` は、ユーザーが本製品を手動で再起動した後に、アップデート可能なカーネルモジュールを起動します。

更新可能なカーネルモジュールの使用に切り替えるには、本製品を自動的に再起動することを推奨します。本製品を再起動した後、更新可能なカーネルモジュールを手動で起動すると、アプリケーションエラーが発生する可能性があります。

Web コンソールでは、ポリシープロパティ（**製品設定 → 全般設定設定 → OS 連携設定**）でシステムイベント遮断を設定できます。

この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。

本製品は、次の状況で更新可能なカーネルモジュールの使用に切り替えることができます：

- 製品設定で、システムイベントを傍受するメカニズムを更新可能なカーネルモジュールに変更しました。
- 更新可能なカーネルモジュールが起動されていないデバイスでは、定義データベースとモジュールの更新によって、更新可能なカーネルモジュールに対応するアップデートが導入されました。

本製品が正しく動作するには、本製品が自動的に再起動された後に、更新可能なカーネルモジュールの使用への切り替えを実行する必要があります。

更新可能なカーネルモジュールに基づく傍受メカニズムを選択した場合は、更新可能なカーネルモジュールの起動時にエラーが発生し、モジュールが起動しない場合の動作を設定できます。この場合、本製品はfanotifyにフォールバックするか、システムイベントの読み取りを無効にすることができます。

デバイス上のアップデート可能なカーネルモジュールのステータスと可用性に関する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、**更新可能なカーネルモジュール**機能コンポーネントのステータスを確認します。
- コマンドラインで、`kesl-control --app-info` コマンドの出力に表示されます。

更新可能なカーネルモジュールの状態に関する情報は、次のステータスとして表示されます：

- **実行中**は、モジュールがインストールされ、実行されていることを意味します。
- **停止**は、モジュールがインストールされているが実行されていないことを意味します。
- **使用不可**は、モジュールがデバイスに対応していないことを意味します。
- **誤動作**は、モジュールの起動中にエラーが発生し、モジュールが実行されていないことを意味します。

アップデート可能なカーネルモジュールをインストールできるかどうかの確認

Kaspersky ULKM ツールを使用して、デバイスがアップデート可能なカーネルモジュールのインストール要件を満たしているかどうかを確認できます。

Kaspersky Security Center Web コンソールまたは管理コンソールを使用してこのツールを実行する方法

1. ulkmtool.zip アーカイブを、**Kaspersky Endpoint Security for Linux** セクションの本製品のダウンロードページからダウンロードします。
2. ユーティリティのインストールパッケージを作成します。

   Web コンソールでのインストールパッケージの作成

   1. ダウンロードした ulkmtool.zip 圧縮ファイルを、Kaspersky Security Center 管理サーバーがアクセスできるフォルダーに配置します。
   2. 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。
   3. ［**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。
   4. インストールパッケージの作成方法として、「**ファイルからインストールパッケージを作成する**」を選択します。

5. 新しいインストールパッケージの名前を入力し、［**参照**］をクリックして、ダウンロードした ulkmtool.zip 圧縮ファイルへのパスを指定します。

6. ウィザードを終了します。

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。

管理コンソールでのインストールパッケージの作成

1. アーカイブ ulkmtool.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。

2. 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。
   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。

3. ［**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。

4. **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**ボタンをクリックします。

5. 新しいインストールパッケージの名前を指定して、ウィザードの次のステップに進みます。

6. ［**参照**］をクリックし、ファイル ulkmtool.kud へのパスを指定します。このファイルはアーカイブ ulkmtool.zip を解凍したフォルダーにあります。
   ウィザードの次のステップに進みます。

7. ファイルダウンローダーが完了するまで待ってからウィザードを終了します。

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。

3. 更新可能なカーネルモジュールの要件を満たしているかどうかをチェックするデバイスに、 Kaspersky Security Center 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

   1. Linux デバイスをネットワークエージェントのインストール用に準備します。手順は OS によって異なります。

   2. ネットワークエージェントのインストールと初期設定を実行します。手順については、Kaspersky Security Center のヘルプ を参照してください。

4. Kaspersky Security Center Web コンソールまたは管理コンソールで、更新可能なカーネルモジュールの要件を満たしているかどうかをチェックするデバイスを対象としたリモートインストールタスクを作成して、実行します。タスク設定で、作成したインストールパッケージを選択します。
   リモートインストールの手順については、『Kaspersky Security Center のヘルプ』を参照してください。
   各デバイスのタスク結果は、デバイスがアップデート可能なカーネルモジュールのインストールと操作に対応しているかどうかを示します。

タスクのタスク結果に基づいて、各デバイスにタグが付けられます。

- *UpdatableKernelModule=No* は、デバイスがアップデート可能なカーネルモジュールのインストールに対応していないことを意味します。

- *UpdatableKernelModule=Yes* は、デバイスがアップデート可能なカーネルモジュールをインストールして実行するための要件を満たしていることを意味します。

- *UpdatableKernelModule=Use* は、更新可能なカーネルモジュールがデバイスにインストールされていて、稼働していることを意味します。

- *UpdatableKernelModule=Error* は、更新可能なカーネルモジュールがデバイスにインストールされているが、モジュールの起動時にエラーが発生し、モジュールが実行されていないことを意味します。

これらのタグを使用してデバイス選択を作成できます。たとえば、アップデート可能なカーネルモジュールの要件を満たすデバイスを選択し、これらのデバイスにアップデート可能なカーネルモジュールを含むKaspersky Endpoint Security をインストールできます。

更新可能なカーネルモジュールを使用する場合の「セーフ」モード

更新可能なカーネルモジュールを使用しているときに本製品が不安定になった場合、指定された最大異常停止回数に達すると、自動的に「セーフ」モードに切り替わります（kesl.ini 設定情報ファイルで `SafeMode=yes` が設定されます）。既定では、本製品は異常停止が 3 回発生すると「セーフ」モードに入ります。異常停止の最大回数は、kesl.ini 設定情報ファイルの `PanicThreshold` 設定で設定されます。

本製品が「セーフ」モードで実行されている場合、更新可能なカーネルモジュールは起動せず、システムイベントを読み取るために fanotify に切り替わります。本製品は、`UpdatableKernelModule=Error` タグを Kaspersky Security Center に送信します。

本製品のトラブルを解決した後も更新可能なカーネルモジュールを引き続き使用するには、「セーフ」モードを無効にする必要があります。

本製品の「セーフ」モードを無効にする場合：

1. ファイル /var/opt/kaspersky/kesl/common/kesl.ini を開いて編集します。
2. `[General]` セクションで、`SafeMode=no` を設定します。
3. Kaspersky Endpoint Security を再起動します：

   ```
   systemctl restart kesl
   ```

Web コンソールでの読み取り設定の管理

Web コンソールでは、ポリシープロパティ（**製品設定 → 全般設定設定 → OS 連携設定**）でシステムイベント遮断を設定できます。

この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。

管理コンソールでの読み取り設定の管理

管理コンソールでは、ポリシーのプロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（[**全般設定**] → [**OS との連携設定**]、[**システムイベント遮断設定**]）で、システムイベント遮断設定を管理できます。

この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。

システムイベントインターセプターの設定

設定	説明
インターセプターメカニズム	本製品で使用されるシステムイベントインターセプターメカニズム： • **Fanotify テクノロジー**（既定）。このオプションを選択すると、本製品はシステムイベントインターセプターのために fanotify テクノロジーを使用します。 • **アップデート可能なカーネルモジュール**。このオプションを選択すると、本製品はシステムイベントインターセプターのためにアップデート可能なカーネルモジュールを使用します。
アップデート可能なカーネルモジュールが起動に失敗した場合	アップデート可能なカーネルモジュールの起動に失敗した場合のアプリケーションの処理： • **fanotify を使用**（既定）。このオプションを選択すると、本製品はシステムイベントインターセプターのために fanotify テクノロジーに切り替わります。 • **システムイベントインターセプターを無効にする**。本製品がシステムイベントインターセプターを使用しない場合、リアルタイムスキャンは実行されず、デバイスの保護レベルが低下します。 このオプションは、**アップデート可能なカーネルモジュール**インターセプターメカニズ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読み取り設定の管理

コマンドラインでは、`InterceptorMode`、`InterceptorFallbackStrategy`、および `InterceptorApplyStrategy` の全般設定を使用して、システムイベントインターセプターを設定できます。

設定は、オペレーティングシステムが fanotify 技術に対応しているデバイスでのみ表示され、編集が可能です。

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。

`InterceptorMode` を使用すると、本製品で使用されるシステムイベントインターセプターメカニズムを選択できます。この設定は次の値を使用できます：

- `UseFanotify` fanotify テクノロジーを使用してシステムイベントをインターセプトします。
- `UseUpdatableKernelModule` – 更新可能なカーネルモジュールを使用してシステムイベントを遮断します。

アップデート可能なカーネルモジュールを選択した場合、`InterceptorFallbackStrategy` 設定が適用されます。この設定では、アップデート可能なカーネルモジュールの起動に失敗した場合の本製品の動作を指定できます。この設定は次の値を使用できます：

- `FallbackToFanotify` は、アップデート可能なカーネルモジュールの起動に失敗した場合に備えて、システムイベントインターセプターメカニズムを fanotify に切り替えます。
- `FallbackToLimitedMode` は、アップデート可能なカーネルモジュールの起動に失敗した場合に備えて、システムイベントインターセプターをオフにします。本製品がシステムイベントインターセプターを使用しない場合、リアルタイムスキャンは実行されず、デバイスの保護レベルが低下します。

アップデート可能なカーネルモジュールを選択した場合、`InterceptorApplyStrategy` 設定が適用されます。本製品がアップデート可能なカーネルモジュールの使用に切り替えた場合、モジュールを起動するには本製品を再起動する必要があります。この設定では、本製品を自動的に再起動するか、手動で再起動するかを指定できます。

- `RestartServiceAutomatically` は、アップデート可能なカーネルモジュールを起動するために本製品を自動的に再起動します。
- `RestartServiceManually`は、ユーザーが本製品を手動で再起動した後に、アップデート可能なカーネルモジュールを起動します。

更新可能なカーネルモジュールの使用に切り替えるには、本製品を自動的に再起動することを推奨します。本製品を再起動した後、更新可能なカーネルモジュールを手動で起動すると、アプリケーションエラーが発生する可能性があります。

テレメトリの詳細設定の管理

Detection and Response ソリューションと連携されている場合、それらのソリューションに送信されるテレメトリの収集に関する次の詳細設定を管理できます：

- テレメトリソース。テレメトリを取得するには、eBPF テクノロジーと auditd サービスを使用することも、eBPF テクノロジーのみを使用することもできます。
- auditd サービスのモード。Kaspersky Endpoint Security は、排他モードまたはマルチキャストモードで auditd サービスを使用できます。

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 → OS 連携設定**）で詳細テレメトリ設定を管理できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）で追加のテレメトリ設定を管理できます（**全般設定 →OS 連携設定**、**テレメトリの追加設定**）。

テレメトリの詳細設定

設定	説明
テレメトリソース	Kaspersky Endpoint Security がテレメトリを収集するために使用するソース： • **eBPF のみを使用する**ということは、テレメトリの取得に eBPF 技術のみが使用されることを意味します。 • **eBPF と auditd**（既定）を使用するということは、テレメトリを収集するために eBPF技術 と auditd サービスが使用されることを意味します。
auditd の使用	auditd サービスのモード： • **AuditD を排他モードで使用する**（既定）は、Kaspersky Endpoint Security が auditd サービスを排他モードで使用することを意味します。 • **非排他モード**とは、auditd サービスが非排他モードで使用されることを意味します。 この設定は、**テレメトリソース**が **eBPF と auditd を使用する**ように設定されている場合にのみ適用されます。

コマンドラインでの設定

コマンドラインでは、Behavior Detection 事前定義済みタスクの `TelemetrySource` および `UseTelemetryMonopolyMode` 設定を使用して、テレメトリの追加設定を管理できます。

`kesl-control --set-settings 20` コマンドを使用するか、タスクのすべての設定が含まれている設定情報ファイルを編集するか、**< 設定名 >=< 設定値 >** 形式のコマンドラインオプションを使用して、設定を変更できます。

`TelemetrySource` 設定では、テレメトリソースを指定できます。この設定は次の値を使用できます：

- `Default`（既定）は、テレメトリを収集するために eBPF 技術と auditd サービスが使用されることを意味します。
- `OnlyEBPF` は、テレメトリの収集に eBPF 技術のみが使用されることを意味します。

`UseTelemetryMonopolyMode` 設定では、テレメトリの取得に auditd サービスを使用する場合の auditd サービスの使用モードを指定できます。この設定は次の値を使用できます：

- `True`（既定）は、Kaspersky Endpoint Security が auditd サービスを排他モードで使用することを意味します。
- `False` は、auditd サービスが非排他モードで使用されることを意味します。

`UseTelemetryMonopolyMode` 設定は、`TelemetrySource` が `Default` に設定されている場合にのみ適用されます。

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。

既定では、ディレクトリ /var/opt/kaspersky/kesl/common/objects-backup/ がファイルのバックアップコピーの保存に使用されます。このディレクトリには隔離されたファイルも保存されます。コマンドラインを使用して、バックアップおよび隔離オブジェクトを保存するディレクトリを変更できます。

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、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、バックアップコピーからファイルの復元を試行できます。

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。

Web コンソールまたは管理コンソールのポリシーを使用するか、コマンドラインを使用して、バックアップ設定をデバイスで指定できます。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 30 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。

バックアップおよび隔離オブジェクトが保存されるディレクトリへのパス（コマンドラインでのみ設定できます）。

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古いバックアップコピーから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 → リポジトリ → バックアップ**）および Web コンソール（**動作 → リポジトリ → バックアップ**）で利用できます。保護されたデバイスのバックアップストレージ内のファイルのプロパティを表示したり、そこから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。

ファイルは、指定された設定に従ってバックアップから元の場所に復元されます。復元では、MAC ラベル（Astra Linux デバイスのみ）と元のファイルの属性（不変属性と追加専用属性以外）が維持されます。

Astra Linux デバイスでは、次の場合にバックアップからのファイルの復元がエラーで終了します。

- ファイルの MAC ラベルが、ファイルの復元先ディレクトリのMAC ラベルよりも高い場合。
- ファイルの MAC ラベルが、ファイルの復元先のディレクトリの MAC ラベルよりも低く、ディレクトリに ccnr フラグが設定されていない。

Kaspersky Security Center でバックアップ内のファイルを管理するには、バックアップ内のファイルに関するデータを管理サーバーに転送できるようにする必要があります。

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（**アプリケーション設定 → 全般設定 → レポートと保管領域**）および管理対象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** → <device name> リンク → **アプリケーション**タブ → <Kaspersky Endpoint Security application name> リンク → **アプリケーション設定**タブ → **ストレージ設定**セクション）で、バックアップ設定を管理できます。

Web コンソール内ポリシープロパティのバックアップ設定については、付録 5 で説明しています。

管理対象デバイスのプロパティのバックアップ設定については、次の表で説明します。

デバイスプロパティのバックアップ設定で操作

設定	説明
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：1～10000。チェックボックスをオフにすると、バックアップにオブジェクトを保存する期間は無制限になります。 既定値：30
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。 チェックボックスをオフにすると、バックアップのサイズは無制限になります。 既定値：1024

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定 → ストレージ設定**）と管理対象デバイスのプロパティ（**管理対象デバイス → デバイス**タブ → デバイスのプロパティウィンドウ → **アプリケーション**セクション → アプリケーションのプロパティウィンドウ → **ストレージ設定**）で、隔離設定を管理できます。

バックアップ設定

設定	説明
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：0～10000。 0 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。 既定値：30
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：1～999999。チェックボックスをオフにすると、バックアップのサイズは無制限になります。 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バックアップ設定の構成

コマンドラインでは、製品の全般設定の `BackupDaysToLive,`、`BackupSizeLimit`、および `QuarantineBackupFolder` 設定を使用してバックアップ設定を構成できます。

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。

バックアップ設定

設定	説明	値
`BackupDaysToLive`	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）。指定された時間が経過すると、アプリケーションはファイルの最も古いバックアップコピーを削除します。 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 から 10000 0–無制限の保持。 既定値：30
`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、最も古いファイルのバックアップコピーが削除されます。 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 から 999999 0–無制限のサイズ。 既定値：0
`QuarantineBackupFolder`	バックアップおよび隔離オブジェクトが保存されるディレクトリへのパス。既定のディレクトリとは異なるディレクトリを指定できます。バックアップおよび隔離オブジェクトを保存するディレクトリとして、任意のデバイス上のディレクトリを使用できます。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。 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>**には、クエリ結果を制限するために、and 論理演算子を使用して結合された、**<フィールド> <比較演算> '<値>'** 形式の1つ以上の 論理式を指定します。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>**には、ストレージ内の最新のオブジェクトのうち表示する数を指定します。`-n` オプションを指定しない場合、本製品は直近の 30 個のオブジェクトに関する情報を表示します。すべてのオブジェクトに関する情報を表示する場合は、`0` を指定します。
- `--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 -B --restore <オブジェクト ID>
```

ここで、**<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本製品がその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 -B --restore <オブジェクト ID> --file <ファイルパス>
```

ここで、`--file` **<ファイルパス>**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。

閉鎖ソフトウェア環境モードの Astra Linux デバイスでは、バックアップにファイルを配置したときと同じアカウントでのみ、ファイルを復元できます。

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 -B --mass-remove --query "< フィルター条件 >"
```

< フィルター条件 > は、結果を制限するために、論理演算子 **and** を使用して結合された、**< フィールド > < 比較演算子 > '< 値 >'** 形式の1つ以上の 論理式です。

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

Kaspersky Detection and Response ソリューションは、組織インフラの様々なレベルで高度な脅威や攻撃の兆候を検出するための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：

- Open Single Management Platform (OSMP) 上の Kaspersky Endpoint Detection and Response Expert（オンプレミス）。連携は、Kaspersky Endpoint Security 製品コンポーネント、Endpoint Detection and Response Expert（オンプレミス）（以下「*EDR Expert（オンプレミス）*」とも表記）によって提供されます。
- Kaspersky Anti Targeted Attack Platform 上の Kaspersky Endpoint Detection and Response および Kaspersky Network Detection and Response コンポーネント。連携は、Kaspersky Endpoint Security の次のコンポーネントによって提供されます：
  - Endpoint Detection and Response Expert（オンプレミス）（以下「*EDR Expert（オンプレミス）*」とも表記）。
  - Network Detection and Response (KATA)（以下、*NDR (KATA)* とも表記）。
- Open Single Management Platform (OSMP) または Kaspersky Anti Targeted Attack Platform 上のサンドボックス。連携は、次の Kaspersky Endpoint Security コンポーネントによって提供されます：*サンドボックス*。
- Kaspersky Unified Monitoring and Analysis Platform。
- 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 を Endpoint Detection and Response Agent モードで使用する場合、Open Single Management Platform (OSMP) 上の Kaspersky Endpoint Detection and Response Expert（オンプレミス）、および Kaspersky Anti Targeted Attack Platform 上の Kaspersky Endpoint Detection and Response と Kaspersky Network Detection and Response コンポーネントとの連携のみに対応しています。

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
```

SintezM-Client OS では、既定で 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。

Kaspersky Endpoint Security for Linux がインストールされたイメージから作成された仮想マシンでは、Detection and Response ソリューションが正しく動作しない場合があります。Detection and Response ソリューションと連携する際には、コンピューターの一意の ID（Sensor ID）が使用されます。アプリケーションは初回インストール時にこの ID を生成し、この ID はアプリケーションのアンインストール後も保持されます。イメージをクローンすると、仮想マシンはSensor IDを継承します。これにより、Detection and Response ソリューションが複数の仮想マシンを同じデバイスとして識別する可能性があります。

MDR と正しく統合するための参照イメージの作成に関する推奨事項

EDR Expert（オンプレミス）と正しく連携するための参照イメージを準備する方法

Detection and Response ソリューションからのコマンドに基づく脅威対応処理について

Detection and Response ソリューションと連携すると、Kaspersky Endpoint Security はセキュリティ機能を維持するための脅威対応を実行できます。Detection and Response ソリューションの設定でこの機能が有効になっている場合、Detection and Response ソリューション側で脅威対応を生成し、Kaspersky Endpoint Security デバイスで自動的に実行することができます。脅威対応を手動で設定して実行することもできます。

脅威対応の設定は、Kaspersky Endpoint Security が連携されている Detection and Response ソリューションによって異なります。

Kaspersky Endpoint Security は次の脅威対応を実行できます：

- デバイスをネットワークから分離。

  Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Endpoint Detection and Response (KATA) または Kaspersky Managed Detection and Response と連携されている場合、検出および応答ソリューション側でネットワーク分離が有効または無効になります。デバイスのネットワーク分離を手動で無効化できます。

  Kaspersky Endpoint Detection and Response Optimum と連携すると、デバイスを自動または手動でネットワークから分離できます。ネットワーク分離を設定したり、デバイスのネットワーク分離を手動で無効にしたりすることができます。

- ファイルの隔離。

  この処理は、*ファイルの隔離*タスクを使用して実行されます。

  Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Endpoint Detection and Response (KATA) または Kaspersky Managed Detection and Response と連携されている場合、検出および応答ソリューション側でタスクが作成され、実行されます。

  Kaspersky Endpoint Detection and Response Optimum と連携すると、セキュリティ侵害インジケーターが検知され、ファイルが自動的に隔離されます。

Kaspersky Endpoint Detection and Response Optimum または Kaspersky Managed Detection and Response と連携すると、ファイルを手動で隔離することもできます。

- 隔離からファイルを復元します。

  Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Endpoint Detection and Response (KATA) または Kaspersky Managed Detection and Response と連携されている場合、検出および応答ソリューション側で脅威対応処理が生成されます。Kaspersky Security Center またはコマンドラインを使用して、手動で処理を実行することもできます。

  Kaspersky Endpoint Detection and Response Optimum と連携すると、Kaspersky Security Center またはコマンドラインを使用して手動で処理を実行できます。

- 隔離からファイルを削除。

  Kaspersky Endpoint Detection and Response（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) と連携すると、外とする Detection and Response ソリューション側で脅威対応が生成されます。Kaspersky Security Center またはコマンドラインを使用して、手動で処理を実行することもできます。

  Kaspersky Endpoint Detection and Response Optimum と連携すると、Kaspersky Security Center またはコマンドラインを使用して手動で処理を実行できます。

- 隔離からファイルを取得。

  Kaspersky Endpoint Detection and Response（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) と連携すると、外とする Detection and Response ソリューション側で脅威対応が生成されます。

  Kaspersky Endpoint Detection and Response Optimum と連携すると、 Kaspersky Security Centerを使用して手動で処理を実行できます。

- デバイスからファイルを取得。

  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取得するようにアプリケーションを設定できます。

  Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Endpoint Detection and Response (KATA) または Kaspersky Managed Detection and Response と連携されている場合、検出および応答ソリューション側でタスクが作成され、実行されます。

  Kaspersky Endpoint Detection and Response Optimum ソリューションと連携する場合、Web コンソールでファイル取得タスクを設定できます。

- デバイスからファイルを削除。

  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。

  Kaspersky Endpoint Detection and Response（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) と連携すると、タスクは検出および応答ソリューション側で作成され、実行されます。

  Kaspersky Endpoint Detection and Response Optimum ソリューションと連携する場合、Web コンソールでファイル削除タスクを作成できます。

- 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、*アプリケーションの実行*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*] タスクを使用して作成されたファイルを取得できます。

  Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Endpoint Detection and Response (KATA) または Kaspersky Managed Detection and Response と連携されている場合、検出および応答ソリューション側でタスクが作成され、実行されます。

  Kaspersky Endpoint Detection and Response Optimum ソリューションと連携する場合、Web コンソールで実行プロセスタスクを作成および実行できます。

- 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、*プロセスの強制終了*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。

  Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Endpoint Detection and Response (KATA) または Kaspersky Managed Detection and Response と連携されている場合、検出および応答ソリューション側でタスクが作成され、実行されます。

  Kaspersky Endpoint Detection and Response Optimum ソリューションと連携する場合、Web コンソールでプロセスの強制終了タスクを作成および実行できます。

- デバイス上での*セキュリティ侵害インジケーター (IOC)* の検知。*侵害の兆候（IOC）*は、デバイスへの不正アクセス（侵害されたデータ）を示すオブジェクトまたは処理に関する一連のデータです。たとえば、ログイン試行の失敗回数が多い場合、侵害の兆候が考えられます。

  Kaspersky Endpoint Detection and Response（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) と連携すると、Kaspersky Endpoint Security デバイス上のIOC スキャンタスクは検出および応答ソリューション側で作成され、実行されます。

  Kaspersky Endpoint Detection and Response Optimum と連携している場合、IOC スキャンは *IOC* スキャンタスクを使用して実行されます。IOC スキャンタスクを手動で作成できます。

- *YARA* スキャンの開始。*YARA* スキャンでは、Kaspersky Endpoint Security は YARA ファイルを使用して、デバイス上の悪意のある活動のシグネチャを検索します。*YARA ファイル*は、YARA ルールを含む YARA または YAR 拡張子を持つファイルです。*YARA ルール*は、標的型攻撃と企業の IT インフラストラクチャへの侵入のシグネチャを記述します。Kaspersky Endpoint Security はこれらのルールを使用してオブジェクトをスキャンします。ルールの条件が満たされると、アナライザーは感染が進行中であると判断し、詳細をログに記録します。スキャンする処理はローカルドライブ上で再帰的に実行されます。ネットワーク、リムーバブル、クラウドリソースのスキャンには対応していません。

  Kaspersky Endpoint Security デバイスでの YARA スキャンのコマンドは、Kaspersky Endpoint Detection and Response Expert（オンプレミス）ソリューション側で作成され、実行されます。

- 実行防止

  Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Endpoint Detection and Response (KATA)、または Kaspersky Endpoint Detection and Response Optimum と連携すると、実行防止ルールを有効にすることができます。Kaspersky Endpoint Security は、実行防止ルールの基準に一致するオブジェクトの実行やドキュメントの開封を防止します。

  Kaspersky Endpoint Detection and Response Expert（オンプレミス）またはKaspersky Endpoint Detection and Response (KATA) と連携すると、本製品は Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) から実行防止ルールを受け取ります。

  Kaspersky Endpoint Detection and Response Optimum と連携すると、Web コンソールで実行防止ルールを設定できます。

- フォレンジックの取得。

  Kaspersky Endpoint Detection and Response Expert（オンプレミス）と連携するときは、サイバー犯罪およびデータ流出に関連するインシデントの調査に役立つ可能性のあるデジタルデータを収集できます。

  この処理は、以下のタスクを使用して実行できます。

  - *フォレンジックの取得*タスクでは、次のような情報を収集します：
    - ファイルのリスト
    - プロセスのリスト
    - 自動実行ポイントのリスト
  - *メモリダンプの取得タスク*

- *プロセスメモリダンプの取得タスク*
- *ディスクイメージの取得タスク*

タスクは、Endpoint Detection and Response Expert（オンプレミス）ソリューション側で作成され、実行されます。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携

Kaspersky Endpoint Detection and Response Expert（オンプレミス）は、ほとんどのサイバーセキュリティリスクから防御し、脅威拡散の主なシナリオを網羅できるエンタープライズサイバーセキュリティソリューションです。Open Single Management Platform (OSMP) 上で Kaspersky Endpoint Detection and Response Expert（オンプレミス）のコンポーネントを導入します。ソリューションとプラットフォームの詳細については、「Kaspersky Endpoint Detection and Response Expert（オンプレミス）のヘルプ」を参照してください。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）と連携している場合、Kaspersky Endpoint Security では次の操作が可能です：

- デバイス上のイベントに関するデータ（テレメトリ）を、OSMP プラットフォーム上のテレメトリサーバー（以降、「*OSMP テレメトリサーバー*」とも表記）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、テレメトリ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。
- OSMP 脅威対応サーバー（以降、「OSMP 脅威対応サーバー」とも表記）から受信したコマンドに基づいて、セキュリティ機能の維持を目的とした*脅威対応処理*を実行します。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）ソリューションとの連携は、Kaspersky Endpoint Security アプリケーションコンポーネントである Endpoint Detection and Response Expert（オンプレミス）（以降、*EDR Expert（オンプレミス）*とも表記）によって提供されます。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）と連携する場合、Kaspersky Endpoint Security を実行しているデバイスは、OSMP 脅威対応サーバーおよび OSMP テレメトリサーバーとの暗号化された HTTPS 接続を確立します。安全な接続を実現するため、OSMP サーバーが発行する次の証明書を使用しています：

- 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。そのためには、Kaspersky Endpoint Detection and Response Expert（オンプレミス）ソリューションとの連携を有効にする前に、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、相互認証を使用した追加の接続保護に使用されます（つまり、OSMP サーバーは Kaspersky Endpoint Security を搭載したデバイスを認証します）。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、サーバはクライアント証明書を検証しませんが、Kaspersky Endpoint Detection and Response Expert（オンプレミス）側で相互認証を有効にすることができます。この場合、EDR Expert（オンプレミス）コンポーネントの設定で相互認証を有効にし、クライアント証明書（証明書および秘密鍵を含む暗号コンテナ）を追加する必要があります。

OSMP サーバーとの接続を保護するための証明書は、OSMP プラットフォームの管理者が提供する必要があります。

Kaspersky Endpoint Security の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、OSMP サーバーへの接続にはプロキシサーバーが使用されます。

Endpoint Detection and Response Expert（オンプレミス）機能を使用するには、EDR Expert（オンプレミス）コンポーネントを有効にする必要があります。Kaspersky Endpoint Security を使用しているメインライセンスに Kaspersky Endpoint Detection and Response Expert（オンプレミス）機能が含まれていない場合は、この機能用の別のライセンスを購入し、EDR Expert（オンプレミス）ライセンスを本製品に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、SVM にライセンスを追加することで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。

Endpoint Detection and Response Expert（オンプレミス）との連携は、次の手順で行います：

1. **Kaspersky Endpoint Security の必須コンポーネントの有効化**

   EDR Expert（オンプレミス）コンポーネントは、次のコンポーネントの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
   - アンチクリプター。
   - 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

   Kaspersky Endpoint Security を Kaspersky Endpoint Detection and Response Expert（オンプレミス）と完全に連携させるには、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。ふるまい検知が無効になっている場合、必要なテレメトリは送信されません（同期要求と他の保護コンポーネントからの脅威検知データは例外）。

   ふるまい検知が eBPF メカニズムを使用してシステムテレメトリを取得する場合（eBPF に対応するカーネルバージョン 4.18 以降の 64 ビットオペレーティングシステムで利用可能）、テレメトリデータはより包括的になります。

2. **EDR Expert (オンプレミス) コンポーネントのアクティベートする**

   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 Expert（オンプレミス）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 Expert（オンプレミス）を使用するための別のライセンスを購入し、EDR Expert（オンプレミス）ライセンスをアプリケーションに追加しました。

     仮想環境を保護するために Kaspersky Endpoint Security を Light Agent モードで使用している場合は、追加機能をアクティベートするためのライセンスを SVM に現在のライセンスとして追加する必要があります。

3. **EDR Expert（オンプレミス）コンポーネントの有効化**

   Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携は既定では無効です。連携を有効にするには、EDR Expert（オンプレミス）コンポーネントを有効にして設定する必要があります。

   - Kaspersky Security Center Web コンソールを使用します。
   - コマンドラインを使用する。

   > Kaspersky Security Center の管理コンソールでは、Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携の設定には対応していません。

   > Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携を行うには、EDR Expert（オンプレミス）コンポーネントの設定で*EDR Expert（OSMP）*連携モードを選択する必要があります。Web コンソールを使用している場合は、ポリシー設定で **Endpoint Detection and Response Expert（バージョン 8.0 以降）**を選択します。コマンドラインを使用している場合は、タスク設定で `Mode=EDRExpertOnPrem` を設定します。デバイスで Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携を設定するには、いずれかのバージョン（バージョン 8.0 以降またはバージョン 7.1 以前）について、Web コンソールで「南京錠」を管理する必要があります。

オブジェクトの実行防止を使用する場合は、EDR Expert（オンプレミス）コンポーネントのオブジェクト実行防止ルールを有効にしてください。
EDR Expert（オンプレミス）コンポーネントのステータスは、次の手順で確認できます：

- 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。
  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（**資産（デバイス）→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**）。
- コマンドラインで次のコマンドを実行します： `kesl-control --app-info`。

EDR Expert（オンプレミス）と正しく連携するための参照イメージを準備する方法

> イメージを準備する前に、参照デバイスに `/var/opt/kaspersky/.ids_generated` ファイルが存在しないことを確認してください。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）と正しく連携するための参照イメージを準備するには：

> これらの手順を実行している間は、参照デバイスを再起動したり、Kaspersky Endpoint Security を再起動したりしないでください。

1. 次のコマンドを root 権限で実行します：

```
systemctl stop kesl
systemctl edit kesl
```

2. エディターで、`### Anything between here and the comment below will become the contents of the drop-in file` と `### Edits below this comment will be discarded` の行の間に次の設定のいずれかを追加します：

   - 一時仮想マシンで本製品が起動されるたびに SensorID をアップデートする

     ```
     [Service]
     ExecStartPre=-/usr/bin/uuid-regen.sh -a
     ```

   - 永続仮想マシンでは SensorID を一度だけアップデートする

     ```
     [Service]
     ExecStartPre=-/usr/bin/uuid-regen.sh -b
     ```

3. 変更を保存してエディターを閉じます。

   `/etc/systemd/system/kesl.d/override.conf` ファイルが作成されます。その内容を確認し、追加した設定と一致していることを確認します。

4. 次のコマンドを実行して systemd サービスを再読み込みします：

   ```
   systemctl daemon-reload
   ```

5. 次の内容で **/usr/bin/uuid-regen.sh** ファイルを作成します：

```
#!/usr/bin/env bash
# ------------------------------------------------------------
#  Kaspersky IDs updater
#  Modes:
#    -a   Always regenerate the IDs (default)
#    -b   Generate them only once – subsequent runs do nothing
#  Exit code: always 0
# ------------------------------------------------------------
set -euo pipefail
# ----- configuration ------------------------------------------------
PCID_FILE="/var/opt/kaspersky/kesl/common/pcid"
INSTALL_ID_FILE="/var/opt/kaspersky/epagent/install_id"
KESL_INI="/var/opt/kaspersky/kesl/common/kesl.ini"
# Marker that shows the script has already been executed in mode b
MARKER="/var/opt/kaspersky/.ids_generated"
# ----- default mode -------------------------------------------------
MODE="a"
# ----- parse command-line arguments ---------------------------------
while getopts ":ab" opt; do
   case $opt in
       a) MODE="a" ;;
       b) MODE="b" ;;
       \?) echo "Invalid option: -$OPTARG" >&2; exit 0 ;;
   esac
done
shift $((OPTIND-1))
# ----- helper: generate a new UUID and write to a file --------------
write_uuid() {
   local target=$1
   /usr/bin/uuidgen > "$target"
}
# ----- helper: replace MachineId in kesl.ini ------------------------
replace_machine_id() {
   local new_id
   new_id=$(/usr/bin/uuidgen)
   /usr/bin/sed -i "s/^MachineId=.*/MachineId=${new_id}/" "$KESL_INI"
}
# ----- main logic ---------------------------------------------------
if [[ "$MODE" == "b" && -f "$MARKER" ]]; then
   # Mode b – already ran once → do nothing
   :
else
   # (re)generate all required values
   write_uuid "$PCID_FILE"
   write_uuid "$INSTALL_ID_FILE"
   replace_machine_id
   # In mode b remember that we have already executed
   if [[ "$MODE" == "b" ]]; then
       /usr/bin/touch "$MARKER"
   fi
fi
exit 0
```

6. 次のコマンドを使用して、**/usr/bin/uuid-regen.sh** ファイルの権限を変更します：

```
chmod 700 /usr/bin/uuid-regen.sh
```

これで、参照デバイスはオペレーティングシステムイメージを作成する準備が整いました。

Web コンソールでの Kaspersky Endpoint Detection and Response Expert（オンプレミス）の連携の設定

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 → 組み込みエージェントの設定 → Endpoint Detection and Response Expert（オンプレミス）**）で、EDR Expert（オンプレミス）コンポーネントを有効または無効にし、Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携の設定を管理できます。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）と連携するには、EDR Expert（オンプレミス）コンポーネントを有効にし、
Endpoint Detection and Response Expert（バージョン 8.0 以降）オプション、つまり *EDR Expert (OSMP)* 連携モードを選択する必要があります。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）Integration の設定では、他のすべてのポリシー設定が継承される場合でも、階層内のネストされたポリシーを使用して独立した値を指定できます。親ポリシーで Kaspersky Endpoint Detection and Response Expert（オンプレミス）Integration が有効になっており、子ポリシーで設定の継承が有効になっている場合、既定では子ポリシーの連携設定も継承され、変更できません。個別の連携設定を行う場合は、ドロップダウンリストから［**カスタム接続設定を使用する**］を選択してください。これにより、Kaspersky Endpoint Detection and Response Expert（オンプレミス）Integration 設定を編集できるようになります。

コマンドラインでの Kaspersky Endpoint Detection and Response Expert（オンプレミス）の連携の設定

Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response Expert （オンプレミス）ソリューションの連携は、*Kaspersky Endpoint Detection and Response Expert （オンプレミス）(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。

このタスクでは、Kaspersky Endpoint Detection and Response (KATA) との連携設定も管理できます。Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携では、次を選択します：*EDR Expert（OSMP）連携モード。必要に応じて連携設定を管理します*。

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 Expert（オンプレミス）の連携設定を管理できます。

*Kaspersky Endpoint Detection and Response (KATA) との連携*タスクは既定では実行されません。タスクは、手動で開始および停止できます。

EDR Expert（オンプレミス）コンポーネント管理コマンドを使用して、OSMP サーバーへの接続に使用される証明書を管理できます。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）の連携設定

次の表は、*Kaspersky Endpoint Detection and Response Expert（オンプレミス）(KATAEDR) の連携の*事前定義済みタスクの設定について説明しています。このタスクは、Kaspersky Endpoint Detection and Response Expert（オンプレミス）および連携時に管理できます。

このタスクでは、Kaspersky Endpoint Detection and Response (KATA) との連携設定も管理できます。Kaspersky Endpoint Detection and Response Expert（オンプレミス）の連携では、タスク設定で*EDR Expert (OSMP)* 連携モード (`Mode=EDRExpertOnPrem`) を選択する必要があります。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）の連携設定

設定	説明	値
`Mode`	連携モード。 Kaspersky Endpoint Detection and Response Expert（オンプレミス）の連携では、Kaspersky Endpoint Security は OSMP プラットフォーム上のサーバーと対話します。 Kaspersky Endpoint Detection and Response (KATA) との連携では、Kaspersky Endpoint Security は Kaspersky Anti Targeted Attack Platform 上のサーバと対話します。	`EDRKATA`（既定）はEDR (KATA) 連携モードです。Kaspersky Anti Targeted Attack Platform のコンポーネントである Kaspersky Endpoint Detection and Response (KATA) との連携の有効化を許可します。 `EDRExpertOnPrem` は EDR Expert (OSMP) 連携モードです。Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携を有効にします
`UseClientPinnedCertificate`	OSMP 脅威対応処理サーバーへの接続のセキュリティを強化するために、相互認証を有効または無効にします。 OSMP 脅威対応サーバー側で相互認証が有効な場合、タスクを開始する前に、*Kaspersky Endpoint Detection and Response (KATA) との連携*タスクの設定で相互認証を有効にし、クライアント証明書を追加する必要があります。	`Yes` を選択すると、OSMP 脅威対応処理サーバーへの接続のセキュリティを強化するための相互認証が有効になります。 `No`（既定値）– 双方向認証は使用しません。
`SynchronizationPeriod`	OSMP 脅威対応処理サーバへの同期要求の周期（分単位）。	既定値：`5`。
`ConnectionTimeout`	OSMP 脅威対応処理サーバへの接続を待機する最大時間（秒単位）。	既定値：`10`。
`RequestTimeout`	OSMP 脅威対応処理サーバからの応答を待機する最大時間（秒単位）。	既定値：`10`。
`EnableTelemetry`	OSMP テレメトリサーバーへのイベントデータ（テレメトリ）の送信を有効および無効にします。	`Yes`（既定）は、OSMP テレメトリサーバへのテレメトリの送信を有効にします。 `No` は、テレメトリの送信を無効にします。
［**Endpoints.item_#**］セクションには、OSMP 脅威対応処理サーバーのアドレスとポートが含まれています。複数のサーバーを追加できます。		
`Address`	OSMP脅威対応処理サーバのアドレス。 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。 デバイスでネットワーク分離が有効になっている間にアプリケーション障害が発生してもサーバとの通信が中断されないようにするには、サーバの 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`	OSMP脅威対応サーバに接続するためのポート。	既定値：`443`。
[TelemetrySettings] セクションには、OSMP テレメトリサーバーに接続するための全般設定が含まれています。		

設定	説明	値
`UseClientPinnedCertificate`	OSMP テレメトリサーバへの接続のセキュリティを強化するために、相互認証を有効または無効にします。 OSMP テレメトリサーバー側で相互認証が有効な場合、タスクを開始する前に、*Kaspersky Endpoint Detection and Response (KATA) との連携*タスクの設定で相互認証を有効にし、クライアント証明書を追加する必要があります。	`Yes` を選択すると、OSMP テレメトリサーバーへの接続のセキュリティを強化するための相互認証が有効になります。 `No`（既定値）– 双方向認証は使用しません。
`ConnectionTimeout`	OSMP テレメトリサーバへの接続を待機する最大時間（秒単位）。	既定値：`10`。
`RequestTimeout`	OSMP テレメトリサーバからの応答を待機する最大時間（秒単位）。	既定値：`10`。
`OnlyTaggedEvents`	攻撃の兆候 (IOA) があるテレメトリのみの送信を有効または無効にします。*攻撃の兆候*とは、組織の IT インフラストラクチャにおけるオブジェクトの疑わしい動作の説明であり、組織への攻撃者による標的型攻撃の兆候である可能性があります。	`Yes` – 攻撃者の兆候 (IOA) があるテレメトリのみを送信します。 `No`（既定）– すべてのテレメトリを送信します。
[TelemetrySettings.Endpoints.item_#] セクションには、OSMPテレメトリサーバーのアドレスとポートが含まれています。複数のサーバーを追加できます。		
`Address`	OSMP テレメトリサーバ証明書のアドレス 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。 デバイスでネットワーク分離が有効になっている間にアプリケーション障害が発生してもサーバとの通信が中断されないようにするには、サーバの 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`	OSMP テレメトリサーバーに接続するためのポート	既定値：`443`。
[TelemetrySettings.EventTransferSettings] セクションには、OSMP テレメトリサーバへのデータ転送の設定が含まれています。		
`MaximumDataTransferTime`	OSMP テレメトリ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：`30`。
`UseRequestCountLimits`	OSMP テレメトリサーバーに送信されるイベント数の規制を有効または無効にします。	`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：`3000`。
`MaximumNumberOfEventsInPackage`	1 パッケージあたりの最大イベント数。	既定値：`1024`。
`EventLimitExceededPercentage`	イベント数が制限値（パーセンテージ）を超えています。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）を超える場合、イベントの送信は制限されます。	既定値：`15`。

OSMP 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、管理者 (admin) ロールを持つユーザーの権限が必要です。

コマンドを使用して、OSMP サーバーへの接続に使用する証明書を管理できます。証明書を使用すると、次の操作を実行できます：

- OSMP サーバー（脅威対応サーバーおよびテレメトリサーバー）の証明書を追加または置き換える
- 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
- OSMP サーバー（脅威対応サーバーおよびテレメトリサーバー）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追加または置き換える
- 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

OSMP 脅威対応サーバーへの接続用証明書の管理

脅威対応処理サーバーの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 <file> --server-type response
```

`<file>`は、サーバー証明書を含むファイルへのパスです。

脅威対応サーバー接続のクライアント証明書を追加または置き換える場合：

1. 次のコマンドを実行します：

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
   ```

   `<file>`は、クライアント証明書と秘密鍵を含む暗号化されたコンテナ（PFX アーカイブ）へのパスです。
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。

OSMP サーバーの設定でクライアント証明書の検証が有効になっており、*Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携*のタスク設定で、`[KATAEDR]` セクションの `UseClientPinnedCertificate` 設定の値が `yes` である場合、クライアント証明書は OSMP サーバーへの接続の追加保護に使用されます。

脅威対応処理サーバー証明書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 [-R] --query-kataedr-server-certificate --server-type response
```

脅威対応処理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 [-R] --query-kataedr-client-certificate --server-type response
```

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
- 証明書の発行元
- 証明書の開始日

- 証明書の有効期限
- SHA1 および SHA256 証明書のフィンガープリント

脅威対応処理サーバー証明書を削除するには、次のコマンドを実行します：

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type response
```

脅威対応処理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するには、次のコマンドを実行します：

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type response
```

OSMP テレメトリサーバーに接続するための証明書の管理

テレメトリサーバーの証明書を追加または置き換えるには、次のコマンドを実行します：

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
```

`<file>`は、サーバー証明書を含むファイルへのパスです。

テレメトリサーバー接続のクライアント証明書を追加または置き換える場合：

1. 次のコマンドを実行します：

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
   ```

   `<file>`は、クライアント証明書と秘密鍵を含む暗号化されたコンテナ（PFX アーカイブ）へのパスです。
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。

OSMP サーバーの設定でクライアント証明書の検証が有効になっており、*Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携*のタスク設定で、`[TelemetrySettings]` セクションの `UseClientPinnedCertificate` 設定の値が `yes` である場合、クライアント証明書は OSMP サーバーへの接続の追加保護に使用されます。

テレメトリサーバー証明書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 [-R] --query-kataedr-server-certificate --server-type telemetry
```

テレメトリ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 [-R] --query-kataedr-client-certificate --server-type telemetry
```

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

- 証明書の発行元
- 証明書の開始日
- 証明書の有効期限
- SHA1 および SHA256 証明書のフィンガープリント

テレメトリサーバー証明書を削除するには、次のコマンドを実行します：

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type telemetry
```

テレメトリ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するには、次のコマンドを実行します：

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type telemetry
```

Kaspersky Anti Targeted Attack Platform との連携

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。ソリューションについて詳しくは、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

Kaspersky Endpoint Security アプリケーションは、Kaspersky Anti Targeted Attack Platform の次のコンポーネントと連携できます。

- Kaspersky Endpoint Detection and Response (KATA) との連携。このコンポーネントは、組織のローカルネットワークにあるデバイスを保護します。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：
  - デバイスの情報イベントに関する情報（テレメトリ） を、Kaspersky Endpoint Detection and Response (KATA) (以降、「*KATA サーバー*」とも表記) との連携を提供する Central Node 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、Kaspersky Anti Targeted Attack Platform のセントラルノードサーバーに送信するとともに、本製品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) 7.1 以前との統合がサポートされています。

- Kaspersky Network Detection and Response (KATA)このコンポーネントは、組織の内部ネットワークを保護します。Kaspersky Network Detection and Response (KATA) と連携すると、Kaspersky Endpoint Security は、デバイス上のイベントに関する情報 （テレメトリ）を、Kaspersky Network Detection and Response (KATA) との対話を提供する セントラルノード（以降、「*NDR* サーバー」とも表記）に送信できます。

- Sandbox。サンドボックス技術により、展開されたオペレーティングシステムの仮想イメージを使用して特別なサーバ上のオブジェクトを分析およびスキャンし、企業の IT インフラストラクチャに対する悪意のあるアクティビティおよび標的型攻撃の兆候を検知することができます。Kaspersky Endpoint Securityアプリケーションを Kaspersky Anti Targeted Attack Platform上のサンドボックスに連携すると、本製品はスキャン用のファイルをセントラルノードサーバーに送信し、このサーバーがサンドボックスとの対話を処理します。

Kaspersky Anti Targeted Attack Platform との連携は、Kaspersky Endpoint Security アプリケーションの次のコンポーネントによって提供されます。

- Endpoint Detection and Response Expert（オンプレミス）コンポーネント（以下、*EDR Expert（オンプレミス）*とも呼ばれます）。

  Kaspersky Endpoint Security 12.4 for Linux 以降、Endpoint Detection and Response (KATA) コンポーネントは Endpoint Detection and Response Expert (オンプレミス) に名前が変更されました。このコンポーネントは、 Kaspersky Anti Targeted Attack Platform のコンポーネントである Kaspersky Endpoint Detection and Response (KATA) との統合だけでなく、Kaspersky Endpoint Detection and Response Expert（オンプレミス） ソリューションとの連携も提供します。

- Network Detection and Response (KATA)（以降「*NDR (KATA)*」とも表記）

- *Sandbox* コンポーネント

Kaspersky Endpoint Security アプリケーションと Kaspersky Anti Targeted Attack Platform ソリューションのすべてのコンポーネントの連携、および各コンポーネントの連携を個別に設定できます。

Kaspersky Anti Targeted Attack Platform と連携している場合、Kaspersky Endpoint Security を実行しているデバイスは、連携を提供するセントラルノードサーバーと暗号化された HTTPS 接続を確立します。安全な接続を実現するため、セントラルノードサーバーが発行する次の証明書を使用しています：

- 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。この操作には、Kaspersky Anti Targeted Attack Platform ソリューションとの連携を有効にする前に、サーバー証明書を追加する必要があります。

- クライアント証明書。この証明書は、相互認証を使用した追加の接続保護に使用されます（つまり、セントラルノードサーバーは Kaspersky Endpoint Security アプリケーションを搭載したデバイスを認証します）。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、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、EDR Expert（オンプレミス）、NDR (KATA)、またはサンドボックスコンポーネントの設定で相互認証を有効にし、クライアント証明書（証明書および秘密鍵を含む暗号コンテナ）を追加する必要があります。

Kaspersky Anti Targeted Attack Platform ソリューションのコンポーネントとの対話を処理するサーバーへの接続を保護するための証明書は、 Kaspersky Anti Targeted Attack Platform 管理者が提供する必要があります。

カスペルスキー Kaspersky Endpoint Security の全般設定でプロキシサーバーを使用するよう規定されている場合、Kaspersky Anti Targeted Attack Platform コンポーネントとの対話を処理するサーバーへの接続はプロキシサーバーを介して行われます。

Kaspersky Endpoint Detection and Response (KATA) 機能を使用するには、EDR Expert（オンプレミス）コンポーネントを有効にする必要があります。Kaspersky Endpoint Security を使用しているメインライセンスに Kaspersky Endpoint Detection and Response Expert（オンプレミス）機能が含まれていない場合は、この機能用の別のライセンスを購入し、EDR Expert（オンプレミス）ライセンスを本製品に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、SVM にライセンスを追加することで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 Endpoint Detection and Response (KATA) およびKaspersky Network Detection and Response (KATA) コンポーネントとの連携を設定するには、以下の手順に従います。

1. **Kaspersky Endpoint Security の必須コンポーネントの有効化**

   EDR Expert (KATA) および NDR (KATA) コンポーネントは、次のコンポーネントの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
   - アンチクリプター。
   - 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

   Kaspersky Endpoint Security 製品を Kaspersky Anti Targeted Attack Platform と適切に接続するには、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。ふるまい検知が無効になっている場合、必要なテレメトリは送信されません（同期要求と他の保護コンポーネントからの脅威検知データは例外）。

   ふるまい検知が eBPF メカニズムを使用してシステムテレメトリを取得する場合（eBPF に対応するカーネルバージョン 4.18 以降の 64 ビットオペレーティングシステムで利用可能）、テレメトリデータはより包括的になります。

2. **EDR Expert (オンプレミス) コンポーネントのアクティベートする**

   Kaspersky Endpoint Detection and Response (KATA) との連携を行うには、EDR Expert（オンプレミス）コンポーネントをアクティベートする必要があります。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 Expert（オンプレミス）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 Expert（オンプレミス）を使用するための別のライセンスを購入し、EDR Expert（オンプレミス）ライセンスをアプリケーションに追加しました。

     仮想環境を保護するために Kaspersky Endpoint Security を Light Agent モードで使用している場合は、追加機能をアクティベートするためのライセンスを SVM に現在のライセンスとして追加する必要があります。

Kaspersky Endpoint Security のメインライセンスで Kaspersky Network Detection and Response (KATA) との連携機能が既にカバーされているため、NDR (KATA) コンポーネントをアクティベートする必要はありません。

3. **EDR Expert（オンプレミス）コンポーネントの有効化**

   既定では、 Kaspersky Endpoint Detection and Response (KATA) の連携は無効になっています。連携を有効にするには、EDR Expert（オンプレミス）コンポーネントを有効にして設定する必要があります。

   - Kaspersky Security Center Web コンソールを使用します。
   - Kaspersky Security Center 管理コンソールを使用する。
   - コマンドラインを使用する。

   > Web コンソールまたはコマンドラインを使用して Kaspersky Endpoint Detection and Response (KATA) と連携するには、EDR Expert（オンプレミス）コンポーネントの設定で *EDR (KATA)* 連携モードを選択する必要があります。Web コンソールを使用している場合は、ポリシー設定で **Endpoint Detection and Response Expert（バージョン 7.1 以前）**を選択します。コマンドラインを使用している場合は、タスク設定で`Mode=EDRKATA`を設定します。デバイス上で Kaspersky Endpoint Detection and Response (KATA) との連携を設定するには、どちらのバージョン（バージョン 8.0 以降およびバージョン 7.1 以前）についても、Web コンソールで「南京錠」を管理する必要があります。

   オブジェクトの実行防止を使用する場合は、EDR Expert（オンプレミス）コンポーネントのオブジェクト実行防止ルールを有効にしてください。

4. **NDR (KATA) コンポーネントの有効化**

   既定では、Kaspersky Network Detection and Response (KATA) との連携は無効になっています。連携を有効にするには、NDR (KATA) コンポーネントを有効にして設定する必要があります。

   - Kaspersky Security Center Web コンソールを使用します。
   - Kaspersky Security Center 管理コンソールを使用する。
   - コマンドラインを使用する。

EDR Expert（オンプレミス）コンポーネントと NDR (KATA) コンポーネントのステータスは、以下の手順で確認できます。

- 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。

  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（**資産（デバイス）→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**）。

- コマンドラインで次のコマンドを実行します： `kesl-control --app-info`。

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、ポリシーのプロパティ（[**製品設定**] → [**組み込みエージェントの設定**] → [**Endpoint Detection and Response Expert（オンプレミス）**]）で、Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response (KATA) の連携設定を管理できます。

Kaspersky Endpoint Detection and Response (KATA) と連携するには、EDR Expert（オンプレミス）コンポーネントを有効にし、**Endpoint Detection and Response Expert（バージョン 7.1 以前）**オプション、つまり *EDR (KATA)* 連携モードを選択する必要があります。

Web コンソールのポリシーで Endpoint Detection and Response Expert（KATA）コンポーネントの**データ転送設定**に指定された**イベント送信時の最大遅延時間（秒）**設定の値を適用するには、ポリシーのプロパティで、**データ転送設定**および**リクエストのスロットリング**設定グループの「ロック」を閉じる必要があります。デバイス上で `MaximumDataTransferTime` 設定をローカルに変更できるようにするには、EDR（KATA）モードの KATAEDR タスクの `[EventTransferSettings]` セクションで、ポリシーのプロパティにある**データ転送設定**および**リクエストのスロットリング**設定グループの「ロック」を解除する必要があります。

管理コンソールで Kaspersky Endpoint Detection and Response (KATA) の連携の設定

管理コンソールでは、ポリシープロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）で、EDR Expert（オンプレミス）コンポーネントを有効または無効にしたり、Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response (KATA) コンポーネントとの連携設定を管理したりできます（**Detection and Response → EDR Expert（オンプレミス）**）。

EDR Expert（オンプレミス）コンポーネントの Web コンソールで **Endpoint Detection and Response Expert（バージョン 8.0 以降）**が選択されている場合、つまり EDR Expert (OSMP) 連携モードが選択されている場合は、管理コンソールに警告が表示され、Kaspersky Endpoint Detection and Response (KATA) との連携の設定は使用可能ではありません。連携モードは、Web コンソールで変更できます。

Kaspersky Endpoint Detection and Response（KATA）連携設定

設定	説明
Endpoint Detection and Response Expert（オンプレミス）を有効にする	このチェックボックスは、Kaspersky Endpoint Detection and Response (KATA) との連携を提供する EDR Expert（オンプレミス）コンポーネントを有効または無効にします。 コンポーネントは、既定で無効になっています。
オブジェクトの実行防止を有効にする	このチェックボックスは、オブジェクトの実行防止のための EDR Expert（オンプレミス）ルールを有効または無効にします。
KATA サーバー	[**設定**] をクリックすると、KATA サーバーへの接続を設定したり、接続が設定されているサーバーのリストを表示したりできるウィンドウが開きます。
サーバー接続設定	[**設定**] 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**] 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転送の設定を行えます。

KATA サーバー接続の設定

このテーブルには、KATA サーバーの接続設定がリストされます。テーブルには、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 サーバー接続設定を追加する
- 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

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。 デバイスでネットワーク分離が有効になっている間にアプリケーション障害が発生してもサーバとの通信が中断されないようにするには、サーバの 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`。
ポート	KATA サーバーに接続するためのポート。 既定値：`443`。

KATA サーバー接続の全般設定の管理

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（分）：	KATA サーバーへの同期リクエストの送信頻度（分）。 既定値：`5`。
サーバーとの接続を待つ時間（秒）	KATA サーバーへの接続を待つ最大時間（秒）。 既定値：`10`。
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時間（秒）。 既定値：`10`。
テレメトリの送信を許可する	このチェックボックスは、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。

設定	説明
サーバー証明書	このセクションには、サーバー証明書を追加または削除するためのボタンが含まれています： • ［**追加**］をクリックすると、サーバー証明書を追加できる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。 証明書を追加するウィンドウでは、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、DER または PEM 形式の証明書が含まれる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。 • 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	このセクションには、相互認証を使用して接続の追加セキュリティを構成するためのコントロールが含まれています： • ［**相互認証を使用する**］は、KATA サーバーへの接続をさらに安全にするために相互認証を有効または無効にします。相互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。 • ［**追加**］は、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を開きます。［**相互認証を使用する**］がオンで、クライアント証明書がまだ追加されていない場合、このボタンが表示されます。 クライアント証明書を追加するには、証明書を追加するウィンドウで、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 圧縮ファイル）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。アーカイブがパスワードで保護されている場合、［**暗号化されたコンテナのパスワード**］フィールドにパスワードを入力します。 • ［**削除**］は、以前に追加されたクライアント証明書を削除します。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のみ表示されます。

KATA サーバーへのデータ転送の設定

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の設定

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：`30`。
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有効または無効にします。
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：`3000`。
制限を超えるイベント数（パーセント）	イベント数が制限値（パーセンテージ）を超えています。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：`15`。

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) コンポーネントの連携は、*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。

このタスクでは、Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携設定も管理できます。Kaspersky Endpoint Detection and Response (KATA) との連携では、タスク設定で*EDR (KATA)* 連携モードを選択し、必要に応じて連携設定を管理する必要があります。

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*タスクは既定では実行されません。タスクは、手動で開始および停止できます。

EDR Expert（オンプレミス）コンポーネント管理コマンドを使用して、KATA サーバーへの接続に使用される証明書を管理できます。

Kaspersky Endpoint Detection and Response（KATA）連携設定

次のテーブルは、Kaspersky Endpoint Detection and Response Expert（オンプレミス）(KATAEDR) の連携の*事前定義済みタスク*の設定について説明しています。このタスクは、Kaspersky Endpoint Detection and Response (KATA) と連携時に管理できます。

このタスクでは、Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携設定も管理できます。Kaspersky Endpoint Detection and Response (KATA) との連携では、タスク設定で *EDR (KATA)* 連携モードを選択する必要があります (`Mode=EDRKATA`)。

Kaspersky Endpoint Detection and Response（KATA）連携設定

設定	説明	値
`Mode`	連携モード。 Kaspersky Endpoint Detection and Response Expert（オンプレミス）の連携では、Kaspersky Endpoint Security は OSMP プラットフォーム上のサーバーと対話します。 Kaspersky Endpoint Detection and Response (KATA) との連携では、Kaspersky Endpoint Security は Kaspersky Anti Targeted Attack Platform 上のサーバと対話します。	`EDRKATA`（既定）はEDR (KATA) 連携モードです。Kaspersky Anti Targeted Attack Platform のコンポーネントである Kaspersky Endpoint Detection and Response (KATA) との連携の有効化を許可します。 `EDRExpertOnPrem` は EDR Expert（OSMP）連携モードです。Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携を有効にします
`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 サーバー側で相互認証が有効な場合、タスクを開始する前に、*Kaspersky Endpoint Detection and Response (KATA) との連携*タスクの設定で相互認証を有効にし、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、双方向認証を使用します。 `No`（既定値）– 双方向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：`5`。

設定	説明	値
ConnectionTimeout	KATA サーバーへの接続を待つ最大時間（秒）。	既定値：10。
RequestTimeout	KATA サーバーからの応答を待つ時間（秒）。	既定値：10。
EnableTelemetry	KATA 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 は、テレメトリの送信を無効にします。
［Endpoints.item_#］セクションには、KATA サーバーのアドレスとポートが含まれています。複数のサーバーを追加できます。		
Address	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。 デバイスでネットワーク分離が有効になっている間にアプリケーション障害が発生してもサーバとの通信が中断されないようにするには、サーバの 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：443。
[EventTransferSettings] セクションには、KATA サーバーにデータを送信するための設定が含まれています。		
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：30。
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：3000。
MaximumNumberOfEventsInPackage	1 パッケージあたりの最大イベント数。	既定値：1024。
EventLimitExceededPercentage	イベント数が制限値（パーセンテージ）を超えています。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）を超える場合、イベントの送信は制限されます。	既定値：15。

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、管理者 (admin) ロールを持つユーザーの権限が必要です。

コマンドを使用して、KATA サーバーへの接続に使用される証明書を管理できます。証明書を使用すると、次の操作を実行できます：

- KATA サーバー証明書を追加または置き換える
- 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
- KATA サーバーへの接続を安全性の高いために使用されるクライアント証明書を削除または置き換える
- 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 <file>
```

`<file>`は、サーバー証明書を含むファイルへのパスです。

クライアント証明書を追加または変更するには：

1. 次のコマンドを実行します：

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file>
   ```

   `<file>`は、クライアント証明書と秘密鍵を含む暗号化されたコンテナ（PFX アーカイブ）へのパスです。

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 サーバー設定、および*カスペルスキー Endpoint Detection and Response Expert（オンプレミス）の連携*の*タスク設定*でクライアント証明書の検証が有効になっており、`UseClientPinnedCertificate` が `yes` に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。

サーバー証明書情報を表示するには、次のコマンドを実行します：

```
kesl-control [-R] --query-kataedr-server-certificate
```

クライアント証明書情報を表示するには、次のコマンドを実行します：

```
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
- 証明書の発行元
- 証明書の開始日
- 証明書の有効期限
- 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
```

Web コンソールで Kaspersky Network Detection and Response (KATA) との連携の設定

Web コンソールでは、ポリシーのプロパティ（**製品設定 → 組み込みエージェントの設定 → Network Detection and Response (KATA)**）で Kaspersky Network Detection and Response (KATA) の連携設定を管理できます。

Web コンソールのポリシーで Network Detection and Response (KATA) コンポーネントの **データ転送設定** に指定した **イベント送信時の最大遅延時間（秒）** の値を適用するには、ポリシーのプロパティで **データ転送設定** および **リクエストのスロットリング** 設定グループの「ロック」を閉じる必要があります。デバイス上で `MaximumDataTransferTime` 設定をローカルに変更できるようにするには、KATANDR タスクの `[EventTransferSettings]` セクションで、ポリシーのプロパティにある **データ転送設定** および **リクエストのスロットリング** 設定グループの「ロック」を解除する必要があります。

管理コンソールで Kaspersky Network Detection and Response (KATA) との連携の設定

管理コンソールでは、ポリシーのプロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**Detection and Response → Network Detection and Response (KATA)**）で、NDR (KATA) コンポーネントを有効または無効にしたり、Kaspersky Endpoint Security アプリケーションと Kaspersky Network Detection and Response (KATA) コンポーネントの連携設定を管理したりできます。

Kaspersky Endpoint Detection and Response (KATA) の連携設定

設定	説明
Network Detection and Response (KATA) の有効化。	このチェックボックスでは、NDR (KATA) を有効または無効にするかを選択します。 コンポーネントは、既定で無効になっています。
NDR サーバー	［**設定**］をクリックすると、NDR サーバーへの接続を設定したり、接続が設定されているサーバーのリストを表示したりできるウィンドウが開きます。
サーバー接続設定	［**設定**］をクリックすると、NDR 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、NDR 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**］をクリックすると、ウィンドウが開き、NDR サーバーへのデータ転送の設定を行えます。

NDR サーバー接続の設定

このテーブルには、NDR サーバーの接続設定がリストされます。テーブルには、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：

- NDR サーバー接続設定を追加する
- 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

サーバー接続設定

設定	説明
アドレス	NDR 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。 既定値：`127.0.0.1`。
ポート	NDR サーバーに接続するためのポート。 既定値：`443`。

NDR サーバー接続の全般設定の管理

このウィンドウでは、NDR サーバーに接続するための全般設定を設定できます。

NDR サーバー接続設定

設定	説明
NDR サーバーに同期リクエストを送信する間隔（分）：	NDR サーバーへの同期リクエストの送信頻度（分）。 既定値：`5`。
サーバーとの接続を待つ時間（秒）	NDR サーバーへの接続を待つ最大時間（秒）。 既定値：`10`。
サーバーからの応答を待つ最大時間（秒）	NDR サーバーからの応答を待つ時間（秒）。 既定値：`10`。
サーバー証明書	このセクションには、サーバー証明書を追加または削除するためのボタンが含まれています： • ［**追加**］をクリックすると、サーバー証明書を追加できる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。 証明書を追加するウィンドウでは、次のいずれかの方法で NDR 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、DER または PEM 形式の証明書が含まれる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。 • 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	このセクションには、相互認証を使用して接続の追加セキュリティを構成するためのコントロールが含まれています： • ［**相互認証を使用する**］は、NDR サーバーへの接続をさらに安全にするために相互認証を有効または無効にします。相互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。 　NDR 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。 • ［**追加**］は、NDR 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を開きます。［**相互認証を使用する**］がオンで、クライアント証明書がまだ追加されていない場合、このボタンが表示されます。 クライアント証明書を追加するには、証明書を追加するウィンドウで、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 圧縮ファイル）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。アーカイブがパスワードで保護されている場合、［**暗号化されたコンテナのパスワード**］フィールドにパスワードを入力します。 • ［**削除**］は、以前に追加されたクライアント証明書を削除します。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のみ表示されます。

NDR サーバーへのデータ転送の設定

このウィンドウでは、NDR 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。

NDR サーバーへのデータ送信の設定

設定	説明
イベント送信時の最大遅延（秒）	NDR 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：`30`。
1パッケージあたりの最大イベント数	1パッケージあたりの最大イベント数。 既定値：`1024`。
サーバーのポーリング頻度	NDR サーバーへの同期リクエストの送信頻度（秒）。 既定値：`450`。
イベントスロットリングをオンにする	NDR サーバーに送信されるイベント数の規制を有効または無効にします。
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：`3000`。
制限を超えるイベント数（パーセント）	イベント数が制限値（パーセンテージ）を超えています。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：`15`。

コマンドラインで Kaspersky Network Detection and Response (KATA) の連携の設定

Kaspersky Network Security と Kaspersky Endpoint Detection and Response (KATA) の連携は、*Kaspersky Network Detection and Response (KATA) Integration (KATANDR)* 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 Network Detection and Response (KATA) Integration は既定では実行されません。タスクは、手動で開始および停止できます。

事前定義済みタスクの設定を編集することで、Kaspersky Network Detection and Response (KATA) の連携設定を構成できます。

NDR (KATA) コンポーネント管理コマンドを使用して、NDR サーバーへの接続に使用される証明書を管理できます。

Kaspersky Endpoint Detection and Response (KATA) の連携設定

この表では、*Kaspersky Network 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 Network Detection and Response（KATA）との連携タスク設定

設定	説明	値
`UseClientPinnedCertificate`	NDR 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。 NDR サーバー側でクライアント証明書の検証が有効になっている場合は、*Kaspersky Network Detection and Response (KATA) の連携*タスクを開始する前に、クライアント証明書の使用を有効にし、クライアント証明書を追加します。	`Yes` – NDR サーバーとの接続をさらに安全にするために、双方向認証を使用します。 `No`（既定値）– 双方向認証は使用しません。
`SynchronizationPeriod`	NDR サーバーへの同期リクエストの送信頻度（分）。	既定値：`5`。
`ConnectionTimeout`	NDR サーバーへの接続を待つ最大時間（秒）。	既定値：`10`。
`RequestTimeout`	NDR サーバーからの応答を待つ時間（秒）。	既定値：`10`。

設定	説明	値
［**Endpoints.item_#**］セクションには、NDR サーバーのアドレスとポートが含まれています。		
`Address`	NDR 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。	既定値：`127.0.0.1`。
`Port`	NDR サーバーに接続するためのポート。	既定値：`8081`。
[EventTransferSettings] セクションには、NDR サーバーにイベントを送信するための設定が含まれています。		
`MaximumDataTransferTime`	NDR 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：`30`。
`MaximumNumberOfEventsInPackage`	1パッケージあたりの最大イベント数。	既定値：`1024`。
`UseRequestCountLimits`	NDR 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：`3000`。
`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）を超える場合、イベントの送信は制限されます。	既定値：`15`。
`PingPeriod`	NDR サーバーのポーリング期間（秒）。	既定値：`450`。

NDR 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、管理者 (admin) ロールを持つユーザーの権限が必要です。

コマンドを使用して、NDR サーバーへの接続に使用される証明書を管理できます。証明書を使用すると、次の操作を実行できます：

- NDR サーバー証明書を追加または置き換える
- 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
- NDR サーバーへの接続を安全性の高いために使用されるクライアント証明書を削除または置き換えます
- 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-katandr-server-certificate <file>
```

`<file>`は、サーバー証明書を含むファイルへのパスです。

クライアント証明書を追加または変更するには：

1. 次のコマンドを実行します：

```
kesl-control [-R] --add-katandr-client-certificate <file>
```

<file>は、クライアント証明書と秘密鍵を含む暗号化されたコンテナ（PFX アーカイブ）へのパスです。

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。

NDR サーバー設定でクライアント証明書の検証が有効になっており、*Kaspersky Network Detection and Response (KATA) との連携* の *タスク設定* で `UseClientPinnedCertificate` が `yes` に設定されている場合、クライアント証明書は NDR サーバーへの接続をさらに保護するために使用されます。

サーバー証明書情報を表示するには、次のコマンドを実行します：

```
kesl-control [-R] --query-katandr-server-certificate
```

クライアント証明書情報を表示するには、次のコマンドを実行します：

```
kesl-control [-R] --query-katandr-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
- 証明書の発行元
- 証明書の開始日
- 証明書の有効期限
- 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-katandr-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-katandr-client-certificate
```

サンドボックス統合

サンドボックス技術により、展開されたオペレーティングシステムの仮想イメージを使用して特別なサーバ上のオブジェクトを分析およびスキャンし、企業の IT インフラストラクチャに対する悪意のあるアクティビティおよび標的型攻撃の兆候を検知することができます。

Kaspersky Endpoint Security は、Open Single Management Platform (OSMP) または Kaspersky Anti Targeted Attack Platform 上のサンドボックスと対話できます。プラットフォームに応じて、Kaspersky Endpoint Security とサンドボックスの対話は、*サンドボックスサーバー*（OSMP サーバーまたはセントラルノードサーバー）によって処理されます。

サンドボックスとの連携は、Kaspersky Endpoint Security のサンドボックスコンポーネントによって提供されます。

サンドボックスと連携する時、Kaspersky Endpoint Security を実行しているデバイスは、Integration Server との暗号化された HTTPS 接続を確立します。安全な接続を実現するため、OSMP サーバーまたはセントラルノードサーバーが発行する次の証明書を使用しています：

- 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。そのためには、サンドボックスとの連携を有効にする前に、サーバー証明書を追加する必要があります。

- クライアント証明書。この証明書は、相互認証を使用した追加の接続保護に使用されます（つまり、OSMP サーバーまたはセントラルノードサーバーは Kaspersky Endpoint Security を搭載したデバイスを認証します）。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、サーバーはクライアント証明書をチェックしませんが、OSMP 側または Kaspersky Anti Targeted Attack Platform 側で相互認証を有効にすることができます。この場合、サンドボックスコンポーネントの設定で相互認証を有効にし、クライアント証明書（証明書および秘密鍵を含む暗号コンテナ）を追加する必要があります。

サンドボックスとの対話を処理するサーバーとの接続を保護するための証明書は、OSMP プラットフォームまたは Kaspersky Anti Targeted Attack Platform の管理者が提供する必要があります。

Kaspersky Endpoint Security の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、サンドボックスとの対話を処理するサーバーへの接続にはプロキシサーバーが使用されます。

ファイルとディレクトリは、次の通りのいずれかのモードでサンドボックスに送信してスキャンすることができます：

- *手動*.このモードでは、コマンドまたはグラフィカルインターフェイスを使用することで、オブジェクトを手動でサンドボックスに送信してスキャンすることができます。

- *自動のみ*。本製品は自動的にオブジェクトをスキャンに送信します。サンドボックスでスキャンするオブジェクトを手動で送信することはできません。

- *自動と手動*。本製品は自動的にオブジェクトをスキャンする用に送信しますが、コマンドまたはグラフィカルインターフェイスを使用してオブジェクトを手動でサンドボックスに送信することもできます。

サンドボックスとの連携は、既定でオフになっています。Web コンソールまたはコマンドラインを使用して、サンドボックスコンポーネントを有効または無効にしたり、次の通り連携設定を管理したりできます：

- スキャンする用オブジェクトの送信モードを選択します（手動、および自動のみ、自動および手動）。

- 脅威が検知された時に本製品が実行する処理を選択します（サンドボックスにオブジェクトを送信する非同期モードが有効な場合）。

  - 検知されたオブジェクトを含むファイルを削除し、ファイルのコピーを隔離します。

  - 簡易スキャンタスクを開始します。既定では、プロセスメモリ、カーネルメモリ、ブートセクター、起動オブジェクト、および検知されたオブジェクトへのパスをスキャンします。

  - IOC スキャンタスクを作成します。本製品は自動的に IOC スキャンタスクを作成します。タスクの開始モード、スキャン範囲、および IOC 検知時に実行する処理（検知されたオブジェクトの削除、簡易スキャンタスクの開始）を設定できます。

- サンドボックスサーバー接続の全般設定を構成します。

- サンドボックスサーバー証明書を追加または削除します。
- サンドボックスサーバーに接続するときに相互認証を設定し、クライアント証明書を追加します。

Web コンソールでのサンドボックス連携の設定

Web コンソールでは、ポリシーのプロパティ（**製品設定 → 組み込みエージェントの設定 → Sandbox**）で、Sandbox との連携設定を管理できます。

コマンドラインでの サンドボックス連携の設定

コマンドラインでは、*サンドボックス連携*事前定義済みタスクを使用して、Kaspersky Endpoint Security アプリケーションとサンドボックスの連携を管理できます。

既定では、*サンドボックス連携*タスクは実行されていません。このタスクは、手動で開始および停止できます。

サーバー証明書が追加されていない場合、*［サンドボックスとの連携］*タスクを開始できません。

*［サンドボックス連携］*タスクが実行されている場合は、コマンドラインを使用してファイルをサンドボックスに送信し、スキャンすることができます。

スキャンのためにファイルをサンドボックスに送信するには、次のコマンドを実行します：

```
kesl-control [-X] --sandbox <パス>
```

<パス>は、スキャンするファイルまたは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。

事前定義済みタスクの設定を編集することで、サンドボックス連携の設定を管理できます。

サンドボックスとの連携の設定を管理するコマンドを使用して、サンドボックスサーバーとの対話を行うサーバーへの接続に使用される証明書を管理することができます。

Sandbox との連携の設定

次のテーブルは、*サンドボックス連携*タスクで指定できるすべての設定と、それらの設定の既定値を示しています。

設定	説明	値
UseClientCertificate	サンドボックス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。 サンドボックスサーバー側でクライアント証明書の検証が有効になっている場合は、*サンドボックスの連携*タスクを開始する前に、クライアント証明書の使用を有効にし、クライアント証明書を追加します。	Yes – サンドボックスサーバーとの接続をさらに安全にするために、双方向認証を使用します。 No（既定値）– 双方向認証は使用しません。
ConnectionTimeout	サーバーへの接続を待つ最大時間（秒）	既定値：10。
RequestTimeout	サーバーからの応答を待つ最大時間（秒）	既定値：10。
SendingMode	オブジェクトをスキャン対象サンドボックスに送信するモードです。	AutoOnly（既定値）ーファイルへのアクセスが試行された時、自動的にスキャンするファイルを送信します。 Manual ー手動でスキャンするファイルを送信します。 AutoAndManual ー自動と手動の両方でスキャンするファイルを送信します。
QuarantineFile	脅威が検知された時にファイルを隔離します。	Yes （既定値）－脅威が検知された場合、元のファイルを削除し、ファイルのコピーを隔離に保存します。 No ー脅威が検知されてもファイルを隔離しません。
ScanCriticalAreas	脅威が検知された時、簡易スキャンします。	Yes （既定値）－脅威が検知された時、簡易スキャンを行います。 No ー脅威が検出されても、簡易スキャンを開始しません。
CreateIocScanTask	脅威が検知された時、IOC スキャンタスクを作成します。	Yes（既定）－脅威が検知された時、IOC スキャンタスクを作成します。 No ー脅威が検知されても、IOCスキャンタスクを作成しません。
QuarantineFileOnIocDetected	セキュリティ侵害インジケーターが検知された時、オブジェクトを隔離します。	Yes （既定値）－セキュリティ侵害インジケーターが検知された場合、元のオブジェクトを削除し、そのオブジェクトのコピーを隔離します。 Noーセキュリティ侵害インジケーターが検知されてもオブジェクトを隔離しません。
ScanCriticalAreasOnIocDetected	セキュリティ侵害インジケーターが検知された時、簡易スキャンを行います。	Yes （既定値）－セキュリティ侵害インジケーターが検知された時に簡易スキャンを行います。 No ーセキュリティ侵害インジケーターが検知されても簡易スキャンを開始しません。
Drives	IOC スキャンの範囲です。	Critical（既定）– ユーザーディレクトリとシステムディレクトリ内のファイルをスキャンします。 System – root ファイルシステム内のすべてのファイルをスキャンします。
ScheduleMode	IOC スキャンタスク開始モードです。	Manually（既定）－ IOC スキャンタスクを手動で開始します。 AfterTreatDetected ー脅威が検知された後、IOC スキャンタスクを開始します。
[Servers.item_#] セクションには、サンドボックスサーバーの設定が含まれています。		
Address	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。	既定値：127.0.0.1。
Port	サーバーに接続するためのポート	既定値：443。

設定	説明	値
[SandboxTransferSettings] セクションには、サンドボックスにスキャンファイルを送信するための設定が含まれています。		
SandboxQueue	スキャン要求キューの最大サイズ（メガバイト単位）。	既定値：1024。

Sandbox 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、管理者 (admin) ロールを持つユーザーの権限が必要です。

コマンドを使用して、Sandbox との連携を担う OSMP サーバーまたは Central Node サーバー（以下、「Sandbox サーバー」とも表記します）への接続に使用される証明書を管理できます。証明書を使用すると、次の操作を実行できます：

- 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 [-X] --add-sandbox-server-certificate <file>
```

<file>は、サーバー証明書を含むファイルへのパスです。

クライアント証明書を追加または変更するには：

1. 次のコマンドを実行します：

   ```
   kesl-control [-X] --add-sandbox-client-certificate <file>
   ```

   <file>は、クライアント証明書と秘密鍵を含む暗号化されたコンテナ（PFX アーカイブ）へのパスです。

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。

クライアント証明書は、Sandbox サーバーの設定でクライアント証明書の検証が有効になっており、*Sandbox との連携*タスクの設定で **UseClientCertificate** が **yes** に設定されている場合に、Sandbox サーバーへの接続をさらに保護するために使用されます。

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 [-X] --query-sandbox-server-certificate
  ```

- クライアント証明書の場合：

  ```
  kesl-control [-X] --query-sandbox-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
- 証明書の発行元
- 証明書の開始日
- 証明書の有効期限
- 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 [-X] --remove-sandbox-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 [-X] --remove-sandbox-client-certificate
```

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脅威対応処理を実行できるようにします。

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 Security 12.4 for Linux は、Kaspersky Endpoint Detection and Response Optimum バージョン 3.1 と互換性があります。

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脅威対応処理を実行します。

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 Detection and Response Optimum 機能を使用するには、EDR Optimum コンポーネントを有効にする必要があります。Kaspersky Endpoint Security を使用しているメインライセンスに Kaspersky Endpoint Detection and Response Optimum 機能が含まれていない場合は、この機能用の別のライセンスを購入し、EDR Optimum ライセンスを本製品に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、SVM にライセンスを追加することで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 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、機能し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

   オブジェクトの実行防止を有効にすることもできます。

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。

> 仮想環境を保護するために Kaspersky Endpoint Security を Light Agent モードで使用している場合は、追加機能をアクティベートするためのライセンスを SVM に現在のライセンスとして追加する必要があります。

4 **Kaspersky Endpoint Detection and Response Optimum 管理プラグインのインストール**

Kaspersky Endpoint Detection and Response Optimum 管理プラグインは、Windows、Mac、Linux オペレーティングシステム上のエージェントを管理するための統合プラグインであり、アラートの表示やアラートの詳細の表示に必要です。

5 **EDR Optimum コンポーネントの有効化**

既定では、EDR Optimum は無効になっています。コンポーネントを有効化または無効化し、整合性設定を管理できます。

- Web コンソールを使用。
- コマンドラインを使用する。

> 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する。

6 **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、次の設定が必要です。

- バックアップと隔離内のファイルに関する情報の Kaspersky Security Center ストレージへの送信を有効にします。このためには、ポリシーのプロパティで次のチェックボックスをオンにする必要があります：
  - **バックアップにあるファイルについて**
  - **隔離にあるファイルについて**

- アラートリストの表示を許可する このためには、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［**EDR アラートを表示**］トグルスイッチを有効にします。

  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

EDR Optimum コンポーネントを有効または無効にできます。

- Web コンソールを使用。
- コマンドラインを使用する。

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 コンソールでは、EDR Optimum コンポーネントを有効または無効にし、Kaspersky Endpoint Detection and Response Optimum との連携を設定できます。

- ポリシーのプロパティ（**製品設定** → **組み込みエージェントの設定** → **Endpoint Detection and Response**）で
- 管理対象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 → **アプリケーション**タブ → <Kaspersky Endpoint Security アプリケーション名>リンク → **製品設定**タブ → **Detection and Response**セクション → **Endpoint Detection and Response Optimum**）。

  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 EDR Optimum コンポーネントを有効または無効にすることはできません。

デバイスのプロパティの 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 を Kaspersky Endpoint Detection and Response Optimum ソリューションと連携するために必要な EDR Optimum 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。
ネットワーク分離	［**デバイスへのブロック解除の設定**］リンクをクリックすると、［**デバイスへ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。
除外リスト	［**除外リストの設定**］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

全般設定の `UseEdrOptimum` 設定を使用して、EDR Optimum 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。

コマンドラインオプションを使用して EDR Optimum コンポーネントを有効にするには：

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

コマンドラインオプションを使用して EDR Optimum コンポーネントを無効にするには：

```
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**］タブ →［<Kaspersky Endpoint Security アプリケーション名> リンク →［**全般**］タブ → **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

コマンド `kesl-control --app-info` 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

アラートの詳細ウィンドウでは、次の脅威対応処理を実行できます：

- 脅威が検知されたデバイスを分離する
- ファイルを隔離する
- *IOC* スキャンタスクを作成する

アラート詳細の保存期間は 30 日間です。この時間が経過すると、古いエントリは自動的に削除されます。

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。

Kaspersky Managed Detection and Response との連携

Kaspersky Managed Detection and Response は、テレメトリと高度な機械学習テクノロジーを使用して、インフラストラクチャ内のセキュリティインシデントを自動的に検知し、分析するソリューションです。インシデントに関する情報はカスペルスキーのエキスパートに送信され、エキスパートはインシデントを自ら処理するか、解決方法に関する推奨事項を提供します。

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 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脅威対応処理を実行します。

Kaspersky Endpoint Security と Kaspersky Managed Detection and Response ソリューションの連携は、本製品の Managed Detection and Response (MDR) コンポーネントによって容易になります。

Kaspersky Managed Detection and Response 機能を使用するには、次のいずれかの方法で MDR コンポーネントをアクティベートする必要があります：

- 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ライセンスを追加します。Kaspersky Endpoint Security は、Kaspersky Managed Detection and Response 機能を含むライセンスでアクティベートできます（詳細については、Kaspersky Managed Detection and Response ヘルプを参照してください）。本製品を使用しているメインライセンスに Kaspersky Managed Detection and Response 機能が含まれていない場合は、この機能用の別のライセンスを購入し、MDR ライセンスを本製品に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、SVM にライセンスを追加することで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 Managed Detection and Response 機能を有効にするライセンスは、まず MDR ポータルに登録する必要があります。

- Kaspersky Managed Detection and Response のライセンス情報が含まれる *MDR BLOB ファイル*をデバイスにアップロードします。BLOB ファイルは、MDR 設定情報ファイルの ZIP 圧縮ファイル内にあります。BLOB ファイルは、Web コンソール、管理コンソール、またはコマンドラインでアップロードできます。

設定が KPSN 設定ファイルなしでの動作要件を満たしていない場合は、 Kaspersky Managed Detection and Response と連携させるには、 KPSN 設定情報ファイル を Kaspersky Security Center 管理サーバーにアップロードする必要があります。このファイルには必要なテレメトリ設定が含まれています。拡張子 .pkcs7 の KPSN 設定情報ファイルは、MDR 設定情報ファイルの ZIP 圧縮ファイルにあります。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。

Kaspersky Managed Detection and Response 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、機能していることを確認します。

   - ファイル脅威対策
   - ふるまい検知

   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。

2. **拡張モードでの Kaspersky Security Network の使用の有効化。**

   Kaspersky Security Network が無効になっているか標準モードで使用されている場合、Kaspersky Managed Detection and Response 機能は使用できません。Kaspersky Security Network の使用は、Web コンソール、管理コンソール、またはコマンドラインで設定できます。

3. **MDR コンポーネントのアクティベーション**

   ライセンスに基づいて MDR コンポーネントを使用する場合は、次のいずれかの条件が満たされていることを確認してください：

   - Kaspersky Endpoint Security は、Kaspersky Managed Detection and Response 機能を含むライセンスに基づいて使用されています。
   - Kaspersky Managed Detection and Response 機能を使用するための別のライセンスを購入し、MDR ライセンスをアプリケーションに追加しました。

     仮想環境を保護するために Kaspersky Endpoint Security を Light Agent モードで使用している場合は、追加機能をアクティベートするためのライセンスを SVM に現在のライセンスとして追加する必要があります。

   MDR BLOB ファイルを使用して MDR コンポーネントをアクティベートする場合は、Web コンソール、管理コンソール、またはコマンドラインで BLOB ファイルをアップロードする必要があります。

4. **KPSN 設定情報ファイルのアップロード**

   設定が KPSN 設定ファイルなしでの動作要件を満たしていない場合は、 KPSN 設定情報ファイルを Kaspersky Security Center 管理サーバーへアップロードする必要があります。

5. **MDR コンポーネントの有効化**

   MDR コンポーネントは、既定で無効になっています。次の操作で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：

   - Web コンソールを使用。
   - 管理コンソールを使用。
   - コマンドラインを使用する。

   次の操作で MDR コンポーネントのステータスを確認できます：

   - Web コンソールまたは 管理コンソールのデバイスプロパティで。
   - コマンドラインを使用。

MDR と正しく連携するための参照イメージの作成に関する推奨事項

参照イメージに Kaspersky Endpoint Security for Linux を含めることは推奨しません。

参照イメージに Kaspersky Endpoint Security for Linux が含まれている場合、このイメージに基づく各デバイスで次の手順を実行します：

1. 新しい UUID を作成するには、次のコマンドを実行します：

```
uuidgen > /var/opt/kaspersky/kesl/common/pcid
uuidgen > /var/opt/kaspersky/epagent/install_id
```

2. Kaspersky Endpoint Security for Linux をアンインストールしてから、再インストールします。

これらの手順を実行しない場合、デバイスが正しく識別されない可能性があります。

Kaspersky Managed Detection and Response との連携のための KPSN 設定情報ファイルのアップロード

設定が KPSN 設定ファイルなしでの動作要件を満たしていない場合は、 Kaspersky Managed Detection and Response と連携させるには、 *KPSN 設定情報ファイル* を Kaspersky Security Center 管理サーバーにアップロードする必要があります。このファイルには必要なテレメトリ設定が含まれています。拡張子 .pkcs7 の KPSN 設定情報ファイルは、MDR 設定情報ファイルの ZIP 圧縮ファイルにあります。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。

KPSN 設定情報ファイルを Web コンソールまたは管理コンソールにアップロードできます。

KPSN 設計情報ファイルをアップロードすることで、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 コンソールを使用して KPSN 設定情報ファイルをアップロードする場合：

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. pkcs7 拡張子の付いた KSN 設定情報ファイルを選択し、［**開く**］をクリックします。
8. KPSN に関する声明の利用規約に同意し、［**保存**］をクリックします。

管理コンソールを使用して KPSN 設定情報ファイルをアップロードする場合：

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. ［**KPSN 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. pkcs7 拡張子の付いた KSN 設定情報ファイルを選択し、［**開く**］をクリックします。
8. KPSN に関する声明の利用規約に同意し、［**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、ポリシーのプロパティ（[**製品設定**] → [**Built-in Agents Configuration**] → [**Managed Detection and Response**]）で Kaspersky Managed Detection and Response の連携設定を管理できます。

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、ポリシーのプロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**Detection and Response → Managed Detection and Response**）で、MDR コンポーネントを有効または無効にしたり、MDR BLOB ファイルを読み込んだりできます。

MDR コンポーネントがライセンスでアクティベートされている場合は、MDR BLOB ファイルをアップロードする必要はありません。

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 MDR コンポーネントを有効または無効にします。 コンポーネントは、既定で無効になっています。 MDR コンポーネントを有効にし、 Kaspersky Security Network が無効になっているか標準モードで使用されている場合は、Kaspersky Security Network を拡張モードで有効にするために、Kaspersky Security Network に関する声明に同意するように求められます。 親ポリシーによって KSN 設定の変更が禁止されている場合は、エラーメッセージが表示され、MDR コンポーネントは有効化されません。
アップロード	このボタンをクリックすると、標準の Microsoft Windows のウィンドウが表示され、アップロードする MDR BLOB ファイルを選択できます。

BLOB ファイルは、Kaspersky Managed Detection and Response の配布キットに含まれる MDR 設定情報ファイルの ZIP アーカイブ内にあります。

BLOB ファイルをアップロードすることで、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。送信されたデータの処理に同意しない場合は、ファイルをアップロードしないでください。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：

- MDR コンポーネントを有効または無効にします。
- Kaspersky Managed Detection and Response ライセンスの情報が含まれる MDR BLOB ファイルをアップロードまたは削除します。

  MDR コンポーネントがライセンスでアクティベートされている場合は、MDR BLOB ファイルをアップロードする必要はありません。

- 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。

MDR 連携を有効または無効にするには、本製品の全般設定で `UseMDR` を編集します。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。

［`UseMDR`］パラメータが取り得る値は、次のとおりです：

- `Yes` は、MDR コンポーネントが有効にします。
- `No` は、MDR コンポーネントは無効にします。

MDR コンポーネントを有効にし、Kaspersky Security Network が無効になっているか基本モードで使用されている場合は、エラーメッセージが表示され、MDR コンポーネントは有効になりません。MDR コンポーネントを有効にするには、拡張モードで KSN を有効にする必要があります。

ライセンス管理コマンドを使用して MDR BLOB ファイルをアップロードまたは削除できます。BLOB ファイルは、MDR 設定情報ファイルの ZIP 圧縮ファイル内にあります。

BLOB ファイルをアップロードするには、次のコマンドを実行します：

```
kesl-control --load-mdr-blob <ファイルパス MDR BLOB>
```

BLOB 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。

ネットワーク分離

Detection and Response ソリューションと連携すると、脅威対応処理の一環としてデバイスをネットワークから分離できます。

ネットワーク分離に関する特別な考慮事項

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
- KSN 接続（Kaspersky Managed Detection and Response と連携している場合）

次のいずれかの条件が満たされた場合に、ネットワーク分離を適用できます。

- Kaspersky Endpoint Security が Kaspersky Endpoint Detection and Response Optimum ソリューションと連携すると、EDR Optimum コンポーネントがアクティベートされます。
- Kaspersky Endpoint Security アプリケーションと Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) コンポーネントとの連携が有効になり、EDR Expert（オンプレミス）コンポーネントがアクティベートされます。
- Kaspersky Endpoint Security と Kaspersky Managed Detection and Response ソリューションの連携が有効になり、MDR コンポーネントがアクティベートされます。

Kaspersky Managed Detection and Response（オンプレミス）、Kaspersky Endpoint Detection and Response (KATA)、および Kaspersky Managed Detection and Response と連携すると、デバイスのネットワーク分離が有効または無効になり、ネットワーク分離の除外リストが Detection and Response ソリューション側で設定されます。詳細については、Kaspersky Endpoint Detection and Response Expert（オンプレミス）のヘルプをご覧ください。Kaspersky Anti Targeted Attack Platform のヘルプ、または Kaspersky Managed Detection and Response ヘルプ。必要に応じて、デバイスのネットワーク分離を手動で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（Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) と連携されている場合のみ）
- コマンドラインで操作

Detection and Response ソリューションとの連携が有効になっているかどうか、および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、ネットワーク分離を手動で無効にすることは可能です。

Kaspersky Endpoint Detection and Response Optimum と連携すると、次のいずれかのモードでネットワーク分離を適用できます。

- 自動ネットワーク分離モード。セキュリティ侵害インジケーターが検知されると、デバイスはネットワークから自動的に分離されることがあります。［**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 検知時の応答処理を適用する**］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、本製品がセキュリティ侵害インジケーター (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。

  次の自動ネットワーク分離設定を管理できます。

  - ネットワーク分離が自動的に無効になるまでの期間を変更します。
  - 自動的に分離されたデバイスのネットワーク分離除外リストを設定します。

  > 自動的に分離されるデバイスがポリシーの対象である場合、ポリシーで指定された設定が適用されます。ポリシーが適用されていない場合は、デバイスのプロパティで指定された設定が適用されます。

- 手動ネットワーク分離モード。検知された脅威を調査している間、デバイスをネットワークから分離できます。［アラートの詳細］ウィンドウと Web コンソールのデバイスプロパティで、デバイスのネットワーク分離を手動で有効にすることができます。

  次の手動ネットワーク分離設定を管理できます。

  - ネットワーク分離が自動的に無効になるまでの期間を変更します。
  - 手動で分離されたデバイスのネットワーク分離除外を設定します。

Kaspersky Endpoint Detection and Response Optimum と連携すると、 Web コンソールのデバイスプロパティおよびコマンドラインでデバイスのネットワーク分離を手動で無効にすることができます。

コマンドラインでデバイスのネットワーク分離ステータスを確認できます。

分離されたデバイスには、**ISOLATED FROM NETWORK** タグが自動的に割り当てられます。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。

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、関連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 に不具合が発生した場合（かつ本製品が実行されていない場合）、Kaspersky Managed Detection and Response でネットワーク分離が有効になっていると、トラフィックがブロックされない可能性があります。

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。

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 が連携用の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。

名前によるネットワーク分離からのプロセスの除外は、eBPF および BTF に対応し、カーネルトレース用にトレースポイントと kprobes 機能が有効になっているカーネルバージョン 4.18 以降のデバイスに対応しています。

Kaspersky Endpoint Security を標準モードまたは Endpoint Detection and Response Agent モードで使用している場合、ネットワーク分離を使用するときは、以下をお勧めします：

- 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、使用するプロキシサーバーを設定し、除外リストに追加する必要があります。
- 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。

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

Kaspersky Endpoint Detection and Response Optimum と連携されている場合にのみ、Web コンソールを使用してデバイスのネットワーク分離を有効にできます。

Kaspersky Endpoint Detection and Response Optimum と連携して手動で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手動で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済みのアプリケーションのリストで、［Kaspersky Endpoint Security］をクリックします。

6. 開いたアプリケーションプロパティウィンドウで、［**製品設定**］タブで、［**Detection and Response**］→［**Endpoint Detection and Response Optimum**］リンクを選択します。

7. ウィンドウが開き、そのウィンドウの［**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**］ボタンをクリックします。

     このボタンをクリックすると、本製品は*ネットワーク分離を有効にする（NetworkIsolationStart）*タスクのプロパティで指定した期間、デバイスを分離します。

   - デバイスのネットワーク分離を無効にするには、［**隔離デバイスのブロックを解除**］ボタンをクリックします。

8. ［**OK**］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。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) と連携する場合に、デバイスのネットワーク分離を手動で無効にする

デバイスのネットワーク分離を手動で無効にします：

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済みのアプリケーションのリストで、［Kaspersky Endpoint Security］をクリックします。

6. 開いたアプリケーションプロパティウィンドウで、［**製品設定**］タブの［**Detection and Response**］セクションを選択します。

7. **ネットワーク分離（EDR Expert（オンプレミス））**で、［**分離されたデバイスのブロック解除**］をクリックして、デバイスのネットワーク分離を無効にします。

デバイスのネットワーク分離を無効にすると、Kaspersky Endpoint Security はデバイスから［**ISOLATED FROM NETWORK**］タグを削除します。

自動ネットワーク分離の期間設定

Kaspersky Endpoint Detection and Response Optimum と連携されている場合にのみ、自動ネットワーク分離の期間を設定できます：

*［IOC スキャン］*タスクによって分離されたデバイスのネットワーク分離は、一定の時間が経過すると自動的に無効になります。このタイムアウトは、Web コンソールのデバイスプロパティとポリシープロパティで設定できます。Web コンソール内ポリシープロパティのネットワーク隔離設定については、付録 5 で説明しています。管理対象デバイスのプロパティのネットワーク隔離設定については、次の表で説明します。

デバイスにポリシーが適用されている場合は、ポリシーで指定された設定が適用されます。自動ネットワーク分離タイムアウトはデバイスのプロパティでは設定できません。ポリシーがデバイスに適用されていない場合は、デバイスのプロパティで指定された設定が適用されます。

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済みのアプリケーションのリストで、［Kaspersky Endpoint Security］をクリックします。

6. 開いたアプリケーションプロパティウィンドウで、［**製品設定**］タブで、［**Detection and Response**］→［**Endpoint Detection and Response Optimum**］リンクを選択します。

7. ［**ネットワーク分離**］→［**デバイスへのブロック解除の設定**］の順にクリックします。

8. デバイスの［**ブロック解除の設定**］ウィンドウが開き、そのウィンドウで、［**自動的に隔離されたデバイスのブロックを解除するまでの期間**］チェックボックスをオンにし、その下の入力フィールドで、デバイスのブロックを自動的に解除するまでの期間を指定します。

9. 変更内容を保存します。

ネットワーク分離の手動構成

デバイスをネットワークから手動で分離するには、Kaspersky Endpoint Detection and Response Optimum との連携が必要です。

デバイスのネットワーク分離を手動で有効にする場合は、*ネットワーク分離の有効化* (*NetworkIsolationStart*) ローカルタスクを使用して、ネットワーク分離を事前に構成できます。デバイスのネットワーク分離の除外リストとネットワーク分離の期間を設定できます。

*ネットワーク分離の有効化*は事前定義済みタスクであり、次の場合にのみ自動的に実行されます：

- デバイスのプロパティで［**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た場合。
- アラート詳細ウィンドウでデバイスのネットワーク分離を有効にした場合。

［**追加**］ボタンをクリックして［*ネットワーク分離の有効化*］タスクの新しいインスタンスを作成したり、［**開始**］ボタンをクリックしてこのタスクを実行したりすることはできません。このタスクはデバイスのプロパティでのみ使用でき、デバイスのネットワーク分離を有効にする前に設定を変更できます。

*ネットワーク分離の有効化*タスク設定は、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適用されます。

デバイスのネットワーク分離パラメータを構成する場合：

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、［**タスク**］タブに移動します。

5. タスクリストで、*［ネットワーク分離の有効化］*タスクをクリックします。

   タスク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. ［**除外リストの設定**］をクリックすると、［**除外**］ウィンドウが表示されます。

8. 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。

9. ［OK］をクリックします。

10. ［**デバイスを分離する時間**］フィールドに、デバイスのネットワーク分離の希望期間（1時間単位）を入力します。

    ネットワーク分離の既定の期間は 5 時間です。

    ネットワーク分離の最短期間は 1 時間です。

11. ［**保存**］をクリックして、変更内容を保存します。

Web コンソールでのネットワーク分離からの除外設定

Kaspersky Endpoint Security が Endpoint Detection and Response Expert (オンプレミス)、Kaspersky Endpoint Detection and Response (KATA)、または Kaspersky Managed Detection and Response と連携されている場合、ネットワーク分離からの除外は、Detection and Response ソリューション側で設定されます。詳細については、Kaspersky Endpoint Detection and Response Expert（オンプレミス）のヘルプをご覧ください。Kaspersky Anti Targeted Attack Platform のヘルプ、または Kaspersky Managed Detection and Response ヘルプ。

Kaspersky Endpoint Security が Kaspersky Endpoint Detection and Response Optimum と連携されている場合、次の方法でネットワーク分離からの除外リストを設定できます：

- Web コンソールのポリシープロパティで操作。ポリシーで設定された除外は、ポリシーが適用されているデバイスに対してネットワーク分離が自動的に有効になったときに適用されます。

- Web コンソールのデバイスプロパティで操作。デバイスのプロパティで設定された除外リストは、ポリシーが適用されていないデバイスに対してネットワーク分離が自動的に有効になったときに適用されます。

- *ネットワーク分離の有効化 (NetworkIsolationStart) ローカルタスクの設定*。このタスクのプロパティで設定された除外リストは、デバイスのネットワーク分離を手動で有効にしたときに適用されます。*ネットワーク分離の有効化*タスクの設定は、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適用されます。

本製品には、ネットワーク分離の除外を設定するための*標準ネットワークプロファイル*のリストが用意されています。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。標準ネットワークプロファイルの設定を管理し、除外リストを手動で設定できます。

自動ネットワーク分離からの除外の設定

ポリシープロパティまたはデバイスプロパティで、自動的に分離されたデバイスのネットワーク分離除外を設定できます。Web コンソール内ポリシープロパティのネットワーク隔離設定については、付録 5 で説明しています。

Kaspersky Endpoint Detection and Response Optimum と連携されている場合のみ、ネットワーク分離から除外を設定できます：

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済みのアプリケーションのリストで、［Kaspersky Endpoint Security］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. 開いたアプリケーションプロパティウィンドウで、［**製品設定**］タブで、［**Detection and Response**］→［**Endpoint Detection and Response Optimum**］リンクを選択します。

7. ウィンドウが開き、そのウィンドウ［**除外**］の下にある［**除外の設定**］リンクをクリックして、［**除外**］ウィンドウを開きます。

8. 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。

9. **OK** をクリックして、変更内容を保存します。

ネットワーク分離除外を追加するウィンドウ

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を入力するフィールド。
通信方向	ドロップダウンリストで、ネットワーク接続の方向を選択できます： • **送信**。 • **受信**。 • **送受信**。
Protocol	ドロップダウンリストで、ネットワーク接続によって使用されるプロトコルを選択できます： • **すべて**。 • **カスタム**。 • ICMP。 • IPv6_ICMP： • TCP。 • UDP。 • IGMP。 • GRE。 • IPv4： • IPv6：
番号	ネットワーク接続番号を入力するフィールド。 このフィールドは、［**プロトコル**］ドロップダウンリストで［**カスタム**］を選択した場合に利用可能です。
ローカルポート / 範囲	このチェックボックスは、次のフィールドにリストされているローカルポート番号またはローカルポート範囲をネットワーク分離除外リストに追加します。
リモートポート / 範囲	このチェックボックスは、次のフィールドにリストされているリモートポート番号またはリモートポート範囲をネットワーク分離除外リストに追加します。
リモートアドレス	このチェックボックスは、次のフィールドで指定されたリモートデバイスの IP アドレスをネットワーク分離除外リストに追加します。
補足資料	このチェックボックスは、チェックボックスの下の表にリストされているアプリケーションをネットワーク分離除外リストに追加します。 ［**追加**］ボタンをクリックすると、ネットワーク接続をブロックしたくないアプリケーションへのパスを追加できます。開いたウィンドウで、［**アプリケーションへのパス**］フィールドにアプリケーションへのパスを入力し、変更を保存します。 削除するアプリケーションの横にあるチェックボックスをオンにして、［**削除**］ボタンをクリックすると、表からアプリケーションを削除できます。 これらの製品設定は、eBPF および BTF に対応し、カーネルトレース用にトレースポイントおよび kprobes 機能が有効になっているカーネルバージョン 4.18 以降のデバイスに適用されます。

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プロファイルを 1 つ以上選択できます。

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。

ネットワーク接続プロファイル	説明
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の作成を必要としないサービスです。
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	NetworkManager などの Linux ネットワークシステムサービス。

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

Detection and Response ソリューションと連携すると、コマンドラインで次の操作ができます：

- デバイスのネットワーク分離ステータスを確認し、ネットワーク分離除外リストを表示します。
- デバイスのネットワーク分離を無効にします。

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
```

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するには、次のコマンドを実行します：

```
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。*

隔離の管理

*隔離*は、ウイルスに感染している可能性があるファイルや検知時に駆除できないファイルをデバイス上で保存する特別な場所です。隔離により、ファイルを孤立させた上で調査することができます。隔離されたファイルは暗号化された形式で保存され、デバイスのセキュリティを脅かすことはありません。隔離とは対照的に、バックアップは、悪意のあるコードが検知され、駆除中に削除または変更されたファイルのバックアップコピーを保存します。

本製品は、Detection and Response ソリューションと連携し、推奨される脅威対応処理を実行する場合にのみ、隔離を使用します。本製品が Kaspersky Endpoint Detection and Response Optimum または Kaspersky Managed Detection and Response と連携している場合は、デバイスにとって危険であると思われるファイルを手動で隔離することもできます。

既定では、ディレクトリ /var/opt/kaspersky/kesl/common/objects-backup/ が隔離されたファイルの保存に使用されます。このディレクトリには、バックアップオブジェクトも含まれています。コマンドラインを使用して、バックアップおよび隔離オブジェクトを保存するディレクトリを変更できます。

隔離ファイルには、個人データが含まれる場合があります。隔離されたファイルにアクセスするには、root 権限が必要です。

Web コンソールまたは管理コンソールのポリシーを使用するか、コマンドラインを使用して、デバイスの隔離設定を構成できます。次の隔離設定を行うことができます：

- 隔離の容量に達したことを示すイベントを生成するために必要な隔離の使用割合。既定では、隔離が 90% の容量に達するとイベントが生成されます。
- 隔離の最大サイズ（メガバイト単位）。保管領域の最大サイズに到達すると、古いオブジェクトから削除されます。既定では、隔離の最大サイズは、アプリケーションが標準モードまたは EDR Agent モードで使用されている場合は 200 MB、Light Agent モードで使用されている場合は 100 MB です。
- バックアップおよび隔離オブジェクトが保存されるディレクトリへのパス（コマンドラインでのみ設定できます）。

ファイルの隔離

一部のファイルは、オペレーティングシステムとアプリケーションの動作にとって非常に重要になる場合があります。このようなファイルを隔離すると、システムの動作が中断される可能性があります。

システムクリティカルオブジェクト (SCO) を隔離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。

ファイルを隔離に置くことは、次のいずれかの条件が満たされた場合にのみ可能です。

- Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response Optimum の連携が有効であり、EDR Optimum コンポーネントがアクティベートされている場合。
- Kaspersky Endpoint Security アプリケーションと Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) コンポーネントとの連携が有効になり、EDR Expert（オンプレミス）コンポーネントがアクティベートされます。
- Kaspersky Endpoint Security と Kaspersky Managed Detection and Response の連携が有効であり、MDR コンポーネントがアクティベートされている場合。

隔離されたオブジェクトを保存するディレクトリは、書き込み可能であることが必要です。

Kaspersky Endpoint Detection and Response（オンプレミス）またはKaspersky Endpoint Detection and Response (KATA) と連携する場合、次のいずれかの方法でファイルを隔離できます：

- Detection and Response ソリューション側で構成されたタスク。詳細については、Kaspersky Endpoint Detection and Response Expert（オンプレミス）のヘルプ または Kaspersky Anti Targeted Attack Platform ヘルプ を参照してください。.
- プロセスメモリをスキャンする YARA スキャンタスク。

Kaspersky Managed Detection and Response と連携すると、ファイルは次のいずれかの方法で隔離されます：

- Kaspersky Managed Detection and Response 側で設定されたタスクの実行の結果として。
- デバイス上の隔離を管理するコマンドの実行の結果として。

Kaspersky Endpoint Detection and Response と連携した場合の隔離の扱い方の詳細については、Kaspersky Endpoint Detection and Response ヘルプを参照してください。

Kaspersky Endpoint Detection and Response と連携すると、ファイルは次のいずれかの方法で隔離されます：

- 侵害の兆候の検知の結果として自動的に。
- *Web コンソール*で作成できる隔離タスクの結果として。
- デバイス上の隔離を管理するコマンドの実行の結果として。
- アラートの詳細にある推奨事項に従った結果として。

Kaspersky Endpoint Detection and Response Optimum と連携した場合の隔離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。

隔離されたファイルの管理

隔離されたファイルを管理できます。

- Kaspersky Security Center では、 カスペルスキー製品によって隔離されたファイルの共通リストにあります。

  > Kaspersky Security Center で隔離されたファイルを管理するには、隔離されたファイルに関するデータを管理サーバーに転送できるようにする必要があります。

- コマンドラインを使用してデバイス上でローカルに実行します。

隔離されたファイルに関する情報を表示したり、隔離されたファイルを削除したり復元したりできます。

Detection and Response との連携が有効になっているかどうか、また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、隔離からファイルを復元、削除、および取得できます。

クライアントデバイス上のカスペルスキーアプリケーションによって隔離されたファイルの一般的なリストは、Kaspersky Security Center に保存され、管理コンソール（[**詳細設定**] → [**リポジトリ**] → [**隔離**]）および Web コンソール（[**操作**] → [**リポジトリ**] → [**隔離**]）で利用できます。Kaspersky Security Center は、隔離ストレージ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、クライアントデバイスの隔離ストレージに保存されます。Kaspersky Security Center での隔離ファイルの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。

隔離されたファイルは、指定された設定に従って元の場所に復元されます。復元では、MAC ラベル（Astra Linux デバイスのみ）と元のファイルの属性（不変属性と追加専用属性を含む）が保持されます。不変かつ追加専用の属性を持つファイルは、元のファイルが存在しない場合にのみその GPS 追跡に復元できます。また、元の GPS 追跡に復元することもできますが、名前が異なります。隔離ファイルを別のディレクトリに復元、別の名前で元の GPS 追跡に復元したりするには、root 権限が必要です。

復元プロセスが完了すると、アプリケーションは復元されたファイルの隔離されたコピーを削除します。

次の場合には、隔離からファイルを復元できません。

- 復元するファイルが隔離ストレージ内に見つかりませんでした。
- 復元するファイルの名前が間違って指定されているか、大文字と小文字が間違っています。
- ファイル ID が正しく指定されていません。
- 宛先ディレクトリが削除、移動、名前変更されたか、アクセス権がありません。
  この場合、アプリケーションはファイルをディレクトリ /var/opt/kaspersky/kesl/common/restored/ へ移動します。このディレクトリから任意のディレクトリにファイルを手動で移動できます。
- 指定されたパスに同じ名前のファイルが既に存在します。
- デバイスに十分なスペースがありません。
- Astra Linux デバイスのみ：ファイルの MAC ラベルが、ファイルの復元先ディレクトリの MAC ラベルよりも高い場合。
- Astra Linux デバイスファイル上のみ：ファイルの MAC ラベルが、ファイルの復元先のディレクトリの MAC ラベルよりも低く、ディレクトリに ccnr フラグが設定されていない。

次の場合には、隔離からファイルを削除できません。

- 削除するファイルが隔離ストレージ内に見つかりませんでした。
- 削除するファイルの名前が間違って指定されているか、大文字と小文字が間違っています。
- ファイル ID が正しく指定されていません。

Web コンソールを使用したファイルの隔離

Kaspersky Endpoint Detection and Response Optimum と連携する場合、Web コンソールの*隔離ファイル*タスクを使ってファイルを隔離できます。

すべての管理対象デバイスまたは特定のデバイスに対して隔離ファイルタスクを作成して実行できます。

タスクは、［**ファイルの隔離**］テーブルにある［**製品設定**］タブのタスクプロパティに記載されたファイルに対して実行されます。表には、隔離する必要があるファイルに関する次の情報が含まれています：

- **パス** – ファイルが保存されているデバイス上のディレクトリへのパス。
- **チェックサム種別** – ファイルチェックサム検証種別。

表の上にあるボタンを使用して、隔離するファイルに関する情報を追加または削除できます。

隔離するファイルに関する情報を追加するには、［**追加**］ボタンをクリックし、表示されるウィンドウでタスク設定を指定する必要があります。

隔離ファイルタスクの設定

設定	説明
隔離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、隔離するファイルへのパスを指定する方法を選択できます： • **完全パスでファイルを指定** • **ディレクトリパスとチェックサムでファイルを指定する**
ファイルへの完全パス	隔離するファイルへの完全パスを入力するフィールド。 このフィールドは、［**隔離するファイルを指定してください**］のドロップダウンリストで［**完全パスでファイルを指定**］を選択した場合に表示されます。 ファイルがネットワークドライブにある場合は、「`//`」の文字から始まるファイルへのパスを入力してください。たとえば、`//server_ip/shared_folder` と入力できます。
チェックサム種別	ドロップダウンリストでは、隔離するファイル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、［**隔離するファイルを指定してください**］のドロップダウンリストで［**ディレクトリパスとチェックサムでファイルを指定**］を選択した場合に表示されます。
ファイルチェックサム	隔離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、［**隔離するファイルを指定してください**］のドロップダウンリストで［**ディレクトリパスとチェックサムでファイルを指定**］を選択した場合に表示されます。
ファイルパス	隔離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、［**隔離するファイルを指定してください**］のドロップダウンリストで［**ディレクトリパスとチェックサムでファイルを指定**］を選択した場合に表示されます。 ファイルがネットワークドライブにある場合は、「`//`」の文字から始まるファイルへのパスを入力してください。たとえば、`//server_ip/shared_folder` と入力できます。

隔離するファイルが大きすぎると、［*ファイルの隔離*］タスクが［*隔離領域が不足しています*］というエラーで終了することがあります。この場合は、隔離を消去するか、隔離領域を追加してから再試行してください。

プロセスの開始タスクの結果は、Web コンソールのタスクプロパティの［**結果**］で確認できます。

Web コンソールでの隔離設定の編集

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** → **レポートと保管領域**）と管理対象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 → **アプリケーション**タブ → <Kaspersky Endpoint Security アプリケーション名>リンク → **製品設定**タブ → **ストレージ設定**セクション）で、隔離設定を管理できます。

管理対象デバイスのプロパティの隔離設定については、次のテーブルで説明します。

デバイスのプロパティの隔離設定

設定	説明
隔離のサイズを制限する（MB）：	隔離の最大サイズ (MB) を入力するテキストボックス。チェックボックスをオフにすると、隔離のサイズは制限されません。 既定値：200
隔離のサイズが次の割合に達した場合通知する（%）：	隔離の容量に達したことを示すイベントを生成するために必要な隔離の使用割合を入力するフィールド。チェックボックスをオフにすると、隔離が容量に達したというイベントは生成されません。 使用できる値：1～100。 既定値：90

管理コンソールでの隔離設定の編集

管理コンソールでは、ポリシーのプロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定 → ストレージ設定**）と管理対象デバイスのプロパティ（**管理対象デバイス → デバイス**タブ → デバイスのプロパティウィンドウ → **アプリケーション**セクション → アプリケーションのプロパティウィンドウ → **ストレージ設定**）で、隔離設定を管理できます。

隔離の設定

設定	説明
隔離のサイズを制限する（MB）：	このチェックボックスでは、隔離の最大サイズを指定された値（メガバイト単位）に制限するかどうかを有効または無効にします。チェックボックスをオフにすると、隔離のサイズは制限されません。 使用できる値：1～999999。 既定値：アプリケーションが標準モードまたは Endpoint Detection and Response Agent モードで使用されている場合は200 MB、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既定値は 100 MB です。
隔離のサイズが次の割合に達した場合通知する（%）：	このチェックボックスは、隔離の容量に達したことを示すイベントを生成するために必要な隔離の使用割合の制限を有効または無効にします。チェックボックスをオフにすると、隔離が容量に達したというイベントは生成されません。 使用できる値：1～100。 既定値：90

コマンドラインでの隔離設定の編集

コマンドラインでは、本製品の全般設定の `QuarantineSizeLimit`、`QuarantineFillingNotification` および `QuarantineBackupFolder` 設定を使用して隔離を構成できます。

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。

隔離の設定

設定	説明	値
`QuarantineFillingNotification`	隔離の容量に達したことを示すイベントを生成するために必要な隔離の使用割合。 隔離が容量に達したことに関するイベントの生成を無効にするには、0 を入力します。	0 から 100 0 – 隔離が容量に達したことに関するイベントの生成は無効です。 既定値：90

設定	説明	値
`QuarantineSizeLimit`	隔離の最大サイズ（メガバイト単位）。隔離の最大サイズに到達すると、最も古いファイルから削除されます。 隔離のサイズを無制限にするには、0 を入力します。	0 から 999999 0 は隔離のサイズが無制限でないことを意味します。 既定値：アプリケーションが標準モードまたは Endpoint Detection and Response Agent モードで使用されている場合は200 MB、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既定値は 100 MB です。
`QuarantineBackupFolder`	バックアップおよび隔離オブジェクトが保存されるディレクトリへのパス。既定のディレクトリとは異なるディレクトリを指定できます。バックアップおよび隔離オブジェクトを保存するディレクトリとして、任意のデバイス上のディレクトリを使用できます。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。 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隔離されたファイルの管理

Detection and Response ソリューションとす連携すると、コマンドラインで隔離管理コマンドを使用して次の操作を実行できます。

- ファイルを隔離します（Kaspersky Endpoint Detection and Response Optimum または Kaspersky Managed Detection and Response と連携されている場合のみ）。
- 隔離されたファイルに関する情報を表示します。
- 隔離からすべてのファイルまたは指定されたファイルを削除します。
- 隔離からファイルを復元します。

感染しているファイルを復元すると、デバイスへの感染の原因となる可能性があります。

ファイルを隔離する

ファイルを隔離するには、次のコマンドを実行します。

```
kesl-control [-Q] --put <ファイルパス> [--md5] [--sha256] [--save-original-file]
```

説明：

- **<ファイルパス>**は、隔離するファイルへのパスです。
- `--md5` は、隔離するファイルの MD5 ハッシュです。
- `--sha256` は、隔離するファイルの SHA256 ハッシュです。

- `--save-original-file` は元のファイルを保持します。このオプションを指定しない場合は、元のファイルは削除されます。

  ユーザーアカウントにオブジェクトを削除する権限がある場合にのみ、元のファイルが削除されます。権限が不十分な場合は、ファイル削除エラーメッセージが表示されます。

このコマンドは、Kaspersky Endpoint Detection and Response Optimum または Kaspersky Managed Detection and Response と連携されている場合にのみ利用できます。

隔離されたファイルに関する情報の表示

隔離されたファイル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 -Q --query ["<フィルター条件>"] [-n <数値>] [--json]
```

説明：

- **<フィルター条件>**には、クエリ結果を制限するために、and 論理演算子を使用して結合された、**<フィールド> <比較演算> '<値>'** 形式の1つ以上の 論理式を指定します。フィルター条件を指定しない場合、隔離されているすべてのファイルの詳細を表示します。
- **<数値>**は、表示する直近に隔離されたファイルの数です。`-n` オプションを指定しない場合は、最後の 30 個のファイルが表示されます。0 を指定してすべてのファイルを表示します。
- `--json` – データを JSON 形式で出力します。

`ObjectId` 行には、ファイルを隔離に配置するときにファイルに割り当てた数値 ID が表示されます。この ID は、ファイルの復元や隔離からの削除など、ファイルに対する処理を実行するために使用されます。

隔離からファイルを復元

隔離されたファイル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 -Q --restore <オブジェクト ID>
```

<オブジェクト ID>は、ファイルの隔離時にアプリケーションによってファイルに割り当てられた数値 ID です。

隔離からファイル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 -Q --restore <オブジェクト ID> --file <ファイルパス>
```

`--file <ファイルパス>`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。

ユーザーに root 権限がある場合にのみ、隔離されたファイルを別のディレクトリに復元できます。ユーザーの権限が不十分な場合、ファイルは元の位置にのみ復元できます。

閉鎖ソフトウェア環境モードの Astra Linux デバイスでは、バックアップにファイルを配置したときと同じアカウントでのみ、ファイルを復元できます。

隔離からファイルを削除

選択したファイルを隔離から削除するには、次のコマンドを実行します。

```
kesl-control -Q --mass-remove --query "<フィルター条件>"
```

<フィルター条件>は、結果を制限するために、論理演算子 **and** を使用して結合された、**<フィールド> <比較演算子> '<値>'** 形式の1つ以上の 論理式です。

例：
名前またはパスに「test」を含むファイルを削除します：

```
kesl-control -Q --mass-remove --query "FileName like '%test%'"
```

隔離からすべての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 -Q --mass-remove
```

プロセスの開始

Kaspersky Endpoint Security をDetection and Response ソリューションと連携すると、*［プロセスの実行］*タスクを使用して、保護対象デバイス上のプロセスと実行ファイルをリモートで実行できるようになります。

Kaspersky Endpoint Detection and Response Optimum と連携がある場合にのみ、Web コンソールで［プロセスの実行］タスクを作成して実行できます。Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Endpoint Detection and Response (KATA) または Kaspersky Managed Detection and Response と連携されている場合、検出および応答ソリューション側でタスクが作成され、実行されます。

*［開始プロセス］*タスクを使用すると、次の処理を開始できます：

- 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、［プロセスの終了］タスクを使用して停止したプロセスを、リモートで開始できます。
- 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、追加の SELinux の設定が必要です。

Web コンソールで［プロセスの開始］タスクを作成および実行し、*その設定を編集できます。コマンドラインでは［プロセスの開始］タスクを管理できません。*

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確認する `klnagchk` ツールを実行する場合は、**/< ユーティリティがあるディレクトリへの完全パス >/**`klnagchk` を入力し、必要に応じて、下の表で説明されているその他のフィールドに入力します。
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 /tmp/klnagchk.log` 引数を入力できます。この引数は、 `/tmp` 内の `klnagchk.log` という名前のファイルに結果を保存するようツールに指示します。 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 /tmp/klnagchk.log -savecert /home/user/certificate.cer` 引数を入力できます。これらの引数は、結果を `tmp` ディレクトリ内の `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の確認に使用する証明書を `/home/user/` ディレクトリ内の `certificate.cer` ファイルに保存するようツールに指示します。
作業用ディレクトリのパス（省略可能）	**実行コマンド**フィールドのコマンドが実行される作業ディレクトリへのパスを指定するフィールド。 たとえば、`/tmp` と入力し、次の引数を指定して `klnagchk` ユーティリティを実行できます：`-logfile klnagchk.log -savecert certificate.cer`。この場合、両方のファイルが `tmp` に作成されます。

［*プロセスの開始*］タスクの結果は、Web コンソールのタスクプロパティの［**製品設定**］→［**実行結果**］の順に選択して表示できます。

表には、［*プロセスの開始*］タスクが実行されたデバイスのリストと、タスクの結果が表示されます。［**デバイス**］ドロップダウンリストでは、タスクが実行されたすべての管理対象デバイスのタスク結果を表示するか、特定のデバイスのタスク結果を表示するかを選択できます。

表には次の情報が含まれます：

- **ステータス** – タスク完了ステータス
- **デバイス** – タスクが開始されたデバイスの名前
- **日時** – タスクが実行された日付と時刻
- **結果** – 戻りコードの形式でのタスク実行結果 戻りコードへのリンクをクリックすると、［**タスク結果**］ウィンドウが開き、次の情報が表示されます：
  - タスク完了ステータス
  - プロセス開始時間
  - タスク完了時間
  - プロセスが開始されたセッションの ID
  - 実行済みコマンド

- コマンドライン引数
- 作業用ディレクトリのパス
- リターンコード

［**タスク結果**］ウィンドウの **STDOUT ストリームをダウンロード**リンクをクリックすると、タスクの正常な実行に関するレポートを TXT 形式でダウンロードできます。［*プロセス開始*］タスクが失敗した場合、このレポートをダウンロードしようとするとエラーメッセージが表示されます。

［**タスク結果**］ウィンドウの **STDERR ストリームをダウンロード**リンクをクリックすると、タスク実行中に発生したエラーに関するレポートを TXT 形式でダウンロードできます。［*プロセス開始*］タスクが正常に完了した場合、このレポートをダウンロードしようとするとエラーメッセージが表示されます。

プロセスの終了

Kaspersky Endpoint Security を Detection and Response ソリューションと連携すると、*［プロセスの終了］*タスクを使用して、保護対象デバイス上のプロセスをリモートで終了できます。

Kaspersky Endpoint Detection and Response Optimum と連携がある場合にのみ、Web コンソールでプロセスを終了するタスクを作成して実行できます。Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Endpoint Detection and Response (KATA) または Kaspersky Managed Detection and Response と連携されている場合、検出および応答ソリューション側でタスクが作成され、実行されます。

*［プロセスの終了］*タスクを使用すると、次の処理を終了できます：

- 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し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) のプロセスは終了できません。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*および*実行し、*その設定を編集できます。コマンドラインでは［プロセスの終了］タスクを管理できません。*

設定	説明
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、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のパス別** • **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	ファイルへの完全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［**完全パス**］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、［**プロセスを終了させるファイルを指定**］ドロップダウンリストで［**ディレクトリへのパスと チェックサム**による］を選択した場合に表示されます。
ファイルチェックサム	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るファイルを指定**］ドロップダウンリストで［**ディレクトリへのパスとチェックサムによる**］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のパス別**］を選択した場合に表示されます。
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**］を選択した場合に表示されます。

［*プロセスの終了*］タスクの結果は、Web コンソールのタスクプロパティの［**結果**］で確認できます。

デバイスからのファイルの受信

Kaspersky Endpoint Security を Detection and Response ソリューションと連携すると、*ファイルの取得*タスクを使用して保護されたデバイスからファイルを取得できます。

Kaspersky Endpoint Detection and Response Optimum と連携されている場合にのみ、Web コンソールでデバイスからファイルを取得するタスクを作成して実行できます。Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Endpoint Detection and Response (KATA) または Kaspersky Managed Detection and Response と連携されている場合、検出および応答ソリューション側でタスクが作成され、実行されます。

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*［デバイスからのファイルの受信］タスクを作成および実行し、その設定を編集できます。コマンドラインでは［デバイスからのファイルの受信］タスクを管理できません。*

*［デバイスからファイルを受信する］*タスクは、［**製品設定**］タブの［**ファイルの取得**］表のタスクプロパティで指定されたファイルに対して実行されます。

表には、タスクが取得するファイルに関する次の情報が含まれています：

- **ディレクトリパス** – ファイルが保存されているデバイス上のディレクトリへのパス。
- **チェックサム検証種別** – ファイルチェックサム検証種別。

表の上にあるボタンを使用して、デバイスから取得するファイルに関する情報を追加、変更、または削除できます。

取得するファイルに関する情報を追加するには、［**追加**］ボタンをクリックし、表示される［**ファイルの取得**］ウィンドウでタスク設定を指定する必要があります。

デバイスタスク設定からのファイルの受信

設定	説明
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、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のパス別** • **完全パス**
ファイルへの完全パス	ファイルへの完全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［**完全パス**］を選択した場合に表示されます。
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、［**取得するファイルを指定**］ドロップダウンリストで［**ディレクトリへのパスとチェックサム**による］を選択すると表示されます。
ファイルチェックサム	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のパス別**］を選択した場合に表示されます。
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**］ドロップダウンリストで［**ディレクトリへのパスと チェックサム**による］を選択した場合に表示されます。

*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隔離されます。Web コンソールを使用して、このコピーを隔離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。

ファイルのサイズは 100 MB を超えることはできません。

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。

Kaspersky Security Center の隔離されたファイルのリストでは、ファイルスキャンの結果に関係なく、［*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のステータスが*「感染」*になります。

次の場合、［*デバイスからファイルを受信*］タスクはエラーで終了します。

- 指定されたファイルが見つかりません。
- 間違ったファイル情報（ファイル名またはチェックサム）が指定されています。
- 指定されたファイルを管理するための権限が不十分です。
- 指定されたファイルはブロックされています。

- 隔離のスペースが不足しています。
- 指定されたファイルは大きすぎます（100 MB 以上）。

プロセスの開始タスクの結果は、Web コンソールのタスクプロパティの［**結果**］で確認できます。

デバイスからのファイルの削除

Kaspersky Endpoint Security を Detection and Response ソリューションと連携すると、*ファイルの削除*タスクを使用して保護されたデバイスからファイルを削除できます。

Kaspersky Endpoint Detection and Response Optimum と連携されている場合にのみ、Web コンソールでファイルを削除するタスクを作成して実行できます。Kaspersky Endpoint Detection and Response (KATA) コンポーネントと連携されると、タスクは Kaspersky Endpoint Detection and Response (KATA) 側で生成され、実行されます。

重要なシステムオブジェクト（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［デバイスからのファイルの削除］タスクを作成および実行し、*その設定を編集できます。コマンドラインでは［デバイスからのファイルの削除］タスクを管理できません。*

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** • **完全パス**
ファイルへの完全パス	削除するファイルへの完全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［**完全パス**］を選択した場合に表示されます。
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、［**削除するファイルを指定**］ドロップダウンリストで［**ディレクトリへのパスとチェックサムによる**］を選択した場合に表示されます。
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**］ドロップダウンリストで［**パスまたはチェックサムによる**］を選択した場合に表示されます。
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**］ドロップダウンリストで［**パスまたはチェックサムによる**］を選択した場合に表示されます。
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。この場合、ファイルに対して *［プロセスを終了］* タスクを作成して実行し、再試行する必要があります。

プロセスの開始タスクの結果は、Web コンソールのタスクプロパティの［**結果**］で確認できます。

侵害の兆候の調査

*侵害の兆候（IOC）*は、デバイスへの不正アクセス（侵害されたデータ）を示すオブジェクトまたは処理に関する一連のデータです。たとえば、ログイン試行の失敗回数が多い場合、侵害の兆候が考えられます。Kaspersky Endpoint Security を検知および脅威対応ソリューションと連携すると、保護されたデバイス上のセキュリティ侵害インジケーターを検出し、脅威対応処理を実行できます。

侵害の兆候スキャン機能は、以下の条件のいずれかが満たされている場合に、Kaspersky Endpoint Security セキュリティ製品で利用できます。

- Kaspersky Endpoint Security が Kaspersky Endpoint Detection and Response Optimum ソリューションと連携すると、EDR Optimum コンポーネントがアクティベートされます。
- Kaspersky Endpoint Security アプリケーションと Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) コンポーネントとの連携が有効になり、EDR Expert（オンプレミス）コンポーネントがアクティベートされます。

Kaspersky Endpoint Detection and Response（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) と連携すると、関連する Detection and Response ソリューション側で IoC スキャンが生成されます。

Kaspersky Endpoint Detection and Response Optimum と連携している場合、IOC スキャンは *IOC* スキャンタスクを使用して実行されます。IOC スキャンタスクを作成できます。

- Web コンソールでのポリシーの設定
- ［アラート詳細］ウィンドウで操作
- コマンドラインで操作

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。

Kaspersky Endpoint Security は、*侵害の兆候*を検索するために、ユーザーが準備した IOC ファイルを使用します。侵害の兆候を手動で追加する場合は、IOC ファイルの要件を参照してください。IOC ファイルが要件を満たしていない場合、そのファイルは使用できません。

［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。同じ ID を持つ複数の IOC ファイルを読み込んだ場合、本製品はそれらの IOC ファイルのうちの 1 つだけを使用します。その他の IOC ファイルは自動的に除外されます。

Web コンソールでの侵害の兆候の検索

Kaspersky Endpoint Detection and Response Optimum と連携されている場合にのみ、Web コンソールのセキュリティ侵害インジケーターの［IOC スキャン］タスクを使用して侵害の兆候をスキャンできます。Kaspersky Endpoint Detection and Response（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) と連携すると、関連する Detection and Response ソリューション側で IoC 対応が生成されます。

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。

IOC スキャンタスクの場合、スケジュール設定で 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 スキャンタスクの基本設定は、タスクのプロパティの ［**製品設定**］タブ→［**IOC スキャン設定**］で変更できます。

［*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 ファイルを追加する**］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。

設定	説明
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。 • **簡易スキャンを開始する**。 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［*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、ブートセクター、およびその他**主要領域**をスキャンします。 • /lib/systemd • /lib/udev • /lib/dbus-1.0 • /usr/local/lib/systemd/user • /usr/share/dbus-1 • /usr/share/gdm/autostart • /usr/share/gnome/autostart • /var/spool/at • /var/spool/at/spool • /var/spool/anacron • /var/spool/cron • /boot • /bin • /sbin • /lib • /lib32 • /lib64 • /libx32 • /usr/lib • /usr/lib32 • /usr/lib64 • /usr/libx32 • ~/.config/autostart • ~/.config/autostart-scripts • ~/.config/plasma-workspace/env • ~/.config/plasma-workspace/shutdown • ~/.config/lxsession • ~/.fluxbox/startup • ~/.kde/Autostart • /etc • **コピーを隔離し、オブジェクトを削除する**。 チェックボックスをオンにすると、侵害の兆候が検出されると、アプリケーションはオブジェクトのコピーを隔離し、元のオブジェクトを削除します。

設定	説明
	• **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。 ポリシーが分離されたデバイスに適用される場合、ポリシープロパティで指定された［指定された期間後に自動的に分離を無効化］および［ネットワーク分離の除外］設定が適用されます。ポリシーがデバイスに適用されない場合は、分離されたデバイスのプロパティで指定された設定が適用されます。 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脅威対応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。

IOC スキャンタスクの詳細設定は、タスクプロパティの［**製品設定**］タブ→［**追加**］で変更できます。

［**IOC ファイルの再設定**］パネルで IOC ファイルを読み込んだ場合は、［**追加**］セクションを編集できます。

［*IOC* スキャン］タスクの詳細設定

設定	説明
IOC スキャン中に解析するデータ種別（IOC ドキュメント）	［**追加**］セクションのチェックボックスには、IOC スキャン中の分析に次のデータタイプ（IOC ドキュメント）が含まれます： • **プロセス - ProcessItem。** • **ファイル - FileItem。** • **IOC ドキュメント。** ［**IOC ファイルの再設定**］パネルで IOC ファイルを読み込んだ場合、［**IOC ドキュメント**］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、［**ファイルのスキャン設定 - FileItem**］ウィンドウに移動し、スキャン範囲を追加できます。 • **ARP テーブル - ArpEntryItem。** • **Network ポート - PortItem。** • **ユーザーアカウント - UserItem。** • **システムオブジェクト - SystemItem。**
次の範囲で IOC を検索する	このチェックボックスでは、次の範囲をスキャンするかどうかを選択できます。 • **デバイスのすべてのドライブのファイル。** • **デバイスのシステムドライブのファイル。** • **デバイスの重要な領域。**既定ではこのオプションが選択されます。 • **定義済みの領域をスキャンしない。**
カスタム領域をスキャンします	チェックボックスをオンにすると、チェックボックスの下の表にリストされている範囲がスキャン範囲のリストに追加されます。 ［**追加**］ボタンをクリックすると、スキャンする範囲へのパスを追加できます。開いたウィンドウで、［**範囲**］へのパスフィールドに範囲へのパスを入力し、変更を保存します。 削除する範囲の横にあるチェックボックスをオンにして、**[削除]** ボタンをクリックすると、表から範囲を削除できます。 ［**次の範囲で IOC を検索する**］リストで［**定義済みの領域をスキャンしない**］オプションが選択されている場合は、このチェックボックスをオフにすることはできません。

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 スキャンの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作成することを推奨します。

［*IOC* スキャン］タスクの結果は、Web コンソールのタスクプロパティの［**アプリケーション設定**］→［**IOC スキャンの結果**］で確認できます。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、タスクの結果が表示されます。［**デバイス**］ドロップダウンリストでは、タスクが実行されたすべての管理対象デバイスのタスク結果を表示するか、特定のデバイスのタスク結果を表示するかを選択できます。

表には次の情報が含まれます：

- **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。
- **デバイス** – タスクが開始されたデバイスの名前
- **日時** – タスクが実行された日付と時刻
- **結果** – ［*IOC スキャン*］タスクの結果に関する情報。次のいずれかのステータスが表示されます：
  - *IOC の検出* – 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。*

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。

コマンドラインでの侵害の兆候の検索

Kaspersky Endpoint Detection and Response Optimum と連携されている場合にのみ、コマンドラインでセキュリティ侵害インジケーターをスキャンするタスクを使用してセキュリティ侵害インジケーターをスキャンできます。Kaspersky Endpoint Detection and Response（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) と連携すると、関連する Detection and Response ソリューション側で IoC 対応が生成されます。

コマンドラインから IOC スキャンタスクを作成、設定、実行するには、次のコマンドを実行します：

```
kesl-control [-T] --scan-ioc --path <ディレクトリまたはファイルへのパス> [--process on|off] [--hint <正規表現>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--excludes <除外リスト>] [--scope <ディレクトリのリスト>] [--action Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

説明：

- `--path <ディレクトリまたはファイルへのパス>` は、スキャンの実行に使用する、.IOC または .XML 拡張子を持つ IOC ファイル、または IOC ファイルを含む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。両方の種別のパス（ファイルへのパスとディレクトリへのパス）を指定することもできます。

- `--process` – デバイス上で実行されているプロセスの分析を有効にします。
  考えられる引数：
  - `on` – デバイス上で実行されているプロセスの分析を有効にします（既定値）。
  - `off` – デバイス上で実行されているプロセスの分析を無効にします。

--process オプションを指定しない場合、アプリケーションは使用される IOC ファイルでこれらのプロセスの詳細 (ProcessItem) が指定されている場合にのみプロセスを分析します。

- --hint <**正規表現**> は、分析対象のファイル（FileItem）またはプロセスの実行ファイル（ProcessItem）への完全パスに一致する正規表現です。

  次の正規表現要素を使用できます：

  - メタ文字：. ^ $ |
  - 文字クラス：数字、英字、小文字、大文字、cntrl
  - 量指定子：* + ? {n} {n,} {n, m}
  - 否定：[^a-c]
  - エスケープ文字：\a \e \f, \n \r \t \v \b

- --arpentry – ARP テーブル (ArpEntryItem) 内のエントリの分析を有効にします。

  考えられる引数：

  - on – ARP 表内のエントリの分析を有効にします（既定値）。
  - off – ARP 表内のエントリの分析を無効にします。

  --arpentry オプションを指定しない場合、使用される IOC ファイルで ARP 表の詳細 (ArpEntryItem) が指定されている場合にのみ ARP 表を分析します。

  --ports – 接続用に開いているポートの分析を有効にします。

  考えられる引数：

  - on – 接続用に開いているポートの分析を有効にし、デバイス上のアクティブな接続をスキャンします（既定値）。
  - off – 接続用に開いているポートの分析を無効にし、デバイス上のアクティブな接続をスキャンしません。

  --ports オプションを指定しない場合、使用される IOC ファイルでこれらのポートの詳細 (PortItem) が指定されている場合にのみポートを分析します。

- --system – システム環境の分析を有効にします。

  考えられる引数：

  - on – システム環境の分析を有効にします（既定値）。
  - off – システム環境の分析を無効にします。

  --system オプションを指定しない場合、使用される IOC ファイルでシステム環境の詳細 (SystemInfoItem) が指定されている場合にのみ、システム環境を分析します。

- --files – ファイル分析を有効にします。

考えられる引数：

- `on` – ファイル分析を有効にします（既定値）。
- `off` – ファイル分析を無効にします。

`--files` オプションを指定しない場合、使用される IOC ファイルでファイルの詳細 (`FileItem`) が指定されている場合にのみファイルを分析します。

- `--drives` – スキャンする領域。
  考えられる引数：
  - `all` – 利用可能なすべてのファイル領域をチェックします。
  - `system` – root ファイルシステム内のすべてのファイルをスキャンします。
  - `critical` – ユーザーディレクトリとシステムディレクトリ内のファイルをスキャンします（既定値）。
  - `custom` – 指定した領域内のファイルのみをスキャンします。

  `--drives` オプションを指定しない場合、アプリケーションはユーザーディレクトリとシステムディレクトリ内のファイルを分析します。
- `--excludes <除外リスト>` は、スキャンから除外されるパスのリストです。
  このオプションで指定された除外はグローバルであり、範囲の種別やディレクトリリストに関係なく有効です。これらの除外は、`--hint` や `--scope` などの他のコマンドラインオプションよりも優先されます。

  > 除外はパスとして指定されますが、再帰要素やワイルドカード文字（例：`*`）を含めることはできません。

  `--excludes` オプションを指定しない場合は、除外なしでスキャンが実行されます。
  スペースで区切って複数の除外を指定することもできる。
- `--scope <ディレクトリのリスト>` は、スキャンする追加ディレクトリのリストです。

  > このオプションは、`--drives` オプションに `custom` 引数を指定した場合に必要です。

- `--action` – 侵害の兆候が検知された場合に実行される処理。
  考えられる引数：
  - `Skip` – 検知されたオブジェクトに対して処理を実行しませんが、そのオブジェクトに関する情報はタスク実行結果に保存されます（既定値）。
  - `QuarantineFile` – 検知されたオブジェクトを隔離します。
  - `IsolateHost` – オブジェクトが検知されたデバイスにネットワーク分離を強制します。

- `ScanCriticalAreas` – **簡易スキャン**を実行します。
  - /lib/systemd
  - /lib/udev
  - /lib/dbus-1.0
  - /usr/local/lib/systemd/user
  - /usr/share/dbus-1
  - /usr/share/gdm/autostart
  - /usr/share/gnome/autostart
  - /var/spool/at
  - /var/spool/at/spool
  - /var/spool/anacron
  - /var/spool/cron
  - /boot
  - /bin
  - /sbin
  - /lib
  - /lib32
  - /lib64
  - /libx32
  - /usr/lib
  - /usr/lib32
  - /usr/lib64
  - /usr/libx32
  - ~/.config/autostart
  - ~/.config/autostart-scripts
  - ~/.config/plasma-workspace/env
  - ~/.config/plasma-workspace/shutdown
  - ~/.config/lxsession

- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

スペースで区切って複数のパスを指定することもできます。

> `Skip` 引数を指定する場合は、他の引数を追加しないでください。`Skip` 引数は単独でのみ使用できます。

IOC ファイルの要件

IOC スキャンタスクを作成する際は、次の IOC ファイルの要件および制限を考慮してください：

- 本製品は、侵害の兆候を記述するためのオープンスタンダードである OpenIOC 形式バージョン 1.0 および 1.1 の .IOC または .XML 拡張子を持つ IOC ファイルに対応しています。
- 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。同じ識別子を持つ IOC ファイルが存在した場合、タスクの実行結果に影響を与えることがあります。
- 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 ファイルをダウンロードします

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	"boolean string"、"restricted string"、"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： Content 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 ◦ Content フィールドでの演算子 TO の使用 本製品は、インジケーターが ISO 8601, Zulu time zone, UTC 形式で指定されている場合、date と duration のデータ種別の解釈に対応しています。

オブジェクトの実行防止

Detection and Response ソリューションと連携すると、脅威対応処理の一環として、Kaspersky Endpoint Security は実行ファイルとスクリプトの実行、およびデバイス上の Office アプリケーションファイルを開くことを制御できます。オブジェクトの実行防止は、オフィスアプリケーションの特定のファイル拡張子と特定のスクリプトインタープリターセットに対応しています。オブジェクトの起動をブロックすることで、脅威の拡散を阻止できます。

オブジェクト実行防止は実行防止ルールに基づいています。*実行防止ルール*は、Kaspersky Endpoint Security セキュリティ製品がオブジェクトの実行に応答する際に考慮する一連の基準です。本製品は、オブジェクトが実行防止ルールのすべての基準を満たしている場合にのみ、オブジェクトの実行をブロックします。本製品は、パスや MD5 または SHA256 ハッシュアルゴリズムで計算されたチェックサムからファイルを識別します。

実行防止機能は、以下の条件のいずれかが満たされている場合に、Kaspersky Endpoint Security セキュリティ製品で利用できます：

- Kaspersky Endpoint Security が Kaspersky Endpoint Detection and Response Optimum ソリューションと連携すると、EDR Optimum コンポーネントがアクティベートされます。
- Kaspersky Endpoint Security アプリケーションと Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) コンポーネントとの連携が有効になり、EDR Expert（オンプレミス）コンポーネントがアクティベートされます。

ファイル操作傍受のブロックモードが有効でない場合、設定されている動作モードに関係なく、実行防止は通知モードで動作します。

オブジェクトの実行防止は既定で無効になっています。

オブジェクトの実行防止を有効にすると、OS 内のアプリケーションの起動速度に影響する可能性があります。

オブジェクト実行防止を機能させるには、実行防止ルールを有効にする必要があります。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) と連携する場合のオブジェクト実行防止に関する特別な考慮事項

Kaspersky Endpoint Security アプリケーションが Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) と連携している場合、本製品は *EDR Expert（オンプレミス）コンポーネントの実行防止ルール*を使用します。本製品は、Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) からこれらのルールを取得します。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) と連携している場合、以下のことが可能です：

- Web コンソール、管理コンソール、またはコマンドラインで、EDR Expert（オンプレミス）コンポーネントのオブジェクト実行防止ルールの適用を有効または無効にします。

  実行防止ルールがトリガーされると、Kaspersky Endpoint Security は Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Anti Targeted Attack Platform にレポートを送信します。詳細については、関連する解決策のヘルプを参照してください。

- コマンドラインで EDR Expert（オンプレミス）コンポーネントのオブジェクト実行防止ルールのリストを表示します。

Kaspersky Endpoint Detection and Response Optimum と連携した場合のオブジェクト実行防止に関する特別な考慮事項

Kaspersky Endpoint Security が Kaspersky Endpoint Detection and Response Optimum ソリューションと連携している場合、本製品は *EDR Optimum コンポーネントのオブジェクト実行防止ルール*を使用します。これらのルールは、Web コンソールで手動で作成できます。アラートの詳細ウィンドウで実行防止ルールを自動的に作成することもできます。

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 コンソールまたはコマンドラインで、EDR Optimum コンポーネントのオブジェクト実行防止ルールの適用を有効または無効にします。

- Web コンソールでオブジェクトの EDR Optimum 実行防止ルールを作成および設定します。

  アラート詳細ウィンドウでファイルの実行を防止することによって、オブジェクトの実行防止ルールを自動的に作成することもできます。実行防止ルールは、デバイスが属する管理グループのポリシーに追加されます。

  > デバイスにポリシーが適用されている場合にのみ、アラート詳細ウィンドウでファイルの実行を実行防止することができます。

- EDR Optimum コンポーネントのオブジェクト実行防止ルールのリストをコマンドラインで表示します。

Kaspersky Endpoint Detection and Response Optimum と連携すると、オブジェクト実行防止は次の 2 つのモードのいずれかで動作します。

- **ブロック**：このモードでは、アプリケーションは、防止ルールの基準を満たすオブジェクトの実行またはドキュメントの開封をブロックし、オブジェクトの実行またはドキュメントの開封の試行に関するイベントをログに記録します。

  Kaspersky Endpoint Security アプリケーションは、実行防止ルールによって禁止されているスクリプトの実行を、許可されたスクリプトによってインポートされた場合でもブロックします。

- **通知する**。このモードでは、アプリケーションは、防止ルールの基準を満たす実行可能オブジェクトの実行やドキュメントの開封の試行に関するイベントをログに記録しますが、実際にそれらの実行やオープンをブロックすることはありません。既定ではこのモードが選択されます。

オブジェクトの実行防止の制限

オブジェクト実行防止ルールには次の制限が適用されます：

- Kaspersky Endpoint Security アプリケーションは、起動されるまで、実行防止ルールで指定されたオブジェクトをブロックしません。
- Kaspersky Endpoint Security アプリケーションは、防止ルールが作成または変更される前に開かれたファイルをブロックしません。
- Kaspersky Endpoint Security は、実行防止ルールがこれらのオブジェクトをカバーするように作成または変更される前に実行された、実行防止ルールの対象となるオブジェクトをブロックしません。
- 一部のファイルは、オペレーティングシステムとアプリケーションの動作にとって非常に重要になる場合があります。このようなファイルの実行を防止すると、システムの動作が中断される可能性があります。
- システムが不安定になる可能性があるため、50000 を超える実行防止ルールを作成することは推奨しません。

Web コンソールでのオブジェクトの実行防止の設定

オブジェクトの実行防止（EDR Expert（オンプレミス））の設定

Kaspersky Endpoint Detection and Response Expert（オンプレミス）ソリューションまたは Kaspersky Endpoint Detection and Response (KATA) コンポーネントとの連携が有効な場合、ポリシーのプロパティ（**製品設定 → 組み込みエージェントの設定 → Endpoint Detection and Response Expert（オンプレミス）**）でオブジェクトの実行防止を有効または無効にできます。

［**実行防止**］トグルスイッチは、オブジェクトの実行防止のための EDR Expert（オンプレミス）ルールを有効または無効にします。

オブジェクトに対する EDR Optimum の最適な実行防止の設定。

Kaspersky Endpoint Detection and Response Optimum との連携を有効にした場合、オブジェクト実行防止を有効または無効にしたり、EDR Optimum コンポーネントのオブジェクト実行防止ルールを設定したりできます：

- ポリシーのプロパティ（**製品設定 → 組み込みエージェントの設定 → Endpoint Detection and Response**）で。
- 管理対象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 → **アプリケーション**タブ → <Kaspersky Endpoint Security アプリケーション名>リンク → **製品設定**タブ → **Detection and Response**セクション → **Endpoint Detection and Response Optimum**）。

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オブジェクト実行防止を有効または無効にすることはできません。

デバイスのプロパティのオブジェクト設定に対する EDR Optimum 実行防止

設定	説明
オブジェクトの実行防止が有効/無効	オブジェクトの実行防止のための EDR Optimum ルールを有効または無効にします。 既定では、ルールは適用されません。
オブジェクトを開いた時または開始したときの処理	オブジェクト実行防止のモードを選択できます。 • **ブロック**：このモードでは、アプリケーションは、防止ルールの基準を満たすオブジェクトの実行またはドキュメントの開封をブロックし、オブジェクトの実行またはイベントログにドキュメントの開封の試行に関するイベントのログを」記録します。 • **通知する**。このモードでは、アプリケーションはイベントログに防止ルールの基準を満たす実行可能オブジェクトの実行やドキュメントの開封の試行に関するイベントのログを記録しますが、実際にそれらの実行やオープンをブロックすることはありません。既定ではこのモードが選択されます。
オブジェクト実行防止ルールのリスト。	［**追加**］リンクをクリックすると、EDR Optimum コンポーネントのオブジェクト実行防止ルールを設定できるウィンドウが開きます。 必要に応じて、［**削除**］を使用してリストからルールを削除できます。

デバイスのプロパティの EDR Optimum コンポーネントのオブジェクト実行防止ルールのリストにルールを追加する場合：

1. 実行防止ルールのリストの上にある［**追加**］をクリックします。
2. ウィンドウが開きます。そのウィンドウで、実行防止ルールの名前を入力します。
3. スイッチを適切な位置に設定して、実行防止ルールのステータスを指定します：
   - **有効**とは、ルールが有効であり、アプリケーションがこのルールを適用することを意味します。
   - **無効**とは、ルールが無効であり、アプリケーションによって使用されないことを意味します。

作成したルールはいつでも有効または無効にできます。

4. ［**種別**］ドロップダウンリストで、ブロックしたいオブジェクトを選択します。

   - **実行ファイル**。
   - **スクリプト**。
   - **Office アプリケーションファイル**。

   間違ったオブジェクトタイプを選択した場合、アプリケーションはファイルまたはスクリプトをブロックできなくなります。

5. オブジェクトを追加するには、オブジェクトへのパスおよびオブジェクトのチェックサムを指定します。

   オブジェクトへのパスを指定するには、［**パスを使用する**］を選択し、オブジェクトへのパスを入力します。

   オブジェクトのチェックサムを指定するには、**SHA256** または **MD5** オプションを選択し、オブジェクトのチェックサムを入力します。

6. ［**OK**］をクリックします。

   作成されたルールは、［**オブジェクトの実行防止**］設定ブロックのルールリストに追加されます。

管理コンソールでのオブジェクト実行防止の設定

Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) との連携が有効になっている場合のみ、管理コンソールでオブジェクトの実行防止を有効または無効にすることができます。

ポリシーのプロパティで、オブジェクトの実行防止を有効または無効にできます（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（［**製品設定**］ → ［**Detection and Response**］ → ［**EDR Expert（オンプレミス）**］）。

［**実行防止**］の下の［**オブジェクトの実行防止を有効にする**］は、EDR Expert（オンプレミス）コンポーネントの実行防止ルールを有効または無効にします。

コマンドラインでのオブジェクトの実行防止の管理

コマンドラインでは、次の事前定義済みタスクを使用して、オブジェクトの実行防止ルールの適用を開始または停止できます。

- *オブジェクトの実行防止（EDR Expert（オンプレミス））*(*KATAEDR_Prevention*)。
- *オブジェクトの実行防止 (EDR Optimum)*(*EDRO_Prevention*)。

既定では、*オブジェクトの実行防止（EDR Expert（オンプレミス））*および*オブジェクトの実行防止 (EDR Optimum)* タスクは開始されません。このタスクは、手動で開始および停止できます。

*［オブジェクトの実行防止（EDR Expert（オンプレミス））］*タスクは、Kaspersky Endpoint Detection and Response Expert（オンプレミス）または Kaspersky Endpoint Detection and Response (KATA) との連携が有効になっている場合にのみ実行できます。

Kaspersky Endpoint Detection and Response Optimum との整合性が有効になっている場合にのみ、オブジェクトの実行防止 (EDR Optimum) タスクを実行できます。

オブジェクト実行防止ルール管理コマンドを使用して、EDR Expert（オンプレミス）および EDR Optimum コンポーネントのオブジェクト実行防止ルールのリストを表示できます。

EDR Expert（オンプレミス）実行防止ル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 [-T] --get-prevention-state --kata
```

EDR Optimum オブジェクト実行防止ル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 [-T] --get-prevention-state --edro
```

Cloud Sandbox

Cloud Sandbox テクノロジーにより、デバイス上の高度な脅威を検出できます。Kaspersky Endpoint Security アプリケーションは、検出されたファイルを分析のために Cloud Sandbox に自動的に送信します。Cloud Sandbox は、これらのファイルを隔離された環境で実行して悪意のあるアクティビティを検出し、これらのファイルの評判を判断します。これらのファイルに関する情報は、Kaspersky Security Network に送信されます。したがって、Cloud Sandbox が悪意のあるファイルを検出すると、Kaspersky Endpoint Security は、このファイルを検出したすべてのデバイスで脅威を排除するための処理を実行します。

Cloud Sandbox を機能させるには、Kaspersky Security Network の使用を有効にする必要があります。

Kaspersky Private Security Network を使用している場合、Cloud Sandbox テクノロジーは利用できません。

Cloud Sandbox テクノロジーは常に有効になっており、本製品で使用しているライセンスの種別に関係なく、Kaspersky Security Network のすべてのユーザーが利用できます。

Kaspersky Endpoint Detection and Response Optimum ソリューションを導入している場合は、Cloud Sandbox を使用して検出された脅威に対して、Web コンソールで別のカウンターを有効にすることができます：

- ポリシーのプロパティ（**製品設定 → 組み込みエージェントの設定 → Endpoint Detection and Response**）
- 管理対象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 → **アプリケーション**タブ → <Kaspersky Endpoint Security アプリケーション名>リンク → **製品設定**タブ → **Detection and Response**セクション → **Endpoint Detection and Response Optimum**）。

Cloud Sandbox によって検出された脅威のカウンターも GUI レポートに表示されます。このカウンターを使用して、検出された脅威を分析するときに統計を収集できます。

デバイスのプロパティの Web コンソールで Cloud Sandbox カウンターを有効にします：

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）** → **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. 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済みのアプリケーションのリストで、［Kaspersky Endpoint Security］をクリックします。

6. 開いたアプリケーションプロパティウィンドウで、［**製品設定**］タブで、［**Detection and Response**］→［**Endpoint Detection and Response Optimum**］リンクを選択します。

7. 開いたウィンドウの **[Cloud Sandbox]** で、**[Cloud Sandbox]** トグルスイッチを有効にします。

8. ［**OK**］をクリックします。

Kaspersky Unified Monitoring and Analysis Platform との連携

Kaspersky Endpoint Security は、Kaspersky Unified Monitoring and Analysis Platform ソリューション（以下、KUMA）と互換性があります。

Kaspersky Unified Monitoring and Analysis Platform は、次の機能を提供する包括的なソフトウェアソリューションです。

- 情報セキュリティイベント（テレメトリ）の受信、処理、および保存。
- 受信データの分析と相関。
- 取得したイベント内の検索。
- 情報セキュリティの脅威の兆候を検出した場合の通知の作成。

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

Kaspersky Unified Monitoring and Analysis Platform と連携すると、Kaspersky Endpoint Security を実行しているデバイスは KUMA サーバーとの暗号化された接続を確立します。安全な接続を実現するため、KUMA サーバーが発行する次の証明書を使用しています：

- KUMA 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 Unified Monitoring and Analysis Platform との連携を有効にする前に、KUMA 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、相互認証を使用した接続の追加保護に使用されます（Kaspersky Endpoint Security KUMA 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、KUMA 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 Unified Monitoring and Analysis 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 Unified Monitoring and Analysis Platform 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。

KUMA サーバーへの接続を保護するための証明書は、Kaspersky Unified Monitoring and Analysis Platform の管理者によって提供されます。

Kaspersky Endpoint Security の製品全般設定で、プロキシサーバーの使用が設定されている場合、KUMA 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 Unified Monitoring and Analysis Platform の連会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。

- KUMA サーバー接続の全般設定を構成します。

- KUMA サーバー証明書を追加または削除します。

- KUMA 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。

- イベント転送設定を管理します。

Kaspersky Unified Monitoring and Analysis Platform との連携を有効にする前に、次のいずれかの条件が満たされていることを確認してください：

- Kaspersky Endpoint Security は、Kaspersky Unified Monitoring and Analysis Platform の機能も対象とするライセンスに基づいて使用されています。

- Kaspersky Unified Monitoring and Analysis Platform 機能のライセンスを別途購入し、追加機能のライセンス（KUMA ライセンス）を本製品に追加しました。

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 にライセンスを追加することで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。

Webコンソールで KUMA 連携の設定

Web コンソールでは、ポリシーのプロパティ（**製品設定 → 組み込みエージェントの設定 → KUMA 連携**）で Kaspersky Unified Monitoring and Analysis Platform との連携設定を管理できます。

管理コンソールで KUMA 連携の設定

管理コンソールでは、Kaspersky Endpoint Security と Kaspersky Unified Monitoring and Analysis Platform の連携を有効または無効にしたり、ポリシーのプロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**KUMA 連携 → KUMA 連携**）で連携設定を管理したりできます。

Kaspersky Unified Monitoring and Analysis Platform との連携設定

設定	説明
KUMA 連携を有効にする	Kaspersky Endpoint Security アプリケーションと Kaspersky Unified Monitoring and Analysis Platform ソリューションの連携を有効または無効にします。 KUMA 連携は、既定でオフになっています。
暗号化された接続を使用する	このチェックボックスをオンにすると、KUMA サーバーへの接続をさらに保護するためにサーバー証明書の検証が有効または無効になります。 サーバー証明書を検証するには、このチェックボックスをオンにして、［**KUMA サーバー**］ウィンドウでサーバー証明書を追加する必要があります。 既定では、このチェックボックスはオフです。
KUMA サーバー	**設定**ボタンをクリックすると **KUMA サーバー**ウィンドウが開きます。このウィンドウでは、KUMA 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。
KUMA サーバー接続設定	**設定**ボタンをクリックすると、KUMA 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、KUMA 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**サーバー接続設定**ウィンドウが開きます。
イベント送信時の最大遅延（秒）	KUMA 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：`30`。

［KUMA サーバー］ウィンドウ

ウィンドウ内の表には KUMA 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。接続が設定されている各サーバーについて、表には次の内容が示されます：

- 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）。［**KUMA 連携設定**］ウィンドウで［暗号化された接続を使用する］チェックボックスをオンにした場合は、KUMA を使用するライセンスを購入したときに受け取った証明書からサーバーの完全修飾ドメイン名（FQDN）を指定する必要があります。
- KUMA サーバーに接続するためのポート。
- KUMA サーバーに接続するために使用するプロトコル。

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：

- KUMA 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

［KUMA サーバー］ウインドウ

このウィンドウでは、KUMA サーバーの接続設定を指定できます。

KUMA サーバー接続設定

設定	説明
アドレス	KUMA 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。［**KUMA 連携設定**］ウィンドウで［暗号化された接続を使用する］チェックボックスをオンにした場合は、KUMA を使用するライセンスを購入したときに受け取った証明書からサーバーの完全修飾ドメイン名（FQDN）を指定する必要があります。
ポート	KUMA サーバーに接続するためのポート。 既定値：443。
Protocol	KUMA サーバーに接続するためのプロトコル：TCP または UDP。 UDP プロトコルを選択した場合、接続保護を提供する証明書の使用には対応しておらず、KUMA サーバーへの接続に関するイベントは発生しません。 既定は TCP です。

［KUMA サーバー接続設定］ウィンドウ

このウィンドウでは、KUMA サーバーに接続するための全般設定を設定できます。

KUMA サーバー接続設定

設定	説明
サーバーとの接続を待つ時間（秒）	KUMA サーバーへの接続を待つ最大時間（秒）。 既定値：5。
サーバー証明書	このセクションには、サーバー証明書を追加または削除するためのボタンが含まれています。
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。
追加接続保護	このセクションには、相互認証を使用して接続の追加セキュリティを構成するためのコントロールが含まれています。
相互認証を使用する	このチェックボックスをオンにすると、KUMA サーバーへの接続をさらに保護するために相互認証を使用するが有効または無効になります。 相互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。 KUMA 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**	KUMA サーバーとの接続のセキュリティのための［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、KUMA 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［**相互認証を使用する**］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。
相互認証を使用する	KUMA サーバーへの接続をさらに安全にするために、相互認証を使用するをオンまたはオフにします。 相互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。 KUMA 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。

［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 KUMA 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を追加する］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 KUMA サーバーとの接続をよりセキュアにできます。

接続用の追加保護を設定する場合、KUMA サーバー側でクライアント証明書の認証を有効にし、［**KUMA サーバー接続設定**］ウィンドウで［**相互認証を使用する**］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、［**暗号化されたコンテナのパスワード**］フィールドにパスワードを入力します。

コマンドラインで MDR 連携の設定

コマンドラインでは、事前定義済みタスク［*Kaspersky Unified Monitoring and Analysis Platformの連携*］を使用して、Kaspersky Endpoint Security と Kaspersky Unified Monitoring and Analysis Platform の連携を管理できます。

既定では、［*Kaspersky Unified Monitoring and Analysis Platform の連携*］タスクは実行されていません。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 Unified Monitoring and Analysis Platform の連携設定を構成できます。

Kaspersky Unified Monitoring and Analysis Platform との連携の設定を管理するコマンドを使用して、KUMA サーバーへの接続に使用する証明書を管理できます。

Kaspersky Unified Monitoring and Analysis Platform 統合タスク設定

この表では、*Kaspersky Unified Monitoring and Analysis Platform 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。

設定	説明	値
`UseTls`	KUMA サーバーへの接続をさらに保護するために、サーバー証明書の検証を有効または無効にします。	`Yes` - KUMA サーバーとの接続をさらに安全にするために、証明書を使用します。 `No`（既定）- KUMA サーバーへの接続を保護するために証明書を使用しません。
`UseClientCertificate`	KUMA 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。 KUMA サーバー側でクライアント証明書の検証が有効になっている場合は、 Kaspersky Unified Monitoring and Analysis Platform の連携タスクを開始する前に、クライアント証明書の使用を有効にし、クライアント証明書を追加します。	`Yes` – KUMA サーバーとの接続をさらに安全にするために、双方向認証を使用します。 `No`（既定値）– 双方向認証は使用しません。
`ConnectionTimeout`	KUMA サーバーへの接続を待つ最大時間（秒）。	既定値：`5`。
[Servers.item_#] セクションには、KUMA サーバーの設定が含まれています。		
`ServerAddress`	KUMA 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。 `UseTls=Yes` を設定する場合は、KUMA を使用するライセンスを購入したときに受け取った証明書からサーバーの完全修飾ドメイン名 (FQDN) を指定する必要があります。	既定値：`127.0.0.1`。
`ServerPort`	KUMA サーバーに接続するためのポート。	既定値：`443`。
`ServerProtocol`	KUMA サーバーに接続するためのプロトコル。	`tcp`（既定値）- TCP プロトコルを使用して KUMA サーバーに接続します。 `udp` - UDP プロトコルを使用して KUMA サーバーに接続します。 UDP プロトコルを選択した場合、接続保護を提供するための証明書の使用はサポートされません（`UseTls`、`UseClientCertificate`、および `ConnectionTimeout` 設定の値は無視されます）。また、KUMA サーバーへの接続に関するイベントはありません。
[SiemTransferSettings] セクションには、KUMA サーバーにイベントを送信するための設定が含まれています。		
`EventTransferTimeMax`	KUMA 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：`30`。

KUMA サーバーに接続するための証明書の管理

UDP プロトコルを選択した場合、接続保護を提供するための証明書の使用には対応していません。

証明書を管理するには、管理者 (admin) ロールを持つユーザーの権限が必要です。

コマンドを使用して、KUMA サーバーへの接続に使用される証明書を管理できます。証明書を使用すると、次の操作を実行できます：

- 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 [-M] --add-kuma-server-certificate <ファイルパス>
```

<ファイルパス>は、サーバー証明書を含む DER ファイルまたは PEM ファイルへのパスです。

クライアント証明書を追加または変更するには：

1. 次のコマンドを実行します：

   ```
   kesl-control [-M] --add-kuma-client-certificate <ファイルパス>
   ```

   <ファイルパス>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）へのパスです。

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。

KUMA サーバー設定でクライアント証明書の検証が有効になっており、*Kaspersky Unified Monitoring and Analysis Platform の連携*タスクの設定で `UseClientCertificate` が `yes` に設定されている場合、クライアント証明書は KUMA 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 [-M] --query-kuma-server-certificate
  ```

- クライアント証明書の場合：

  ```
  kesl-control [-M] --query-kuma-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
- 証明書の発行元
- 証明書の開始日
- 証明書の有効期限
- 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 [-M] --remove-kuma-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 [-M] --remove-kuma-client-certificate
```

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 が常時連携している必要があります。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のフラグメントを Protection Server に転送できず、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。

    インフラストラクチャに Linux ベースの高可用性 Integration Server のクラスターを展開する場合は、Integration Server に接続するためのアドレスおよびポートとして、ロードバランサーのアドレスおよびポートを指定する必要があります。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。
  - 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（**アプリケーション設定 → Light Agent モード**）で、Light Agent を SVM に接続するための設定を管理できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**Light Agent モード**）で、Light Agent の SVM 接続設定を管理できます。

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。

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 形式による 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」が指定されていた場合、Integration Server への接続はエラーで終了します。
ポート	Integration Server に接続するためのポート。 既定ではポート 7271 が指定されます。

インフラストラクチャに Linux ベースの高可用性 Integration Server のクラスターを展開する場合は、Integration Server に接続するためのアドレスおよびポートとして、ロードバランサーのアドレスおよびポートを指定する必要があります。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。

［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 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。 SVM の IP アドレス（IPv4 形式）または完全修飾ドメイン名（FQDN）を指定できるウィンドウを開くには、**追加** をクリックします。複数の SVM の IP アドレスまたは完全修飾ドメイン名を 1 行に 1 つずつ入力して入力できます。 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 は拡張 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［**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
接続タグを使用する	この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。 タグには 255 文字までのテキスト文字列を入力できます。［**;**］以外のすべての文字を使用できます。 このフィールドは、［**接続タグを使用する**］のチェックボックスがオンの場合に使用できます。

SVM 選択アルゴリズム

このウィンドウでは、Light Agent が使用する必要のある SVM 選択アルゴリズムを指定し、拡張 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。 接続に適したローカルの SVM が見つからない場合、Light Agent は、仮想インフラストラクチャ内の SVM の位置に関係なく、接続されている Light Agent の数が最も少ない SVM を選択します。 既定ではこのオプションが選択されます。
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。

設定	説明
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、Numa vServer、または Basis Dynamix Standard 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 プラットフォーム、VK Cloud（VK Private Cloud）、または TIONIX Cloud Platform 上で実行されてい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**：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、Numa vServer、または Basis Dynamix Standard 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 プロジェクトに導入されます（OpenStack プラットフォーム、VK Cloud（VK Private Cloud）、または TIONIX Cloud Platform 上で実行されてい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、Numa vServer、または Basis Dynamix Standard 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 プラットフォーム、VK Cloud（VK Private Cloud）、または TIONIX Cloud Platform 上で実行されている仮想インフラストラクチャ内）。 Light Agent のある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に接続可能な SVM がない場合、Light Agent は SVM に接続しません。 • **無視する**：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 は拡張 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**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 の間のデータ転送チャネルの暗号化が有効になっていることを確認します。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。

設定	説明
Light Agent と Protection Server との間のデータチャネルを暗号化する	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 との間に暗号化された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。 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、次のコマンドを実行します：

```
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。

- 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、次のコマンドを実行します：

```
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。

  > インフラストラクチャに Linux ベースの高可用性クラスターがある場合は、ロードバランサーのアドレスとポートが表示されます。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。

- 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 が使用する SVM 検出方法：Integration Server の使用または SVM アドレスのカスタムリストの使用。
- 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。拡張 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します。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、本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の成功や、修正が必要な製品コンポーネントのエラーについて通知する場合があります。

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 コンソールで操作

- コマンドラインで（コマンドラインでのイベントの表示、Kaspersky Security Center でのイベントの表示）

- 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する場合 – ポリシー プロパティまたはアプリケーションの一般設定で通知の表示が有効になっている場合は、ポップアップ通知で表示されます

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。

- Kaspersky Endpoint Security のグラフィカルユーザーインターフェイスには、アプリケーション、コンポーネント、およびタスクのレポートが表示されます。

レポートとイベントの内容

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
- アプリケーションカテゴリ名
- リポジトリの URL
- アプリケーションの実行ファイルのファイル名、パス、ハッシュ

ファイルパスにおける文字のエスケープルール

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）です。

`'\\\\'` は 2 文字（バックスラッシュ + バックスラッシュ）です。

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

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記録できます。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、OS ログへのイベントの記録は既定で無効になります。

Kaspersky Endpoint Security アプリケーションを標準モードまたは Endpoint Detection and Response Agent モードで使用し、Kaspersky Security Center を使用してアプリケーションを管理する場合、ライセンスの追加と削除、およびライセンスの有効期限に関する情報が、既定の OS ログに記録されます。アプリケーションに適用されているポリシーのプロパティで、OS ログに記録するイベントを選択できます。

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 → イベントの設定**）で、オペレーティングシステムログへのイベントログ記録を有効または無効にできます。

イベントの深刻度（緊急イベント、機能エラー、警告、情報メッセージ）の下にある［**設定**］をクリックすると、対応する深刻度のイベントのリストを含むウィンドウが開きます。各イベントについて、オペレーティングシステムのログへのログ記録を設定できます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**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、特定の深刻度のすべてのイベント種別（緊急イベント、機能エラー、警告、情報メッセージ）を選択することもできます。

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］パラメータが取り得る値は、次のとおりです：

- 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

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。

イベントログデータベースには、次のファイルが含まれています：

- イベントを含む複数のファイル。ファイルの数は、イベントログ内の現在のイベント数と、本製品が保存するように設定されているイベントの最大数（MaxEventsNumber 設定）によって異なります。

  イベントを含むファイルの名前には、シリアル番号が含まれます（例えば、events.db.0001）。ファイルがいっぱいになると、新しいファイルが作成されます。最も古いファイルを除くすべてのイベントファイル内のイベントの最大数が MaxEventsNumber 値に達した場合、最も古いファイルが削除されます。つまり、本製品は設定に示されているよりも多くのイベントを保存する場合があります。

- イベントログファイルに関する情報を格納する、イベントファイル管理用データベースのメインファイル。このファイルは削除できません。

次の製品イベントログのオプションは、製品全般設定を介して、コマンドラインから定義できます：

- EventsStoragePath の設定を使用して、製品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

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。

Kaspersky Endpoint Security アプリケーションのイベントは、深刻度に応じて次の種別に分類されます：

- *緊急イベント*は、デバイスのセキュリティに深刻な脅威をもたらします（悪意のあるオブジェクトの検知、脆弱性、アプリケーションの動作の問題）。緊急イベントにはすぐに対応する必要があります。緊急イベントの通知は、無効にしないことを推奨します。
- *機能エラー*は、本製品が正常に動作しない時（処理エラー、タスクの設定ミスなど）に発生します。このようなイベントは、デバイスのセキュリティに直接的な脅威を及ぼすことはありませんが、本製品が正しく動作するためには、ユーザーによる操作が必要となります。
- *警告*は、すぐに対応する必要はありませんが、デバイスのセキュリティに対して今後の潜在的な脅威となる可能性があります。
- *情報メッセージ*は、情報的な性質を持つイベントに相当します。

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 通知の使用に関する詳細については、Kaspersky Security Center のヘルプを参照してください。

コマンドラインでのイベントの表示

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、**and** 論理演算子を使用して結合された、**<フィールド> <比較演算子> '<値>'** 形式の 1 つ以上の論理式で設定します。

例：

TaskStateChanged イベントを表示します：

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

「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>]
```

ここで、**<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完全パスです。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` アプリケーションの全般設定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、`kesl-control -E` 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。

`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。

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>**には、クエリ結果を制限するために、 and 論理演算子を使用して結合された、**<フィールド> <比較演算> '<値>'** 形式の 1 つ以上の 論理式を指定します。
- **<数値>** は、表示する選択範囲内の最新イベントの数（選択範囲の末尾から数えたレコード数）です。
- `--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）。

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 <ファイルパス> [--json]
```

ここで、`--file <ファイルパス>`は、イベントの出力先となるファイルへの完全パスです。

グラフィカルユーザーインターフェイスでポップアップ通知の表示を設定する

既定では、本製品のグラフィカルインターフェイスでは、情報イベントがポップアップ通知に表示されます。管理コンソールまたはコマンドラインを使用して、ポップアップ通知を有効または無効にすることができます。

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（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**全般設定 → 製品設定**）で、グラフィカルインターフェイスでのポップアップ通知の表示を有効または無効にできます。

［**グラフィカルユーザーインターフェイスでポップアップ通知を表示する**］をオンにすると、グラフィカルユーザーインターフェイスにポップアップ通知が表示されます。

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設定

コマンドラインでは、［製品の全般設定］の `ShowPopUpNotifications` 設定を使用して、グラフィカルユーザーインターフェイスでのポップアップ通知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。

［`ShowPopUpNotifications`］パラメータが取り得る値は、次のとおりです：

- `Yes`（既定値）– グラフィカルユーザーインターフェイスでポップアップ通知を表示します。
- `No` – グラフィカルユーザーインターフェイスでポップアップ通知を表示しません。

グラフィカルインターフェイスを使用したアプリケーションの管理

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、グラフィカルインターフェイスでは対応していません。

Kaspersky Endpoint Security グラフィカルインターフェイスを使用して、次の操作を実行できます：

- 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
  - ファイアウォール管理。
  - アンチクリプター。
  - リムーバブルドライブスキャン。
  - ウェブ脅威対策
  - メール脅威対策
  - デバイスコントロール
  - ネットワーク脅威対策
  - 有害 USB 攻撃ブロック
  - ふるまい検知
  - 脆弱性攻撃ブロック
  - アプリケーションコントロール
  - ウェブコントロール
  - 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。
- 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。

- アップデートおよびロールバックタスクの開始と停止。
- サンドボックスでスキャンするファイルまたはディレクトリを送信。
- Kaspersky Security Network を有効化または無効化。
- 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。
- 組織のローカルネットワークの管理者に対する、ブロックされたデバイスへの一時アクセスの要求と取得。
- アプリケーションの統計とレポートを表示。
- 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。

アプリケーションが EDR Agent モードで使用されている場合、使用できるアプリケーションコンポーネントとタスクは一部に限定されます。特定の保護コンポーネントの管理、アプリケーションのアクティベーション、定義データベースのアップデートを実行できます。EDR Agent モードに固有の事項の詳細については、「既知の問題と制限事項」の記事を参照してください。

製品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、製品インターフェイスには、そのコンポーネントまたはタスクに対して*「通知のみ」モードが選択された*という警告が表示されます。

グラフィカルインターフェイス

通知領域の製品アイコン

トレイの Kaspersky Endpoint Security アイコンを使用すると、アプリケーションのグラフィカルインターフェイスのコンテキストメニューとメインウィンドウにアクセスできます。

一部の OS では、製品グラフィカルインターフェイスパッケージをインストールした後に、既定の製品アイコンがなくなる場合があります。

製品アイコンのコンテキストメニューには、次の項目があります：

- **Kaspersky Endpoint Security 12.4 for Linux**。本製品のグラフィカルインターフェイスの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**：グラフィカルインターフェイスを終了します。

本製品のグラフィカルインターフェイスのメインウィンドウ

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：

- 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。
- 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。

本製品のメイングラフィカルインターフェイスウィンドウは、いくつかの部分に分かれています。

- 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。[**表示**]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**]では、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。ここをクリックすると、[**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**]では、*アップデートタスク*のステータスが表示されます。ここをクリックすると、[**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**]ボタン。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。
  - **一時アクセス**ボタン。このボタンをクリックすると、**一時アクセス**ウィンドウが開き、ここでブロックされたデバイスへの一時アクセスを要求して取得できます。
  - [**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、製品情報を表示したり、アプリケーショントレースファイルを作成したりできます。
- 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、製品をアクティベートするために使用する必要のあ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。

グラフィカルインターフェイスを管理するには、管理者 (admin) ロールの権限が必要です。グラフィカルインターフェイスの一部は、他のロールを持つユーザーには使用できない場合があります。

製品コンポーネントの有効化または無効化

グラフィカルインターフェイスのトグルスイッチを使用して、製品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。

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。

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. アプリケーショングラフィカルインターフェイスの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. 該当するコンポーネントのトグルスイッチを有効または無効にします。

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. アプリケーショングラフィカルインターフェイスのメインウィンドウを開きます。
2. メインウィンドウで、［**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。

オブジェクトスキャンとサンドボックススキャンの開始

グラフィカルインターフェイスを使用して、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。

ファイルまたはディレクトリのオブジェクトスキャンを実行します：

1. スキャンするファイルまたはディレクトリを右クリックしてコンテキストメニューを開きます。
2. ファイルまたはディレクトリをスキャンするアプリケーションとして、**Kaspersky Endpoint Security 12.4 for Linux** を選択します。

   デスクトップ環境によっては、コンテキストメニューコマンドの名前が異なる場合があります。

オブジェクトスキャンタスクとその進行状況は、グラフィカルインターフェイスに表示されます。

Kaspersky Endpoint Security アプリケーションとサンドボックスコンポーネントの連携が有効になっている場合は、グラフィカルインターフェイスを使用して、スキャンするファイルまたはディレクトリをサンドボックスに送信できます。

ファイルまたはディレクトリをサンドボックスに送信してスキャンします：

1. スキャン用に送信するファイルまたはディレクトリを右クリックしてコンテキストメニューを開きます。
2. ファイルまたはディレクトリをスキャンするアプリケーションとして、**Kaspersky Endpoint Security 12.4 for Linux** を選択します。

   デスクトップ環境によっては、コンテキストメニューコマンドの名前が異なる場合があります。
3. 開いたウィンドウで、［**スキャン用にサンドボックスに送信する**］を選択してスキャンします。

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、次の手順を実行します：

1. アプリケーショングラフィカルインターフェイスの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. アプリケーショングラフィカルインターフェイスの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

グラフィカルインターフェイスを使用して、Kaspersky Security Network を有効または無効にできます。

Kaspersky Security Network の使用を有効にします：

1. アプリケーショングラフィカルインターフェイスの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. アプリケーショングラフィカルインターフェイスの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. ［**有効化**］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

グラフィカルインターフェイスを使用して、製品コンポーネントとタスクのレポートを表示できます。レポートは、本製品のグラフィカルインターフェイス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。

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*
- *Error*

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
  - メール脅威対策
  - ネットワーク脅威対策
  - 有害 USB 攻撃ブロック

- 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
- 脆弱性攻撃ブロック
- システム変更監視
- ウェブコントロール

- **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タス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。
- **実行防止** このレポートには、EDR Expert（オンプレミス）および EDR Optimum コンポーネントによるオブジェクト実行防止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。

レポートを表示します：

1. アプリケーショングラフィカルインターフェイスの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. イベントの詳細な情報を表示するには、レポート内の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。

レポートを処理しやすくするために、データの表示方法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。
- 検索機能を使用して、具体的なイベントを検索する。
- 選択したイベントをセクションごとに表示する。

Backup オブジェクトの表示

グラフィカルインターフェイスを使用して、バックアップ内のオブジェクトに対して次の操作を実行できます：

- 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。

バックアップにあるオブジェクトを表示するには：

1. アプリケーショングラフィカルインターフェイスの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。
- オブジェクトの完全パス。
- 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、本製品が使用されているライセンスと、そのライセンスに関連付けられたライセンスキーに関する情報を表示します。

保護対象デバイスで Kaspersky Endpoint Security アプリケーションをアクティベートするには、アプリケーションにメインライセンスを追加する必要があります。

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にするプロセスです。

本製品に使用しているメインライセンスで、必要な Kaspersky Endpoint Security の追加機能が対象でない場合は、追加機能を有効化するためにライセンスも追加する必要があります。

- Kaspersky EDR Optimum コンポーネントを有効にするための別のライセンス「Kaspersky Endpoint Detection and Response Optimum Add-on」（以下、「EDR Optimum ライセンス」とも表記）。
- Kaspersky Unified Monitoring and Analysis Platform 機能を有効にするための別のライセンス「Kaspersky Unified Monitoring and Analysis Platform Add-on」（以下、「KUMA」とも表記）。
- MDR コンポーネント機能を有効にするための別の現在のライセンス「Kaspersky Managed Detection and Response Optimum/Expert Add-on」(以下、「MDR 現在のライセンス」とも呼ばれます)。

基本機能用の予備のライセンスと追加機能用の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

本製品がまだアクティベートされていない場合（現在のメインライセンスが追加されていない場合）は、製品版ライセンスまたは試用版ライセンスでアクティベートできます。

アプリケーションをアクティベートします：

1. アプリケーショングラフィカルインターフェイスのメインウィンドウを開きます。
2. 次のいずれかの手順を実行します：
   - 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**］ボタンをクリックし、開いた［**サポート**］ウィンドウで、［**ライセンス**］またはウィンドウの下部にある［**ライセンス**］リンクをクリックします。

   これにより、［**ライセンス**］ウィンドウが開きます。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. 製品版ライセンスでアプリケーションを有効化する場合：
   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、［**ライセンス情報ファイルの選択**］リンクをクリックしてファイル選択ウィンドウを開き、.key の拡張子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。
4. 試用版ライセンスで本製品をアクティベートする場合は、［**試用版ライセンス**］セクションの［**アクティベート**］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。

本製品をアクティベートした後、予備のメインライセンスを追加し、必要に応じて追加機能用の現在のライセンスと予備のライセンスを追加できます。予備のメインライセンスと追加機能のライセンスを追加する手順は同じです。

アプリケーションに追加機能を追加するために予備のメインライセンスを追加する場合：

1. アプリケーショングラフィカルインターフェイスのメインウィンドウを開きます。
2. 次のいずれかの手順を実行します：
   - 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**］ボタンをクリックし、開いた［**サポート**］ウィンドウで、［**ライセンス**］またはウィンドウの下部にある［**ライセンス**］リンクをクリックします。

   これにより、［**ライセンス**］ウィンドウが開きます。ウィンドウには、以前に追加されたライセンスに関する情報が表示されます。
3. ［**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、［**ライセンス情報ファイルの選択**］リンクをクリックしてファイル選択ウィンドウを開き、.key の拡張子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。
4. ［**追加**］をクリックします。

メインライセンスを追加し、本製品がすでにアクティベートされている場合、新しいライセンスは予備のメインライセンスとして追加されます。

追加機能用の別のライセンスを追加すると、その追加機能用のライセンスが以前に本製品に追加されていない限り、現在のライセンスとして追加されます。追加機能のライセンスがすでに本製品に追加されている場合、追加機能の新しいライセンスが予備のライセンスとして追加されます。

> 現在のライセンスと予備のライセンスの両方が以前に本製品に追加されていた場合、新しいライセンスが以前に追加された予備のライセンスに置き換えられます。

試用版のライセンスおよび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。

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. アプリケーショングラフィカルインターフェイスのメインウィンドウを開きます。
2. 次のいずれかの手順を実行します：
   - 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**］ボタンをクリックし、開いた［**サポート**］ウィンドウで、［**ライセンス**］またはウィンドウの下部にある［**ライセンス**］リンクをクリックします。

これにより、［**ライセンス**］ウィンドウが開きます。

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。

ライセンス情報の表示

ライセンスの情報を表示するには：

1. アプリケーショングラフィカルインターフェイスのメインウィンドウを開きます。

2. 次のいずれかの手順を実行します：

   - 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**］ボタンをクリックし、開いた［**サポート**］ウィンドウで、［**ライセンス**］またはウィンドウの下部にある［**ライセンス**］リンクをクリックします。

   これにより、［**ライセンス**］ウィンドウが開きます。

   ウィンドウには、本製品に追加された現在のライセンスと予備の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、追加された現在のライセンス（現在のメインライセンスと追加機能ライセンス）と、これら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：

- ライセンス種別、ライセンスの制限、およびライセンスの有効期間。
- **ライセンス** – 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** – ライセンスの有効期限が切れるまでの日数と終了日 (UTC)。
- **名前** – 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。

［**予備のライセンス**］セクションには、追加された予備のライセンス（予備のメインライセンスと追加機能ライセンス）とこれら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。
- **ライセンス** – 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。
- **名前** – 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。

デバイスへの一時的なアクセス許可

デバイスが接続され、そのデバイスへのアクセスがデバイスコントロールによって拒否された場合、デバイスへのアクセスがブロックされていることを示すメッセージのウィンドウが表示されます。

グラフィカルインターフェイスを使用して、組織のプライベートネットワーク管理者にブロックされたデバイスへの一時アクセスを要求できます。

- デバイスへのアクセスがブロックされていることを示すメッセージのウィンドウで **[OK]** をクリックします。
- アプリケーショングラフィカルインターフェイスのメインウィンドウから

ブロックされたデバイスへの一時アクセスを要求する場合：

1. アプリケーショングラフィカルインターフェイスの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［**一時アクセス**］をクリックします。
   これにより、［**一時アクセス**］ウィンドウが開きます。
   デバイスへのアクセスがブロックされていることを示すメッセージのウィンドウから **[OK]** をクリックして、［**一時アクセス**］ウィンドウを開くこともできます。
3. ［**ブロックされたデバイスへのアクセス要求**］セクションの接続済みデバイスリストから、アクセス権を酢得するデバイスを選択します。
4. ［**デバイスアクセス期間（時間）**］フィールドで、デバイスへのアクセスを許可する期間（時間単位）を指定します。
5. ［**アクセス要求ファイルの作成**］をクリックします。
6. 開いたウィンドウで、.akey 拡張子のアクセス要求ファイルを保存するディレクトリへのパスを指定します。
7. アクセス要求ファイルをメールや利用可能な任意の方法で管理者に送信します（管理者はブロックメッセージテンプレートでこれを設定できます）。

管理者からアクセスキーを取得したら、そのアクセスキーをアップロードしてブロックされたデバイスへの一時的なアクセスを取得できます。

ブロックされたデバイスへの一時アクセスを要求する場合：

1. アプリケーショングラフィカルインターフェイスの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［**一時アクセス**］をクリックします。
   これにより、［**一時アクセス**］ウィンドウが開きます。
3. ［**デバイスへのアクセスの取得**］セクションで、［**アップロードアクセスキー**］をクリックします。
4. 開いたウィンドウで、組織のプライベートネットワークの管理者から受け取ったデバイスアクセスキーを含むファイル（拡張子が .acode のファイル）を選択します。

5. アクセスが許可されたデバイスとアクセス期間に関する情報を示すウィンドウが表示されます。

6. ［**OK**］をクリックします。

製品に関する情報の表示

インストールされている本製品とデバイスに関する情報は、［**サポート**］ ウィンドウで表示できます。サポートウィンドウは、本製品のグラフィカルインターフェイスのメインウィンドウの下部にある［**サポート**］をクリックすると開きます。

［**サポート**］ウィンドウには次の情報が表示されます。

- 本ソフトウェアのバージョン。
- **ライセンス**は、本製品に追加された現在のメインライセンス、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を表示します。このフィールドのリンクは、［**ライセンス**］ウィンドウを開き、詳細なライセンスの情報を表示します。
- **ライセンスのステータス**は、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を表示します。
- **定義データベースの公開日時** – 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。
- **製品管理** – デバイスがポリシーによって管理されているかどうかに関する情報。

［ネットワークエージェント］ポリシーで［**アプリケーションがデバイス上のポリシーの拡張データを取得できるようにする**］が有効になっている場合、ウィンドウには、本製品がインストールされているデバイスに適用されているポリシーに関する次の情報も表示されます。

- **ポリシー名**は、本製品がインストールされているデバイスに適用されるポリシーの名前です。
- **適用日** – 本製品がインストールされたデバイスでポリシーが最後に適用または更新された日時。
- **管理グループ**は、本製品がインストールされ、ポリシーによって管理されるデバイスを含む管理グループの名前です。
- **現在のポリシープロファイル**は、デバイスに適用されている現在のポリシープロファイル（ある場合）のリストです。

［**サポート**］ウィンドウの下部に次のリンクが表示されます：

- **ライセンス**で［**ライセンス**］ウィンドウが開き、詳細なライセンス情報が表示されます。
- **お問い合わせ窓口**でお問い合わせ窓口ページが開きます。
- ［**サポート**］をクリックすると、Kaspersky CompanyAccount ページが開きます。

- **トレース**で［**トレース**］ウィンドウが開きます。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。

［**トレース**］をたどるには、管理者ロールの権限が必要です。

トレースファイルの作成

グラフィカルインターフェイスを使用して、製品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。

トレースファイルを作成し、その詳細レベルを設定するには、管理者ロール (admin) を持つユーザーが必要です。

トレースファイルを作成するには：

1. アプリケーショングラフィカルインターフェイスの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。

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。ハッカーは、アプリケーションの1つ以上の実行可能モジュールまたはファイルを、悪意のあるコードを含む別のファイルに置き換える可能性があります。このようなモジュールやファイルの置換を防ぐために、Kaspersky Endpoint Security はアプリケーションコンポーネントの整合性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の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 Web プラグイン
- Kaspersky Endpoint Security MMC 管理プラグイン

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。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。

Linux デバイス上で整合性チェックユーティリティを実行するには、root 権限を持つアカウントが必要です。Windows デバイス上で整合性チェックユーティリティを実行するには、管理者アカウントが必要です。

製品と一緒にインストールされる整合性チェックユーティリティは、次のパスにあります：

- アプリケーションパッケージ (integrity_checker) の一部として：/opt/kaspersky/kesl/bin/integrity_checker。
- Kaspersky Endpoint Security の MMC 管理プラグイン (integrity_checker.exe) の一部として：
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<バージョン番号>.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_<バージョン番号>.plg\integrity_checker.exe – 64 ビット OS の場合

マニフェストファイルは、以下のパスにあります：

- 製品パッケージの整合性をチェックする場合：/opt/kaspersky/kesl/bin/integrity_check.xml。
- グラフィカルユーザーインターフェイスパッケージの整合性をチェックする場合：/opt/kaspersky/kesl/bin/gui_integrity_check.xml。
- ネットワークエージェントをチェックする場合：
  - /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml – 32 ビット OS の場合
  - /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml – 64 ビット OS の場合
- Kaspersky Endpoint Security MMC 管理プラグインをチェックする場合：
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<プラグインのバージョン>.plg\integrity_check.xml – 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_check.xml – 64 ビット OS の場合
- Kaspersky Endpoint Security 管理 Web プラグインディレクトリをチェックする場合：
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\server\plugins\kesl_<バージョン番号>\integrity_check.xml – Windows OS を搭載したデバイスの場合
  - /var/opt/kaspersky/ksc-web-console/server/plugins/kesl_<バージョン番号>/integrity_check.xml – Linux OS を搭載したデバイスの場合

ソリューションコンポーネントの整合性をチェックするには、そのコンポーネントのツールのフォルダーからツールを実行する必要があります。

整合性チェックユーティリティを実行するには、次のいずれかのコマンドを実行します：

- パッケージのアプリケーションの整合性チェックを実行する場合：

  ```
  integrity_checker [<manifest ファイルへのパス>] --crl
  /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
  ```

- グラフィカルユーザーインターフェイスパッケージの整合性をチェックする場合：

  ```
  integrity_checker <manifest ファイルへのパス> --crl
  /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
  ```

- Kaspersky Endpoint Security MMC 管理プラグインの整合性をチェックする場合：

  ```
  integrity_checker.exe [<manifest ファイルへのパス>]
  ```

- ネットワークエージェントの整合性をチェックする場合：

  ```
  integrity_checker <manifest ファイルへのパス>
  ```

- Kaspersky Endpoint Security 管理 Web プラグインディレクトリの整合性をチェックする場合：

  ```
  integrity_checker <manifest ファイルへのパス> --crl
  /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds
  ```

  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>` は、証明書失効リストが含まれるディレクトリへのパスです。
- `--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の名前です。
- `--signature-type kds` は、チェックする署名の種別です（このオプションは、Kaspersky Endpoint Security 管理 Web プラグインのディレクトリをスキャンする場合に必要です）。
- `--signature-type kds-with-filename` は、チェックする署名の種別です（このオプションは、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チェックに必要です）。
- `--single-file <ファイル>` は、マニフェスト内の指定されたファイルのみをチェックし、マニフェストのその他すべてのオブジェクトを無視します。
- `--version` – ユーティリティのバージョンを表示し、整合性チェックを実行しません。

`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整合性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 で対応のイベントを生成します。

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ご連絡いただく前に、「カスペルスキーのサポートサービス規約」をお読みください。

テクニカルサポートへのご連絡方法は次のとおりです：

- 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します。

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については、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を作成

*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。

トレースファイルを保存するには、最小ハードウェア要件に記載されているディスク容量に加えて、ディスク容量が必要です。

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：

- イベントの日時
- 実行された脅威の数
- イベントを発生させたコンポーネント
- イベントの重大度（情報イベント、警告、緊急イベント、エラー）
- コンポーネントによるコマンド実行およびそのコマンドの実行結果を含むイベントの説明

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。
- アプリケーションのユーザーの活動に関するデータ。
- 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、OSMP サーバー、NDR (KATA) サーバー、およびサンドボックスとの対話を提供する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管理できます。

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 → テクニカルサポート**）でアプリケーショントレース設定を管理できます。

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でアプリケーショントレース設定を管理できます（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**セキュリティコントロール → 製品設定**）。

［**トレースとダンプの設定**］で、［**設定**］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および書き込み権限を持っていることを確認してください。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）	このフィールドでは、アプリケーションのトレース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。 既定値：500
トレースファイルの最大数	このフィールドでは、アプリケーションのトレースファイルの最大数を入力できます。 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、TraceLevel設定の TraceFolder、TraceMaxFileCount、TraceMaxFileSize、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、製品トレースファイルの作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（rwx-------- 700 件）に対して読み取り / 書き込み権限のみ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 の設定では、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 の設定では、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。

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

管理プラグインの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、管理 MMC 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。

管理 Web 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、管理 Web 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内容

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：

- イベントの日時
- 実行された脅威の数
- イベントを発生させたコンポーネント
- イベントの重大度（情報イベント、警告、緊急イベント、エラー）
- コンポーネントによるコマンド実行およびそのコマンドの実行結果を含むイベントの説明

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、ダンプが作成された時点での Kaspersky Endpoint Security プロセスのワーキングメモリに関するすべての情報が含まれています。

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。

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。

ダンプを有効にしている場合、既定では、ダンプファイルは次のディレクトリに保存されます：

- /var/opt/kaspersky/kesl/common/dumps（kesl プロセスのダンプファイル）
- /var/opt/kaspersky/kesl/common/dumps-user（ユーザープロセスのダンプファイル）

既定のダンプ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。kesl プロセスのダンプファイルを保存するための別のディレクトリを指定できます。別の ディレクトリを指定する場合は、このディレクトリに対する読み取りおよび書き込み権限を root ユーザーのみが持っていることを確認してください（`700` または `rwx--------` の権限）。

ダンプファイルを保存するには、最小ハードウェア要件に記載されているディスク容量に加えて、ディスク容量が必要です。

ダンプファイルは、本製品の使用中にコンピューターに保存されます。本製品が削除されると、トレースファイルは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。

ダンプファイル設定の管理

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ダンプファイル設定を管理できます。

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プファイル設定の管理

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 → テクニカルサポート**）で、本製品のダンプファイル設定を管理できます。

Web コンソール内ポリシープロパティのアプリケーションダンプファイル設定については、付録 5 で説明しています。

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プファイル設定の管理

管理コンソールでは、ポリシーのプロパティ（管理コンソールでのポリシーの管理、管理コンソールを使用したポリシーの作成）（**セキュリティコントロール → 製品設定**）で、本製品のダンプ設定を管理できます。

［**トレースとダンプの設定**］で［**設定**］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（次の表を参照）。

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。

コマンドラインでのダンプファイル設定の管理

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. **[General]** 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、<デバイス名> リンクをクリックします。
   デバイスのプロパティウィンドウが表示されます。
3. ［**詳細設定**］タブで、［**リモート診断**］セクションを選択します。

デバイスのリモート診断ウィンドウでは、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インストールログを表示するには、次の手順を実行します：

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インストールログを表示するには、次の手順を実行します：

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。

補足資料

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。

補足資料1：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 <コマンドグループ接頭辞>`

ここで、**<コマンドグループ接頭辞>**には次の値を指定できます：

- -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: 全般的なコンテナスキャン設定を管理するためのコマンド（コンテナスキャン、コンテナ監視）
- -D：デバイスコントロールを管理するコマンド
- -E: アプリケーションイベントを管理するためのコマンド（コマンドラインでのイベントの表示、Kaspersky Security Center でのイベントの表示）
- -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
- -J：システムパフォーマンスメトリックの取得を管理するためのコマンド
- -L：ライセンスを管理するコマンド
- -M：Kaspersky Endpoint Security アプリケーションと Kaspersky Unified Monitoring and Analysis Platform の連携の設定を管理するためのコマンド
- -N：ネットワークトラフィックのスキャン設定を管理するコマンド
- -Q：隔離を管理するためのコマンド
- -R：Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA)、Kaspersky Endpoint Detection and Response Expert（オンプレミス）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
- -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: イベント出力コマンド（コマンドラインでのイベントの表示、Kaspersky Security Center でのイベントの表示）
- -X：Kaspersky Endpoint Security と サンドボックスの連携の設定を管理するためのコマンド

製品のタスクと設定を管理するためのコマンド

接頭辞 -T は、そのコマンドが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属することを示します。

接頭辞 -C は、そのコマンドがコンテナスキャン設定（コンテナスキャン、コンテナ監視）を管理するためのコマンドグループに属することを示します。

接頭辞「-N」は、そのコマンドがネットワークトラフィックのスキャン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します。

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 <設定情報ファイルへのパス>] [--json]`

引数とライセンス

`--file <設定情報ファイルのパス>` は、アプリケーション設定を保存する設定情報ファイルの完全パスです。

`--json` を指定すると、設定は JSON 形式で出力されます。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

kesl-control --import-settings

このコマンドは、コンテナ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]`

引数とライセンス

`--file <設定情報ファイルのパス>` は、アプリケーションへの設定のインポート元となる設定情報ファイルの完全パスです。

`--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。`--json` オプション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。

本製品が Light Agent モードで使用されている場合、コマンドは実行できません。

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 <設定情報ファイルへのパス>] [--json]
```

引数とライセンス

`--file <設定情報ファイルのパス>` は、本製品の全般設定が書き込まれる設定情報ファイルのパスです。`--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。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

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 <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 [-T] --set-app-settings --file <設定情報ファイルへのパス> [--json]`

引数とライセンス

<設定名>=<設定値>は、本製品の全般設定のいずれかの名前と値です。

`--file` **<設定情報ファイルのパス>** は、アプリケーションへの設定のインポート元となる設定情報ファイルの完全パスです。

`--json` を指定すると、設定情報ファイルからアプリケーションに設定が JSON 形式でインポートされます。`--json` オプション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/名前> [--file <設定情報ファイルのパス>] [--json]`

引数とライセンス

<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>** は、タスク設定を書き込む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。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

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 ID/名前> <設定名>=<設定値> [<設定名>=<設定値>] [--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 ID/名前> --file <設定情報ファイルのパス> [--json]`

引数とライセンス

<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、いずれかのタスク設定の名前と値です。

`--add-path` **<パス>** は、スキャン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-path` **<パス>** は、スキャンするオブジェクトが含まれるディレクトリへのパスを削除します。

`--add-exclusion` **<パス>** は、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` **<パス>** は、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削除します。

`--file` **<設定情報ファイルのパス>** は、タスク設定のインポート元となる設定情報ファイルへの完全パスです。

`--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。`--json` オプション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/名前> --set-to-default`

引数とライセンス

< 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/名前 > [--file < 設定情報ファイルのパス >] [--json]`

引数とライセンス

< 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 >** は、タスクスケジュール設定を書き込む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。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

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/名前 > < 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 [-T] --set-schedule < タスク ID/名前 > --file < 設定情報ファイルのパス > [--json]`

引数とライセンス

< 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設定の 1 つの名前と値です。

`--file` **< 設定情報ファイルのパス >** は、タスクスケジュール設定のインポート元となる設定情報ファイルの完全パスです。

`--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。`--json` オプション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]
```

引数とライセンス

`--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]
```

引数とライセンス

<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 <タスク種別> [--file <設定情報ファイルへのパス>] [--json]

引数とライセンス

<タスク名> は、新しいタスクに指定する名前です。

<タスク種別> は、作成するタスクの種別を表します。

--file <設定情報ファイルへのパス> は、タスクの作成に使用される設定を含む設定情報ファイルへの完全パスです。

--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。--json オプション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>

引数とライセンス

<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]

引数とライセンス

<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]`

引数とライセンス

<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>`

引数とライセンス

<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>`

引数とライセンス

<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 <アクション>]`

引数とライセンス

<パス>は、スキャンするファイルまたは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 <アクション>` は、感染したオブジェクトに対して製品が実行するアクションです。`--action` オプションを指定しないと、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 <ID / 名前 [:タグ ]>
```

引数とライセンス

<ID / 名前 [: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。

オブジェクトの実行防止を管理するコマンド

kesl-control --get-prevention-state

このコマンドは、指定されたコンポーネントのオブジェクトの実行防止ルールを出力します。

コマンド構文

```
kesl-control [-T] --get-prevention-state [--kata|--edro]
```

引数とライセンス

`--kata`：EDR Expert（オンプレミス）コンポーネントの実行防止ルール

`--edro`：EDR Optimum コンポーネントの実行防止ルール

コンテナ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 <設定情報ファイルへのパス>] [--json]`

引数とライセンス

`--file <設定情報ファイルへのパス>` は、コンテナスキャンの全般設定が書き込ま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。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

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 <設定情報ファイルへのパス> [--json]`

引数とライセンス

<設定名>=<設定値> は、コンテナスキャンの全般設定のいずれかの名前と値です。

`--file <設定情報ファイルのパス>` は、設定情報ファイルの完全パスです。このファイルのコンテナ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、設定情報ファイルからアプリケーションに設定が JSON 形式でインポートされます。`--json` オプション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。

ネットワークトラフィックのスキャン設定を管理するコマンド

接頭辞「-N」は、そのコマンドがネットワークトラフィックのスキャン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します。

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、現在のネットワークトラフィックのスキャン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 [-N] --get-net-settings [--file <設定情報ファイルへのパス>] [--json]
```

引数とライセンス

`--file <設定情報ファイルのパス>` は、ネットワークトラフィックのスキャン設定が書き込ま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。`--json` オプションを指定しないと、設定は INI 形式で出力されます。

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、ネットワークトラフィックのスキャン設定を構成します。

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 <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 [-N] --set-net-settings --file <設定情報ファイルへのパス> [--json]
```

引数とライセンス

<設定名>=<設定値> は、ネットワークトラフィックのスキャン設定のいずれかの名前と値です。

`--file <設定情報ファイルのパス>` は、ネットワークトラフィックのスキャン設定をインポートする設定情報ファイルの完全パスです。

`--json` を指定すると、設定情報ファイルからアプリケーションに設定が JSON 形式でインポートされます。`--json` オプション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 --list-certificates

このコマンドは、信頼する root 証明書のリストを出力します。

コマンド構文

```
kesl-control [-N] --list-certificates
```

kesl-control --add-certificate

このコマンドは、信頼する root 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 <証明書へのパス>`

引数とライセンス

<証明書へのパス> は、追加する証明書ファイルのパスです（PEM または DER 形式）。

kesl-control --remove-certificate

このコマンドは、信頼する root 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 --add-bypass-endpoints

このコマンドを使用すると、トラフィック読み取りの除外リストを追加できます。

コマンド構文

`kesl-control [-N] --add-bypass-endpoints --direction <in|out> --remote-ip <リモート IP アドレス> --dst-port <宛先ポート>`

引数とライセンス

<in|out> は、除外された接続における通信方向（送信または受信）です。

<リモート IP アドレス> は、リモートデバイスの IPv4 または IPv6 アドレスです。受信トラフィックを読み取りから除外すると、指定された IP アドレスからのトラフィックが除外されます。送信トラフィックを読み取りから除外すると、指定された IP アドレスに送信されるトラフィックが除外されます。

<宛先ポート> は、保護対象デバイス上のポート（受信トラフィックの除外）またはリモートデバイス上のポート（送信トラフィックの除外）です。このポートへのトラフィックは読み取りから除外されます。

kesl-control --list-bypass-endpoints

このコマンドを使用すると、設定されたトラフィック読み取りの除外リストを表示できます。

コマンド構文

`kesl-control [-N] --list-bypass-endpoints`

kesl-control --remove-bypass-endpoints

このコマンドを使用すると、トラフィック読み取りの除外リストを削除できます。

コマンド構文

```
kesl-control [-N] --remove-bypass-endpoints --direction <in|out> --remote-ip <リモート IP アドレス> --dst-port <宛先ポート>
```

引数とライセンス

<in|out> は、除外された接続における通信方向（送信または受信）です。

<リモート IP アドレス> は、トラフィックがインターセプトから除外されるリモートデバイスの IPv4 または IPv6 アドレスです（トラフィックの方向によって異なります）。

<宛先ポート> は、保護対象デバイス上のポート（受信トラフィックの除外）またはリモートデバイス上のポート（送信トラフィックの除外）です。

統計コマンド

-S 接頭辞は、コマンドが統計情報コマンドグループに属することを示します。

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]
```

引数とライセンス

--json を指定すると、設定は JSON 形式で出力されます。

kesl-control --supported-tech-info

このコマンドは、製品機能のリスト、そのステータス（使用中または未使用）に関する製品情報、およびこれらの製品機能が実装されている Linux テクノロジーを表示します。

コマンド構文

```
kesl-control [-S] --supported-tech-info [--json]
```

引数とライセンス

`--json` – データを JSON 形式で出力します。

kesl-control --get-statistic

このコマンドを使用すると、アプリケーションの動作に関する統計情報とデバイス上で見つかったマウントポイントのリストを表示できます。

コマンド構文

```
kesl-control [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

引数とライセンス

`[--files]`：ファイル脅威対策コンポーネントによって最も頻繁にスキャンされるファイルに関する統計と、コンポーネントがこれらのファイルにアクセスする回数。

`[--processes]`：Kaspersky Endpoint Security によって最も頻繁に検出された開始処理の統計とその開始数。

> ふるまい検知コンポーネントによるスキャンからプロセスを除外しても、これらのプロセスは統計情報から削除されませんが、Kaspersky Endpoint Security アプリケーションのパフォーマンスが向上します。

`[--mountpoints]`：マウントポイントのリスト。出力では、マウントポイントへのパスは次のようにソートされます：

- 静的、システム、サービス、その他のマウントポイント
- 名前空間にマウントされたスナップパッケージとマウントポイント
- Docker コンテナ管理システムによって作成されたマウントポイント

1つ以上のオプションを任意の組み合わせで指定することも、オプションをまったく指定しないことも選択できます。オプションを指定しない場合、最も頻繁にスキャンされたファイルの統計、最も頻繁に開始された処理の統計、およびデバイス上で見つかったマウントポイントの リストの 3 つを表示します。

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>"]
```

引数とライセンス

<フィルター条件>には、特定の現在のイベントを出力するために、**and** 論理演算子を使用して結合された、**<フィールド> <比較演算> '<値>'** 形式の1つ以上の論理式を指定します。

製品イベントを管理するコマンド

「-E」は、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に、そのコマンドが属することを示す接頭辞です（コマンドラインでのイベントの表示、Kaspersky Security Center でのイベントの表示）。

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 <ファイルパス>] [--json] [--reverse]
```

引数とライセンス

< 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完全パスです。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 アプリケーションの全般設定によって決まります。

< フィルター条件 > には、クエリ結果を制限するために、 and 論理演算子を使用して結合された、**< フィールド > < 比較演算 > '< 値 >'** 形式の1つ以上の 論理式を指定します。

< 数値 > は、表示する選択範囲内の最新イベントの数（選択範囲の末尾から数えたレコード数）です。

--file **< ファイルパス >** は、イベントを出力するファイルへの完全パスです。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

接頭辞「-L」は、そのコマンドがライセンス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します。

ライセンスを追加または削除するコマンドは、本製品が基本モードまたは Endpoint Detection and Response Agent モードで実行されている場合にのみ使用できます。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。

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、アプリケーションのメインライセンスと追加機能の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へのパス >**

kesl-control [-L] --add-active-key **< アクティベーションコード >**

引数とライセンス

<ライセンス情報ファイルへのパス> は、ライセンス情報ファイルへのパスです。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> は、アクティベーションコードです。

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、アプリケーションのメインライセンスと追加機能の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へのパス>

kesl-control [-L] --add-reserve-key <アクティベーションコード>
```

引数とライセンス

<ライセンス情報ファイルへのパス> は、ライセンス情報ファイルへのパスです。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> は、アクティベーションコードです。

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]

kesl-control [-L] --remove-active-key [--kuma]
```

```
kesl-control [-L] --remove-active-key [--mdr]

kesl-control [-L] --remove-active-key [--edr-kata]
```

引数とライセンス

`--edr-optimum` – 現在の EDR Optimum ライセンスを削除します。

`--kuma –` – 現在の KUMA ライセンスを削除します。

`--mdr –` – 現在の MDR ライセンスを削除します。

`--edr-kata` – 現在の EDR Expert（オンプレミス）ライセンスを削除します。

コマンドラインで `--edr-optimum`、`--kuma`、`--mdr`、または `--edr-kata` オプションを指定しない場合、コマンドは本製品からプライマリの現在のライセンスを削除します。

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]

kesl-control [-L] --remove-reserve-key [--kuma]

kesl-control [-L] --remove-reserve-key [--mdr]

kesl-control [-L] --remove-reserve-key [--edr-kata]
```

引数とライセンス

`--edr-optimum` – 予備の EDR Optimum ライセンスを削除します。

`--kuma` – 予備の KUMA ライセンスを削除します。

`--mdr` – 予備の MDR ライセンスを削除します。

`--edr-kata` – 予備の EDR Expert（オンプレミス）ライセンスを削除します。

コマンドラインで `--edr-optimum`、`--kuma`、`--mdr`、または `--edr-kata` オプションを指定しない場合、コマンドは本製品からプライマリの予備のライセンスを削除します。

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]
```

引数とライセンス

`--json` – データを JSON 形式で出力します。

kesl-control --load-mdr-blob

`--load-mdr-blob` コマンドを使用すると、Kaspersky Managed Detection and Response との連携に使用できる BLOB ファイルをデバイスにアップロードできます。BLOB ファイルは、MDR 設定情報ファイルの ZIP 圧縮ファイル内にあります。

コマンド構文

```
kesl-control [-L] --load-mdr-blob <ファイルパス MDR BLOB>
```

kesl-control --remove-mdr-blob

`--remove-mdr-blob` コマンドを使用すると、Kaspersky Managed Detection and Response との連携に使用される BLOB ファイルをデバイスから削除できます。

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

接頭辞「-F」は、そのコマンドがFirewall管理コマンドに属していることを示します。

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 名>] [--action <処理>] [--protocol <プロトコル>] [--direction <通信方向>] [--remote <リモート アドレス>[:<ポート 範囲>]] [--local <ローカル アドレス>[:<ポート範囲>]] [--at <インデックス>]
```

引数とライセンス

`--name <ルール名>` 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る接続に対して実行する処理です。

--protocol <プロトコル> は、監視するネットワークアクティビティの通信プロトコルの種類です。

--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>[:<ポート範囲>] は、リモートデバイスのネットワークアドレスです。

--local <ローカルアドレス>[:<ポート範囲>] は、Kaspersky Endpoint Security 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内のルールの番号です。--at オプション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>
```

引数とライセンス

--name <ルール名> 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内のルールの番号です。

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>
```

引数とライセンス

--name <ルール名> 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内のルールの現在の番号です。

`--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内のルールの新しい番号です。

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>
```

引数とライセンス

`--zone <ゾーン>` は、ネットワークゾーンの事前定義済みの名前です。

`--address <アドレス>` 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>
```

引数とライセンス

`--zone <ゾーン>` は、ネットワークゾーンの事前定義済みの名前です。

`--address <アドレス>` 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>` は、ネットワークゾーン内のアドレスの番号です。

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」接頭辞は、そのコマンドが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します。

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>
```

引数とライセンス

<アドレス> 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 接頭辞は、そのコマンドがデバイスコントロールを管理するためのコマンドグループに属することを示します。

kesl-control --get-device-list

このコマンドは、コンピューターにインストールされているデバイスまたはコンピューターに接続済みのデバイスのリストを出力するか、接続済みのデバイスのリストを JSON ファイルにエクスポートします。

コマンド構文

```
kesl-control [-D] --get-device-list [--all] [--json] [--export <file>]
```

引数とライセンス

--all は接続済みのすべてのデバイスを一覧表示します。

--json は、接続済みのデバイスをJSON形式で一覧表示します。

--export <ファイル> は、接続済みデバイスのリストを、信頼するデバイスのリストとしてフォーマットされたファイルにエクスポートします。JSON ファイルへの完全パスを指定する必要があります。

kesl-control --trusted-devices

このコマンドを使用すると、信頼するデバイスのリストを表示したり、リストからデバイスを追加または削除したり、ファイルから信頼するデバイスのリストをインポートしたりできます。

コマンド構文

```
kesl-control [-D] --trusted-devices [--list] [--add <ID>] [--delete <ID>] [--merge|--add|--replace --file <ファイル>]
```

引数とライセンス

--list – 信頼するデバイスのリストを表示します。

--add <ID> は、デバイス ID またはデバイス ID マスクを使用して、信頼するデバイスのリストにデバイスを追加します。

--delete <ID> は、デバイス ID またはデバイス ID マスクを使用して、信頼するデバイスのリストからデバイスを削除します。

--merge は、信頼するデバイスのリストをマージします。現在のリストおよびインポートされたリストに同じ ID を持つデバイスのエントリが含まれている場合、既存のエントリがアップデートされます。現在のリストにないデバイスの場合、エントリが追加されます。

--add は、インポート時に現在の信頼するデバイスのリストを追加します。以前にデバイスリストになかったデバイスのエントリのみがリストに追加されます。

--replace は、現在の信頼するデバイスのリストを置き換えます。信頼するデバイスの既存のリストは、インポートされたリストに置き換えられます。

--file <ファイル> は、指定したファイルから信頼するデバイスのリストをインポートします。JSON ファイルへの完全パスを指定する必要があります。

kesl-control --request-temporary-device-access

このコマンドを使用すると、ブロックされたデバイスへの一時的なアクセスを要求するアクセス要求ファイルを作成できます。

コマンド構文

```
kesl-control [-D] --request-temporary-device-access --device-id <デバイス ID> --access-duration <アクセス期間> --path <アクセス要求ファイルへのパス>
```

引数とライセンス

`--device-id <デバイス ID>` は、アクセスする対象のブロックされたデバイスの ID を指定します。

`--access-duration <アクセス期間>` は、デバイスにアクセスできるようにする期間（時間単位）を指定します。可能な値：1 ～ 100

`--path <アクセス要求ファイルへのパス>` は、.akey 拡張子のアクセス要求ファイルを保存するディレクトリへのパスを指定します。

kesl-control --upload-temporary-device-access-key

このコマンドを使用すると、ブロックされたデバイスへの一時的なアクセスを取得するためのアクセスキーをアップロードできます。

コマンド構文

`kesl-control [-D] --upload-temporary-device-access-key --path <アクセスキーを含むファイルへのパス>`

引数とライセンス

`--path <アクセスキーを含むファイルへのパス>` は、デバイスへのアクセスキーを含むファイル（.acode 拡張子のファイル）へのパスです。

アプリケーションコントロールを管理するコマンド

「-A」接頭辞は、このコマンドが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属することを示します。

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]`

引数とライセンス

`--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 <カテゴリ名 1> <カテゴリ名 2> ... <カテゴリ名 N>] [--file <設定情報ファイルへのパス>] [--json]`

引数とライセンス

<カテゴリ名 1> <カテゴリ名 2> ... <カテゴリ名 N> は、情報を表示するカテゴリの名前です。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 <設定情報ファイルへのパス> は、設定の書き込み先となる JSON 設定情報ファイルへの完全パスです。

--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 <カテゴリ名 1> <カテゴリ名 2> ... <カテゴリ名 N>] --file <設定情報ファイルへのパス>`

引数とライセンス

<カテゴリ名 1> <カテゴリ名 2> ... <カテゴリ名 N> は、情報を変更するカテゴリの名前です。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>は、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。

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 <設定情報ファイルへのパス>] [--json]`

引数とライセンス

--file <設定情報ファイルへのパス>は、設定が書き込まれる設定情報ファイルへの完全パスです。

--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 <設定情報ファイルへのパス>] [--json]
```

引数とライセンス

--file <設定情報ファイルへのパス>は、設定のインポート元となる設定情報ファイルへの完全パスです。

--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 <設定情報ファイルへのパス>] [--json]
```

引数とライセンス

--file <設定情報ファイルへのパス>は、設定が書き込まれる設定情報ファイルへの完全パスです。

--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 <設定情報ファイルへのパス>] [--json]
```

引数とライセンス

`--file <設定情報ファイルへのパス>`は、設定のインポート元となる設定情報ファイルへの完全パスです。

`--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 -B --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>"
```

引数とライセンス

< フィルター条件 >には、クエリ結果を制限するために、 and 論理演算子を使用して結合された、**< フィールド > < 比較演算 > '< 値 >'** 形式の1つ以上の 論理式を指定します。

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]
```

引数とライセンス

< フィルター条件 >には、クエリ結果を制限するために、 and 論理演算子を使用して結合された、**< フィールド > < 比較演算 > '< 値 >'** 形式の1つ以上の 論理式を指定します。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 > は、表示する最新のオブジェクトの数です。 -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。すべてのオブジェクトを表示するには、0 を指定します。

--json – データを JSON 形式で出力します。

--reverse – 出力オブジェクトを逆の順序で表示します（最新のオブジェクトが上に表示され、最も古いイベントが下に表示されます）。

kesl-control -B --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 < ファイルパス >]
```

引数とライセンス

< オブジェクト ID > は、バックアップオブジェクトの ID です。

--file **< ファイルパス >**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。 --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。

隔離を管理するためのコマンド

「-Q」接頭辞は、そのコマンドが隔離の管理に使用されるコマンドのグループに属することを示します。

kesl-control -Q --mass-remove

このコマンドは、隔離から一部または全部のファイルを削除します。

コマンド構文

すべてのファイルを削除します：

```
kesl-control -Q --mass-remove
```

フィルター条件に一致するファイルを削除します：

```
kesl-control -Q --mass-remove --query "<フィルター条件>"
```

引数とライセンス

<フィルター条件>には、クエリ結果を制限するために、and 論理演算子を使用して結合された、**<フィールド> <比較演算> '<値>'** 形式の1つ以上の 論理式を指定します。

kesl-control --put

> このコマンドは、Kaspersky Endpoint Security が Kaspersky Endpoint Detection and Response Optimum または Kaspersky Managed Detection and Response と連携されている場合にのみ使用できます。

このコマンドを使用すると、ファイルを隔離できます。

コマンド構文

```
kesl-control [-Q] --put <ファイルパス> [--md5] [--sha256] [--save-original-file]
```

引数とライセンス

<ファイルパス>は、隔離するファイルへのパスです。

`--md5` は、隔離するファイルの MD5 ハッシュです。

`--sha256` は、隔離するファイルの SHA256 ハッシュです。

`--save-original-file` は元のファイルを保持します。このオプションを指定しない場合は、元のファイルは削除されます。

kesl-control -Q --query

このコマンドは、隔離されたファイルに関する情報を出力します。

コマンド構文

隔離されたすべてのファイルに関する情報を出力します。

`kesl-control -Q --query [-n <数値>] [--json]`

フィルター条件に一致する隔離されたファイルに関する情報を表示します。

`kesl-control -Q --query ["<フィルター条件>"] [-n <数値>]`

引数とライセンス

<フィルター条件>には、クエリ結果を制限するために、and 論理演算子を使用して結合された、**<フィールド> <比較演算> '<値>'** 形式の1つ以上の論理式を指定します。フィルター条件を指定しない場合、隔離されているすべてのファイルの詳細を表示します。

<数値>は、表示する直近に隔離されたファイルの数です。-n オプションを指定しない場合は、最後の 30 個のファイルが表示されます。すべてのファイルを表示するには、0 を指定します。

`--json` – データを JSON 形式で出力します。

kesl-control -Q --restore

このコマンドを使用すると、隔離されたファイルを復元できます。

コマンド構文

`kesl-control -Q --restore <ファイル ID> [--file <ファイルパス>]`

引数とライセンス

<ファイル ID>：隔離されたファイルの ID です。

`--file <ファイルパス>`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。`--file` オプションを指定しない場合、ファイルの名前は元に戻り、ファイルは元の場所に復元されます。ディレクトリが削除されているか、ユーザーにアクセス権がない場合は、本製品はファイルをディレクトリ /var/opt/kaspersky/kesl/common/restored/ に配置します。このディレクトリから任意のディレクトリにファイルを手動で移動できます。

ユーザーとロールを管理するためのコマンド

接頭辞「-U」は、そのコマンドがユーザーやロールの管理を目的としたコマンド群に属していることを示しています。

kesl-control --get-user-list

このコマンドは、ユーザーと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 <役割> <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 <役割> <ユーザー>
```

EDR Expert（オンプレミス）コンポーネント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)、Kaspersky Network Detection and Response (KATA)、Kaspersky Endpoint Detection and Response Expert（オンプレミス）および Kaspersky Endpoint Detection and Response Optimum との連携の設定を管理する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

このコマンドを使用すると、KATA サーバー、OSMP 脅威対応サーバー、または OSMP テレメトリサーバー（連携モードによって異なります）の以前に追加された証明書を追加または置き換えることができます。

コマンド構文

```
kesl-control [-R] --add-kataedr-server-certificate <file> [--server-type
<response|telemetry>]
```

引数とライセンス

< ファイル > は、サーバー証明書を含むファイルへのパスです。

`--server-type <response|telemetry>` を使用すると、EDR Expert（OSMP）連携モードで証明書を追加または置き換えるサーバーの種別を選択できます：

- `response` – OSMP 脅威対応処理サーバー
- `telemetry` – OSMP テレメトリサーバー

KATA サーバー証明書を追加または置き換える場合は、`--server-type` オプションを省略します。

kesl-control --remove-kataedr-server-certificate

このコマンドを使用すると、KATA サーバー、OSMP 脅威対応サーバー、または OSMP テレメトリサーバー（連携モードによって異なります）の以前に追加された証明書を削除することができます。

コマンド構文

```
kesl-control [-R] --remove-kataedr-server-certificate [--server-type
<response|telemetry>]
```

引数とライセンス

`--server-type <response|telemetry>` を使用すると、EDR Expert（OSMP）連携モードで証明書を削除するサーバーの種別を選択できます：

- `response` – OSMP 脅威対応処理サーバー
- `telemetry` – OSMP テレメトリサーバー

KATA サーバー証明書を削除する場合は、`--server-type` オプションを省略します。

kesl-control --query-kataedr-server-certificate

このコマンドを使用すると、KATA サーバー、OSMP 脅威対応サーバー、または OSMP テレメトリサーバー（連携モードによって異なります）の以前に追加された証明書の情報を表示することができます。

コマンド構文

```
kesl-control [-R] --query-kataedr-server-certificate [--server-type <response|telemetry>]
```

引数とライセンス

`--server-type <response|telemetry>` を使用すると、EDR Expert（OSMP）連携モードで証明書の情報を表示するサーバーの種別を選択できます：

- `response` – OSMP 脅威対応処理サーバー
- `telemetry` – OSMP テレメトリサーバー

KATA サーバー証明書に関する情報を表示する場合は、 `--server-type` オプションを省略します。

kesl-control --add-kataedr-client-certificate

このコマンドを使用すると、KATA サーバー、OSMP 脅威対応サーバー、または OSMP テレメトリサーバー（連携モードによって異なります）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き換えることができます。

コマンド構文

```
kesl-control [-R] --add-kataedr-client-certificate <file> [--server-type
<response|telemetry>]
```

引数とライセンス

< ファイル > は、クライアント証明書と秘密鍵を含む暗号化されたコンテナ（PFX アーカイブ）へのパスです。

`--server-type <response|telemetry>` を使用すると、EDR Expert（OSMP）連携モードでクライアント証明書を追加するサーバーの種別を選択できます：

- `response` – OSMP 脅威対応処理サーバー
- `telemetry` – OSMP テレメトリサーバー

KATA サーバへの接続用のクライアント証明書を追加または置き換える場合は、 `--server-type` オプションを省略します。

kesl-control --remove-kataedr-client-certificate

このコマンドを使用すると、KATA サーバー、OSMP 脅威対応サーバー、または OSMP テレメトリサーバー（連携モードによって異なります）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削除することができます。

コマンド構文

```
kesl-control [-R] --remove-kataedr-client-certificate [--server-type
<response|telemetry>]
```

引数とライセンス

`--server-type <response|telemetry>` を使用すると、EDR Expert（OSMP）連携モードでクライアント証明書を削除するサーバーの種別を選択できます：

- `response` – OSMP 脅威対応処理サーバー
- `telemetry` – OSMP テレメトリサーバー

KATA サーバへの接続用のクライアント証明書を削除する場合は、`--server-type` オプションを省略します。

kesl-control --query-kataedr-client-certificate

このコマンドを使用すると、KATA サーバー、OSMP 脅威対応サーバー、または OSMP テレメトリサーバー（連携モードによって異なります）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の情報を表示することができます。

コマンド構文

```
kesl-control [-R] --query-kataedr-client-certificate [--server-type <response|telemetry>]
```

引数とライセンス

`--server-type <response|telemetry>` を使用すると、EDR Expert（OSMP）連携モードでクライアント証明書の情報を表示するサーバーの種別を選択できます：

- `response` – OSMP 脅威対応処理サーバー
- `telemetry` – OSMP テレメトリサーバー

KATA サーバへの接続用のクライアント証明書の情報を表示する場合は、`--server-type` オプションを省略します。

NDR (KATA) コンポーネント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)、Kaspersky Network Detection and Response (KATA)、Kaspersky Endpoint Detection and Response Expert（オンプレミス）および Kaspersky Endpoint Detection and Response Optimum との連携の設定を管理する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-katandr-server-certificate

このコマンドは、以前に追加された NDR 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-katandr-server-certificate <ファイル>
```

引数とライセンス

< ファイル > は、サーバー証明書を含むファイルへのパスです。

kesl-control --remove-katandr-server-certificate

このコマンドは、NDR サーバーの証明書を削除します。

コマンド構文

```
kesl-control [-R] --remove-katandr-server-certificate
```

kesl-control --query-katandr-server-certificate

このコマンドは、NDR 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-katandr-server-certificate
```

kesl-control --add-katandr-client-certificate

このコマンドは、NDR 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-katandr-client-certificate <file>
```

引数とライセンス

< ファイル > は、クライアント証明書と秘密鍵を含む暗号化されたコンテナ（PFX アーカイブ）へのパスです。

kesl-control --remove-katandr-client-certificate

このコマンドは、NDR 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-katandr-client-certificate
```

kesl-control --query-katandr-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-katandr-client-certificate
```

管理対象デバイスのネットワーク分離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)、Kaspersky Network Detection and Response (KATA)、Kaspersky Endpoint Detection and Response Expert（オンプレミス）および Kaspersky Endpoint Detection and Response Optimum との連携の設定を管理するコマンドグループに属していることを示す接頭辞です。指定された Detection and Response ソリューションと連携されている場合、脅威の検知時の脅威対応処理としてデバイスのネットワーク分離が適用されます。

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
```

KUMA との連携の設定を管理するためのコマンド

-M プレフィックスは、このコマンドが Kaspersky Unified Monitoring and Analysis Platform の設定を管理するためのコマンド群に属することを示します。

kesl-control --add-kuma-server-certificate

このコマンドは、以前に追加された KUMA 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 [-M] --add-kuma-server-certificate <ファイルパス>
```

引数とライセンス

<ファイルパス>は、サーバー証明書を含むファイルへのパスです。

kesl-control --remove-kuma-server-certificate

このコマンドは、KUMA サーバーの証明書を削除します。

コマンド構文

```
kesl-control [-M] --remove-kuma-server-certificate
```

kesl-control --query-kuma-server-certificate

このコマンドは、KUMA 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 [-M] --query-kuma-server-certificate
```

kesl-control --add-kuma-client-certificate

このコマンドは、KUMA 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 [-M] --add-kuma-client-certificate <ファイルパス>
```

引数とライセンス

<ファイルパス>は、クライアント証明書と秘密鍵を含む暗号化コンテナ（PFX アーカイブ）へのパスです。

kesl-control --remove-kuma-client-certificate

このコマンドは、KUMA 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 [-M] --remove-kuma-client-certificate
```

kesl-control --query-kuma-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 [-M] --query-kuma-client-certificate
```

サンドボックスとの連携の設定を管理するためのコマンド

-X プレフィックスは、そのコマンドがサンドボックス連携設定を管理するためのコマンドのグループに属していることを示します。

kesl-control --add-sandbox-server-certificate

このコマンドは、サンドボックスとの対話を行うサーバーの以前に追加された証明書を追加または置き換えます。

コマンド構文

```
kesl-control [-X] --add-sandbox-server-certificate <ファイル>
```

引数とライセンス

<ファイル> は、サーバー証明書を含むファイルへのパスです。

kesl-control --remove-sandbox-server-certificate

このコマンドは、サンドボックスとの対話を担当するサーバーの証明書を削除します。

コマンド構文

```
kesl-control [-X] --remove-sandbox-server-certificate
```

kesl-control --query-sandbox-server-certificate

このコマンドは、サンドボックスとの対話を行うサーバーの証明書に関する情報を表示します。

コマンド構文

```
kesl-control [-X] --query-sandbox-server-certificate
```

kesl-control --add-sandbox-client-certificate

このコマンドは、サンドボックスとの対話を行う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き換えます。

コマンド構文

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

引数とライセンス

<ファイル> は、クライアント証明書と秘密鍵を含む暗号化されたコンテナ（PFX アーカイブ）へのパスです。

kesl-control --remove-sandbox-client-certificate

このコマンドは、サンドボックスとの対話を担当する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 [-X] --remove-sandbox-client-certificate
```

kesl-control --query-sandbox-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 [-X] --query-sandbox-client-certificate
```

kesl-control --sandbox

このコマンドは、スキャン対象のファイルをサンドボックスに送信します。

コマンド構文

```
kesl-control [-X] --sandbox <パス 1> <パス 2>
```

引数とライセンス

<パス>は、スキャンするファイルまたは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。

IOC スキャンを管理するコマンド

接頭辞 -T は、そのコマンドが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属することを示します。

kesl-control --scan-ioc

このコマンドは、デバイス上の侵害の兆候 (IOC) の検索を開始します。

コマンド構文

```
kesl-control [-T] --scan-ioc --path <ディレクトリまたはファイルへのパス> [--process on|off] [--hint <正規表現>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--excludes <除外リスト>] [--scope <ディレクトリのリスト>] [--action Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

引数とライセンス

--path <ディレクトリまたはファイルへのパス> は、スキャンの実行に使用する、.IOC または .XML 拡張子を持つ IOC ファイル、または IOC ファイルを含む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。両方の種別のパス（ファイルへのパスとディレクトリへのパス）を指定することもできます。

--process – デバイス上で実行されているプロセスの分析を有効にします。

考えられる引数：

- **on** – デバイス上で実行されているプロセスの分析を有効にします（既定値）。
- **off** – デバイス上で実行されているプロセスの分析を無効にします。

--process オプションを指定しない場合、アプリケーションは使用される IOC ファイルでこれらのプロセスの詳細 (**ProcessItem**) が指定されている場合にのみプロセスを分析します。

--hint <正規表現> は、分析対象のファイル（**FileItem**）またはプロセスの実行ファイル（**ProcessItem**）への完全パスに一致する正規表現です。

次の正規表現要素を使用できます：

- メタ文字：`. ^ $ |`
- 文字クラス：数字、英字、小文字、大文字、cntrl
- 量指定子：`* + ? {n} {n,} {n, m}`
- 否定：`[^a-c]`
- エスケープ文字：`\a \e \f, \n \r \t \v \b`

`--arpentry` – ARP テーブル (`ArpEntryItem`) 内のエントリの分析を有効にします。

考えられる引数：

- `on` – ARP 表内のエントリの分析を有効にします（既定値）。
- `off` – ARP 表内のエントリの分析を無効にします。

`--arpentry` オプションを指定しない場合、使用される IOC ファイルで ARP 表の詳細 (`ArpEntryItem`) が指定されている場合にのみ ARP 表を分析します。

`--ports` – 接続用に開いているポートの分析を有効にします。

考えられる引数：

- `on` – 接続用に開いているポートの分析を有効にし、デバイス上のアクティブな接続をスキャンします（既定値）。
- `off` – 接続用に開いているポートの分析を無効にし、デバイス上のアクティブな接続をスキャンしません。

`--ports` オプションを指定しない場合、使用される IOC ファイルでこれらのポートの詳細 (`PortItem`) が指定されている場合にのみポートを分析します。

`--system` – システム環境の分析を有効にします。

考えられる引数：

- `on` – システム環境の分析を有効にします（既定値）。
- `off` – システム環境の分析を無効にします。

`--system` オプションを指定しない場合、使用される IOC ファイルでシステム環境の詳細 (`SystemInfoItem`) が指定されている場合にのみ、システム環境を分析します。

`--files` – ファイル分析を有効にします。

考えられる引数：

- `on` – ファイル分析を有効にします（既定値）。
- `off` – ファイル分析を無効にします。

`--files` オプションを指定しない場合、使用される IOC ファイルでファイルの詳細 (`FileItem`) が指定されている場合にのみファイルを分析します。

`--drives` – スキャンする領域。

考えられる引数：

- `all` – 利用可能なすべてのファイル領域をチェックします。
- `system` – root ファイルシステム内のすべてのファイルをスキャンします。
- `critical` – ユーザーディレクトリとシステムディレクトリ内のファイルをスキャンします（既定値）。
- `custom` – 指定した領域内のファイルのみをスキャンします。

`--drives` オプションを指定しない場合、アプリケーションはユーザーディレクトリとシステムディレクトリ内のファイルを分析します。

`--excludes <除外リスト>` は、スキャンから除外されるパスのリストです。

このオプションで指定された除外はグローバルであり、範囲の種別やディレクトリリストに関係なく有効です。これらの除外は、`--hint` や `--scope` などの他のコマンドラインオプションよりも優先されます。

> 除外はパスとして指定されますが、再帰要素やワイルドカード文字（例：`*`）を含めることはできません。

`--excludes` オプションを指定しない場合は、除外なしでスキャンが実行されます。

スペースで区切って複数の除外を指定することもできる。

`--scope <ディレクトリのリスト>` は、スキャンする追加ディレクトリのリストです。

> このオプションは、`--drives` オプションに `custom` 引数を指定した場合に必要です。

`--action` – 侵害の兆候が検知された場合に実行される処理。

考えられる引数：

- `Skip` – 検知されたオブジェクトに対して処理を実行しませんが、そのオブジェクトに関する情報はタスク実行結果に保存されます（既定値）。
- `QuarantineFile` – 検知されたオブジェクトを隔離します。
- `IsolateHost` – オブジェクトが検知されたデバイスにネットワーク分離を強制します。
- `ScanCriticalAreas` – **簡易スキャン**を実行します。
  - /lib/systemd
  - /lib/udev
  - /lib/dbus-1.0

- /usr/local/lib/systemd/user
- /usr/share/dbus-1
- /usr/share/gdm/autostart
- /usr/share/gnome/autostart
- /var/spool/at
- /var/spool/at/spool
- /var/spool/anacron
- /var/spool/cron
- /boot
- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

スペースで区切って複数のパスを指定することもできます。

`Skip` 引数を指定する場合は、他の引数を追加しないでください。`Skip` 引数は単独でのみ使用できます。

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 接頭辞は、コマンドが（Kaspersky Security for Virtualization Light Agent の一部として）仮想環境保護用 Light Agent モードで使用される Kaspersky Endpoint Security コマンドのグループに属していることを示します。

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
```

システムパフォーマンスメトリックを管理するためのコマンド

kesl-control --export-metrics

このコマンドを使用すると、オペレーティングシステムのパフォーマンスメトリックの取得を設定できます。

コマンド構文

`kesl-control [-J] --export-metrics [--period <エクスポート間の間隔（秒）>|--interactive]`

引数とライセンス

`--period` は結果の定期的な出力を有効にします。

<エクスポート間の間隔（秒単位）>（秒単位）は出力期間を設定します。

`--interactive` は、対話型出力を有効にします（**Enter** キーが押されたとき）。

補足資料 2：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。

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。
- 設定の値を**< 設定名 >=< 設定値 >**形式で指定します（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。

設定情報ファイルに加えた変更を適用するには、Kaspersky Endpoint Security アプリケーションを再起動してください。

ファイルにパラメータが存在しないか、間違ったパラメータ値が指定されている場合、本製品は既定値を使用します。

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 が Kaspersky Security Center に送信するアプリケーションイベントに使用されるロケール。 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 環境変数から引用されます。本製品がこのローカリゼーションに対応していない場合は、既定で英語のローカリゼーションが適用されます。	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。 本製品が OS のロケールを検知できない場合、またはこのロケールに対応していない場合は、イベントのローカライズに英語（RFC 3066 形式の en_US.UTF-8）が使用されます。
`PackageType`	インストールされた製品パッケージの形式。 この設定の値を手動で変更することは推奨しません。この値は、アプリケーションの初期構成時に自動的に入力されます。	`rpm` – RPM パッケージがインストールされます。 `deb` – DEB パッケージがインストールされます。
`UseFanotify`	fanotify テクノロジーを使用してファイル操作を読み取ります。 この設定の値を手動で変更することは推奨しません。この設定は、アプリケーションの初期構成時に指定されます。	`true/yes` – アプリケーションは fanotify テクノロジーを使用してファイル操作を読み取ります。 `false/no` – fanotify テクノロジーは使用されません。

設定	説明	値
KsvlaMode	Kaspersky Endpoint Security の Light Agent モードでの使用。 この設定の値を手動で変更することは推奨しません。この設定は、アプリケーションの初期構成時に指定されます。	true/yes – アプリケーションは仮想環境保護用 Light Agent モードで使用されます。 false/no – 本製品は標準モードで使用されます。
EndpointAgentMode	Endpoint Detection and Response Agent モードでの Kaspersky Endpoint Security の使用	true/yes – 本製品は Endpoint Detection and Response Agent モードで使用されます。 false/no – 本製品は標準モードで使用されます。
KcsMode	Kaspersky Endpoint Security を Kaspersky Container Security の一部として使用するファイル脅威保護コンポーネントとしてのソリューション。 この設定の値を手動で変更することは推奨しません。この設定は、Kaspersky Container Security ソリューションでのみ使用されます。	true/yes は、本製品が Kaspersky Container Security ソリューションのファイル脅威保護コンポーネントとして使用されることを意味します。 false/no（既定）は、本製品が Kaspersky Endpoint Security モード（標準モード、Endpoint Detection and Response Agent モード、または仮想化用の Light Agent モード）のいずれかで使用されることを意味します。
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 – アプリケーションの起動時にトレースファイルを生成します。 false/no（既定値）– 本製品の起動時にトレース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） – トレースファイル内の、個人情報が含まれる可能性のある情報を表示します。 false/no（既定値）–トレースファイル内の、個人情報が含まれる可能性のある情報を表示しません。
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 – 非同期トレースを有効にします。 false/no（デフォルト値）– 非同期トレースを有効にしません。
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：アプリケーションがクラッシュした場合にダンプファイルを作成します。 false/no（既定値）：アプリケーションがクラッシュした場合にダンプファイルを作成しません。
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/kesl/common/dumps。 既定のダンプ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。
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 スキャンするタスクに使用可能なメモリをすべて使い果たしてアプリケーションの再起動が必要になるのを避けるため、ScanMemoryLimit を MaxMemory 設定よりも低く指定することを推奨します。
MachineId	ユーザーの一意のデバイス ID。	設定の値は、アプリケーションのインストール中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/bl4control
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。 オペレーティングシステムの設定が MaxInotifyWatches 設定より小さい場合、本製品はオペレーティングシステムの設定を MaxInotifyWatches の値に変更します。	既定値：299987

設定	説明	値
`MaxInotifyInstances`	/proc/sys/fs/inotify/max_user_instances で 1 ユーザーセットのファイルやディレクトリの変更に対する定期制サービスの数を制限します。 オペレーティングシステムの設定が `MaxInotifyInstances` 設定より小さい場合、本製品はオペレーティングシステムの設定を `MaxInotifyInstances` の値に変更します。	既定値：2047
`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：20
`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： 1. Google Public DNS™（8.8.8.8）。 2. Cloudflare® DNS（1.1.1.1）。 3. Alibaba Cloud® DNS（223.6.6.6）。 4. Quad9® DNS（9.9.9.9）。 5. CleanBrowsing (185.228.168.168)。	`true/yes` – カスペルスキーのサーバーへのアクセスに、パブリック DNS を使用します。 `false/no`（既定値） – カスペルスキーのサーバーへのアクセスに、パブリック DNS を使用しません。 本製品は DNS サーバーとの TCP/UDP 接続を確立するため、要求にはドメインアドレスとユーザーの外部 IP アドレスが含まれる場合があります。たとえば、HTTPS で通信する時に Web リソースの証明書を確認するために、この情報が必要になります。パブリック DNS サーバーが使用されている場合、データ処理ルールは、対応するサービスのプライバシーポリシーによって管理されます。
`PanicThreshold`	更新可能なカーネルモジュールの使用時に発生する異常停止の最大件数。指定された値に達すると、本製品は「セーフ」モードに入り、更新可能なカーネルモジュールは起動されません。	既定値：3
`SafeMode`	更新可能なカーネルモジュールを使用するときに「セーフ」モードを有効にします。このモードでは、本製品は更新可能なカーネルモジュールを起動しません。 本製品が `PanicThreshold` 設定で指定された異常停止の最大回数に達すると、「セーフ」モードが自動的に有効になります。	`true/yes` は、本製品の「セーフ」モードが有効になっていることを意味します。 `false/no`（既定）は、本製品の「セーフ」モードが無効になり、本製品が正常に動作していることを意味します。
`GetContainerName`	Kaspersky Managed Detection and Response と連携する場合、コンテナに関する次の情報がテレメトリに含まれます： • コンテナで発生しているイベントの表示 • コンテナの namespace の ID • コンテナ名 コンテナ名は、コンテナスキャンタスクを使用するライセンスがあり、コンテナの有効期間が十分にある場合にのみ送信されます。	`true/yes` の場合は、Kaspersky Managed Detection and Response と連携するときに、テレメトリにコンテナに関する拡張情報を含まれます。 `false/no` の場合は、Kaspersky Managed Detection and Response と連携するときに、テレメトリにコンテナに関する拡張情報が含まれません。
[Network] セクションには、次の設定が含まれています：		

設定	説明	値
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 0x が付いた 16 進数。 既定値：0x100。 Kubernetes などの分散システムの一部として使用されるノード上で本製品が実行されている場合に、トラフィックの循環的なスキャンを回避するには、上位ビットを使用してネットワークパケットマークの値を変更する必要があります。例：0x1000 または 0x10000（マークは 32 ビット整数に制限されます）。
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。 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 0x が付いた 16 進数。 既定値：0x200。 Kubernetes などの分散システムの一部として使用されるノード上で本製品が実行されている場合に、トラフィックの循環的なスキャンを回避するには、上位ビットを使用してネットワークパケットマークの値を変更する必要があります。例：0x2000 または 0x20000（マークは 32 ビット整数に制限されます）。
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 0x が付いた 16 進数。 既定値：0x400。 Kubernetes などの分散システムの一部として使用されるノード上で本製品が実行されている場合に、トラフィックの循環的なスキャンを回避するには、上位ビットを使用してネットワークパケットマークの値を変更する必要があります。例：0x4000 または 0x40000（マークは 32 ビット整数に制限されます）。
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のマーク。	10 進数の値または先頭に 0x が付いた 16 進数。 既定値：0x800。 Kubernetes などの分散システムの一部として使用されるノード上で本製品が実行されている場合に、トラフィックの循環的なスキャンを回避するには、上位ビットを使用してネットワークパケットマークの値を変更する必要があります。例：0x8000 または 0x80000（マークは 32 ビット整数に制限されます）。
ProxyRouteTable	ルーティングテーブルの番号。	既定値：101
[ScannerImpactStats] セクションには、次の設定が含まれています：		
CollectFileScanStatistics	アプリケーションによるファイルおよびプロセスのスキャン統計のカウントを有効にします。	true/yes （既定値）は、ファイルおよびプロセスのスキャン統計の集計を有効にします。 false/no は、ファイルおよびプロセスのスキャン統計の集計を無効にします。
StatCollectionPeriod	スキャンされたファイルおよび検知された処理の統計情報をトレースファイルおよびレポートに保存する前に、本製品が収集する期間を指定します。	既定値：10 分。

設定	説明	値
StatCollectionCount	StatCollectionPeriod パラメータで指定された時間間隔中にカウントされ、レポートおよびトレースファイルに含まれるスキャン済みファイルと検出されたプロセスの数。	既定値：10
ReportStatAmount	1日に最も頻繁にスキャンされたファイルとプロセスに関するレポートに書き込まれるレコードの数。	既定値：20
［**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。 この設定の値を手動で変更することは推奨しません。この設定は、アプリケーションの初期構成時に指定されます。	true/yes – 保護対象仮想マシンがサーバーとして使用されます。 ［false/no］– 保護対象仮想マシンはワークステーシ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。 この設定の値を手動で変更することは推奨しません。この設定は、アプリケーションの初期構成時に指定されます。	true/yes – VDI 保護モードが有効になっています。 false/no – VDI 保護モードは無効になります。
[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、Watchdog サーバーは kesl プロセスを再起動する手順を開始します。	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 Watchdog 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回数。	既定値：5
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 プロセスを再起動する手順を開始します。	既定値：2 分。
ConnectTimeout	kesl プロセスが開始された瞬間からの本製品の Watchdog サーバーへの接続の最大タイムアウト。 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 プロセスを再起動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。

設定	説明	値
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 プロセスを再起動する手順を開始します。	off – 常駐設定のサイズは制限されません。 < 値 >% – RAM の 1 ～ 100 パーセントの値。 < 値 >MB – メガバイト単位の値。 lowest/< 値 >%/< 値 >MB – パーセンテージ値とメガバイト単位の絶対値のうち小さい方。 highest/< 値 >%/< 値 >MB – パーセンテージ値とメガバイト単位の絶対値のうち大きい方。 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。
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 プロセスを再起動する手順を開始します。	off（既定値）– 仮想メモリサイズは制限されません。 < 値 >MB – メガバイト単位の値。
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 プロセスを再起動する手順を開始します。	off （既定値）– スワップファイルのサイズは制限されません。 < 値 >% – RAM の 0 ～ 100 パーセントの値。 < 値 >MB – メガバイト単位の値。 lowest/< 値 >%/< 値 >MB – パーセンテージ値とメガバイト単位の絶対値のうち小さい方。 highest/< 値 >%/< 値 >MB – パーセンテージ値とメガバイト単位の絶対値のうち大きい方。
TrackProductCrashes	本製品が不安定な場合に、Kaspersky Endpoint Security から Kaspersky Security Center へのデバイスステータスの送信を有効にします。	true/yes にすると、Kaspersky Endpoint Security から Kaspersky Security Centerへのデバイスステータス情報の送信が有効になります。 false/no（既定）は、Kaspersky Endpoint Security から Kaspersky Security Center へのデバイスステータスの送信を無効にします。
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/kesl/private/kesl_health.log.
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	本製品の異常停止の最大回数。この回数を超えると、本製品の不安定な動作に関する通知が表示されます。	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。
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。
SyscallHangProbePeriod	Watchdog サーバーが open および execve システム関数を呼び出し、これらの関数の成功カウンターを増やす期間。	既定値：3 秒。
SyscallHangCheckPeriod	Watchdog サーバーが open および execve 関数の成功カウンターをチェックする期間。 この期間経過後にカウンターの値が変更されない場合、Watchdog サーバーは kesl プロセスを再起動する手順を開始します。	既定値：32 秒。
DumpSuspendPeriod	ダンプファイルアプリケーションの作成を待機する最大時間。この間、Watchdog サーバーはアプリケーションアクティビティのチェックを一時停止します。 この期間経過後にダンプの作成が完了しなかった場合、Watchdog サーバーは kesl プロセスを再起動する手順を開始します。	可能な値：1～30 分。 既定値：2 分。

設定	説明	値
`TimeoutAfterCoredump`	Watchdog サーバーが異常なプロセス終了手順の一部として SIGTRAP シグナルを送信した後、kesl プロセスへのその他のシグナルの送信を一時停止する最大期間。	既定値：2 分。 `TimeoutAfterCoredump` は `DumpSuspendPeriod` 以上の値に設定することを推奨します。 この設定を指定するには、次の単位を使用できます： • `<n> day|days|d`：日単位 • `<n> hour|hours|hr|h`：時間単位 • `<n> minute|minutes|min|m`：分単位 • `<n> second|seconds|sec|s`：秒単位 • `<n> [msec|ms]`：ミリ秒単位 単位が指定されていない場合、値をミリ秒として解釈されます。
既定では、**[Environment]**セクションは設定情報ファイルに存在しません。		
`ExperimentalContainerdSupport`	コンテナモニターコンポーネントが実行中の場合に、containerd 環境のサポートを有効にします（ContainerScan、コンテナ監視）。 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 `[Environment]` 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` – コンテナ監視コンポーネントの操作で containerd 環境への対応を有効にします。 `false/no` – コンテナ監視コンポーネントの操作で containerd 環境への対応を有効にしません。
`ReduceSWMemoryConsumption`	イベントキューの処理における、ふるまい検知コンポーネントによるメモリ消費量を制限します。 メモリ制限を設定すると、脅威の検知に悪影響が生じます。これには、Detection and Response ソリューションとの連携の一環として送信されるテレメトリの品質への影響も含まれます。メモリ消費量が多い問題を解決する他の方法がない場合に限り、高負荷のシステムでのみ、テクニカルサポートに問い合わせて具体的な手順を確認したうえで制限を設定することを推奨します。	1 – イベントキューの処理における、ふるまい検知コンポーネントによるメモリ使用量を制限する。 0（既定） – メモリ使用量を制限しない。 この設定の変更後は、製品を再起動する必要があります。

コマンドラインタスクの既定

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。

`Rollback` と `License` 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

SkipDatabaseJournals=No

TimeLimit=60

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

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

ActionOnThreat=DisinfectDeleteIfNotPossible

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

ActionOnThreat=DisinfectDeleteIfNotPossible

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

ActionOnThreat=DisinfectDeleteIfNotPossible

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

```
ConnectionTimeout=10
```

```
ApplicationUpdateMode=DownloadOnly

[Sources.item_0000]

Enabled=Yes

SourceType=KLServers

URL=
```

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

AllowToRequestTemporaryAccess=No

[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

ActionOnThreat=DisinfectDeleteIfNotPossible

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

UseAEP=No

AEPMode=Block

UseTelemetryMonopolyMode=Yes
```

```
TelemetrySource=Default
```

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

GoldenImageAction=DoNothing

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/usr/bin

AreaMask.item_0000=*
```

KATAEDR タスク（ID:24）の既定

```
Mode=EDRKATA

UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=127.0.0.1

Port=443

[EventTransferSettings]
```

```
MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

[TelemetrySettings]

UseClientPinnedCertificate=No

ConnectionTimeout=10

RequestTimeout=10

OnlyTaggedEvents=No

[TelemetrySettings.Endpoints.item_#]

Address=

Port=443

[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

Web_Control タスク（ID:26）の既定

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

Standalone_Sandbox タスク（ID:29）の既定

```
ConnectionTimeout=10

RequestTimeout=10

UseClientCertificate=No

SendingMode=AutoOnly

QuarantineFile=Yes
```

```
ScanCriticalAreas=Yes

CreateIocScanTask=Yes

QuarantineFileOnIocDetected=Yes

ScanCriticalAreasOnIocDetected=Yes

Drives=Critical

ScheduleMode=Manually

[Servers.item_0000]

Address=127.0.0.1

Port=443

[SandboxTransferSettings]

SandboxQueue=1024
```

KATANDR タスク（ID:31）の既定

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

[Endpoints.item_0000]

Address=127.0.0.1

Port=8081

[EventTransferSettings]

MaximumDataTransferTime=30

MaximumNumberOfEventsInPackage=1024

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

PingPeriod=450
```

KUMA タスク（ID:29）の既定

```
UseClientCertificate=No

UseTls=No

ConnectionTimeout=5

[Servers.item_0000]

Address=127.0.0.1

Port=443

Protocol=TCP

[SiemTransferSettings]

EventTransferTimeMax=30
```

メール脅威対策タスクの既定 (ID: 35)

```
CheckIncomingMessagesOnly=No

ActionOnThreat=DisinfectDeleteIfNotPossible

ScanFileArchive=Yes

ScanFileOffice=Yes

UseTimeLimit=No

TimeLimit=8

UseSizeLimit=No

SizeLimit=5

ExtensionFilter=Rename

UseAnalyzer=Yes

AnalyzerLevel=Medium

[ExtensionMasks.item_0000]

UseExtensionMask=Yes

ExtensionMask=*.txt
```

```
[ExtensionMasks.item_0001]

UseExtensionMask=Yes

ExtensionMask=*.run

[ExtensionMasks.item_0002]

UseExtensionMask=Yes

ExtensionMask=*.exe

[ExtensionMasks.item_0003]

UseExtensionMask=Yes

ExtensionMask=*.js

[ExtensionMasks.item_0004]

UseExtensionMask=Yes

ExtensionMask=*.jse

[ExtensionMasks.item_0005]

UseExtensionMask=Yes

ExtensionMask=*.msi

[ExtensionMasks.item_0006]

UseExtensionMask=Yes

ExtensionMask=*.scr

[ExtensionMasks.item_0007]

UseExtensionMask=Yes

ExtensionMask=*.vbe

[ExtensionMasks.item_0008]

UseExtensionMask=Yes

ExtensionMask=*.vbs

[ExtensionMasks.item_0009]

UseExtensionMask=Yes

ExtensionMask=*.sh
```

BadUSB 攻撃ブロックタスクの既定 (ID: 37)

`MaxAuthAttempts=5`

`TimeoutAfterAttempts=5`

`ProhibitOnScreenKeyboard=No`

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	値
`SambaConfigPath`	Samba 設定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。 この設定の変更後は、製品を再起動する必要があります。	既定では、コンピューター上の SAMBA 設定ファイルの標準ディレクトリが指定されています。 既定値：/etc/samba/smb.conf
`NfsExportPath`	NFS 設定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。 この設定の変更後は、製品を再起動する必要があります。	既定では、コンピューター上の NFS 設定ファイルの標準ディレクトリが指定されています。 既定値：/etc/exports
`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`	本製品のトレースファイルを格納するディレクトリ。 この設定の変更後は、製品を再起動する必要があります。	既定値：/var/log/kaspersky/kesl 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。別の ディレクトリを指定する場合は、このディレクトリに対する読み取りおよび書き込み権限を root ユーザーのみが持っていることを確認してください（`700` または `rwx--------` の権限）。

設定	説明	値
TraceMaxFileCount	本製品のトレースファイルの最大数。 この設定の変更後は、製品を再起動する必要があります。	1 - 10000 既定値：10
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）。 この設定の変更後は、製品を再起動する必要があります。	1 - 1000 既定値：500
BlockFilesGreaterMaxFileNamePath	完全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 に対応していない OS にのみ適用されます。 この設定の値を変更した後、ファイル脅威対策タスクを再起動する必要があります。	4096 - 33554432 既定値：16384
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（既定）– 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無効にします。
NamespaceMonitoring	名前空間とコンテナのスキャンの有効化（コンテナスキャン、コンテナ監視）。 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。	Yes（既定値） – 名前空間とコンテナスキャンを有効にします。 No – 名前空間とコンテナスキャンを無効にします。
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の読み取りモードを有効にします。ファイル操作の読み取りモードは、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。	Yes（既定値）を選択すると、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。 スキャン中にファイルにアクセスする場合はNo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。このファイル操作の読み取り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。ただし、ファイル脅威対策、デバイスコントロール、および実行防止の各コンポーネントは、設定されているモードに関係なく、通知モードで動作します。

設定	説明	値
UseKSN	アプリケーション用に Kaspersky Security Network を設定します。	Basic – 標準モードで Kaspersky Security Network の使用を有効にします。 Extended – 拡張モードで Kaspersky Security Network の使用を有効にします。 No（既定値）– Kaspersky Security Network を使用しません。
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。 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 — Kaspersky Endpoint Security がマルウェアデータベースの軽量バージョンを使用する動作モードを有効にします。 No（既定値）– マルウェア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。
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。 MDR コンポーネントを有効にし、Kaspersky Security Network が無効になっているか基本モードで使用されている場合は、エラーメッセージが表示され、MDR コンポーネントは有効になりません。MDR コンポーネントを有効にするには、拡張モードで KSN を有効にする必要があります。	Managed Detection and Response コンポーネントを有効にするには、Yes を選択します。 No（既定値）– Managed Detection and Response を無効にします。
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 コンポーネントを有効にします。 No（既定）– EDR Optimum コンポーネントを無効にします。
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。プロキシサーバーは、カスペルスキーアクティベーションサーバーへのアクセス、定義データベースと機能のアップデート元、Kaspersky Security Network へのアクセス、およびウェブ脅威対策コンポーネントを使用した Web サイト証明書の検証に使用できます。 Kaspersky Endpoint Security を Light Agent モードで使用する場合、Kaspersky Security Network、SVM、および Integration Server へ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ていません。	Yes：プロキシサーバーの使用を有効にします。 No（既定）– プロキシサーバーの使用を無効にします。

設定	説明	値
`ProxyServer`	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。 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。	次のいずれかの形式でのプロキシサーバーのアドレス： • `[<connection protocol>://]<IP address of the proxy server>:<port>` - プロキシサーバーへの接続に認証が不要な場合。 • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>` - プロキシサーバーへの接続に認証が必要な場合。 HTTPS 経由のプロキシサーバーへの接続には対応していません。
`ProxyBypass`	プロキシサーバーをバイパスするアドレスリスト。	アドレスは、**< アドレス >[:< ポート番号 >** 形式で指定します。 アドレスを指定するには、マスク（*記号）とコメント（\記号の後）を使用できます。
`ProxyBypassEdr`	Kaspersky Endpoint Detection and Response Expert（オンプレミス）Integration Server に接続する時にプロキシサーバが使用されるかどうか。	`Yes` – Kaspersky Endpoint Detection and Response Expert（オンプレミス）Integration Server に接続する時は、プロキシサーバを使用しません。 `No`（既定値）– Kaspersky Endpoint Detection and Response Expert（オンプレミス）Integration Server に接続する時は、プロキシサーバを使用します。
`ProxyBypassNdr`	Kaspersky Network Detection and Response (KATA) Integration Server に接続する時にプロキシサーバが使用されるかどうか。	`Yes` – Kaspersky Network Detection and Response (KATA) Integration Server に接続する時は、プロキシサーバを使用しません。 `No`（既定値）– Kaspersky Network Detection and Response (KATA) Integration Server に接続する時は、プロキシサーバを使用します。
`ProxyBypassSandbox`	サンドボックスとの対話を提供するサーバーに接続するときにプロキシサーバーを使用するかどうか。	`Yes` の場合、サンドボックスとの対話を提供するサーバーに接続するときにプロキシサーバーを介しません。 `No`（既定値）の場合、サンドボックスとの対話を提供するサーバーに接続するときにプロキシサーバーを使用します。
`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 値が 0 の場合、新しいイベントは保存されず、古いイベントは削除されます。
`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 - 100000 0 は、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ないことを意味します。 既定値：5
`UseSyslog`	製品イベントに関する情報の syslog への記録を有効にします。 syslog にアクセスするには、root 権限が必要です。	`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。
`EventsStoragePath`	イベントログ定義データベースのメインファイルへのパス。 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/kesl/private/storage/events.db

設定	説明	値
`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、コンテナ監視（コンテナスキャン、コンテナ監視）コンポーネント、およびリムーバブルドライブスキャンタスクの動作に適用され、ODS および ContainerScan スキャンタスクの動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` ― 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読み取りから除外します。 `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読み取りから除外します。 `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読み取りから除外します。 `Mounted:<` **ファイルシステム種別** `>` ― 指定したファイルシステム種別のマウント済みディレクトリをすべて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の読み取りから除外します。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。 `<` **次を含むパス** `: /mnt/user*  または /mnt/**/user_share>` マスク ― 名前に指定した**マスク**を含むマウントポイント内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、`?` 文字を使用して任意の文字を表示できます。
`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。	`<` **プロセスへの完全パス** `>` – 指定されたローカルディレクトリ内のプロセスをスキャンしません。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。

設定	説明	値
UseOnDemandCPULimit	次の種別のタスクに対して、CPU使用率制限を有効にします：*ODS*、*ContainerScan*、*InventoryScan*。	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（既定）：タスクの CPU 使用量制限を無効にします。
OnDemandCPULimit	次の種別のタスクに対するすべてのプロセッサコアの最大使用率（パーセンテージ）：*ODS*、*ContainerScan*、*InventoryScan*。	10 から 100 までの整数値。 既定値：100
BackupDaysToLive	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）。指定された時間が経過すると、アプリケーションはファイルの最も古いバックアップコピーを削除します。 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 から 10000 0–無制限の保持。 既定値：30
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、最も古いファイルのバックアップコピーが削除されます。 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 から 999999 0–無制限のサイズ。 既定値：0
QuarantineBackupFolder	ファイルと隔離されたファイルのバックアップコピーが保存されるディレクトリへのパス。 既定のディレクトリを変更できます。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/ 既定のディレクトリにアクセスするには、root 権限が必要です。
QuarantineFillingNotification	隔離の容量に達したことを示すイベントを生成するために必要な隔離の使用割合。 隔離が容量に達したことに関するイベントの生成を無効にするには、0 を入力します。	0 から 100 0 – 隔離が容量に達したことに関するイベントの生成は無効です。 既定値：90
QuarantineSizeLimit	隔離の最大サイズ（メガバイト単位）。隔離の最大サイズに到達すると、最も古いファイルから削除されます。 隔離のサイズを無制限にするには、0 を入力します。	0 から 999999 0 は隔離のサイズが無制限でないことを意味します。 本製品が基本モードで使用されている場合の既定値は 200 で、Light Agent モードで使用されている場合の既定値は 100 です。
ShowPopUpNotifications	グラフィカルユーザーインターフェイスでポップアップ通知の表示を有効化する	Yes（既定値）– グラフィカルユーザーインターフェイスでポップアップ通知を表示します。 No – グラフィカルユーザーインターフェイスでポップアップ通知を表示しません。
PowerSaveMode	バッテリー電源で動作しているデバイスでスケジュールされたタスクをキャンセル。	Yes（既定値）の場合、デバイスがバッテリ電源で動作しているときにスケジュールされたタスクをスキップします。 No は、デバイスがバッテリー電源で動作しているかどうかに関係なく、スケジュールされたタスクを実行します。
InterceptorMode	Kaspersky Endpoint Security が使用するシステムイベントインターセプターメカニズム： この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。	UseFanotify（既定）– fanotify テクノロジーを使用してシステムイベントを遮断します。 UseUpdatableKernelModule – 更新可能なカーネルモジュールを使用してシステムイベントを遮断します。

設定	説明	値
InterceptorFallbackStrategy	アップデート可能なカーネルモジュールの起動に失敗した場合のアプリケーションの処理。 この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。	FallbackToFanotify（既定）– システムイベントの遮断のために fanotify に切り替えます。 FallbackToLimitedMode – システムイベントの遮断を使用しません。本製品がシステムイベントインターセプターを使用しない場合、リアルタイムスキャンは実行されず、デバイスの保護レベルが低下します。
InterceptorApplyStrategy	本製品がアップデート可能なカーネルモジュールの使用に切り替えた場合、モジュールを起動するには本製品を再起動する必要があります。この設定では、本製品を自動的に再起動するか、手動で再起動するかを指定できます。 この設定は、fanotify テクノロジーに対応するオペレーティングシステムを使用しているデバイスにのみ適用されます。	RestartServiceAutomatically は、アップデート可能なカーネルモジュールを起動するために本製品を自動的に再起動します。 RestartServiceManually は、ユーザーが本製品を手動で再起動した後に、アップデート可能なカーネルモジュールを起動します。 更新可能なカーネルモジュールの使用に切り替えるには、本製品を自動的に再起動することを推奨します。本製品を再起動した後、更新可能なカーネルモジュールを手動で起動すると、アプリケーションエラーが発生する可能性があります。
SystemEventsTransmission	サードパーティー製品イベントに関する情報の syslog への記録を有効にします。 syslog にアクセスするには、root 権限が必要です。	Yes – サードパーティー製品イベントに関する情報の syslog への記録を有効にします。 No（既定値）– サードパーティ製品イベントに関する情報の syslog への記録を無効にします。

コンテナスキャンの全般設定

コンテナスキャンの全般設定は、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（コンテナスキャン、コンテナ監視）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。 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。	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。この値を指定すると、コンテナで実行される処理は、ActionOnThreat の ActionOnThreat 設定にも依存します。ActionOnThreat が DisinfectDeleteIfNotPossible に設定されていて、本製品が処理の実行中に感染したオブジェクトを駆除または削除できない場合、コンテナは停止されます。 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。

設定	説明	値
UseDocker	Docker コンテナ管理システムの使用。 Docker 28.5.2 以前との連携に対応しています。	Yes（既定）の場合、Docker コンテナ管理システムの使用が有効になります。 No の場合、Docker コンテナ管理システムの使用が無効になります。
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

ネットワークトラフィックのスキャン設定

ネットワークトラフィックのスキャン設定

設定	説明	値
EncryptedConnectionsScan	暗号化された接続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、暗号化された接続のスキャンが既定で無効になっています。	Yes（既定値）– 暗号化された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	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。

設定	説明	値
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_#]（以下を参照）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	本製品がネットワークポートを監視する方法を指定します。	Selected（既定値）– [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。
NetInterceptorMode	Kaspersky Endpoint Security によるトラフィック傍受モード。	UseEBPF — eBPF テクノロジーを使用してトラフィックを傍受します。 UseIPTables（既定値）— iptables ユーティリティを使用してトラフィックを傍受します。 トラフィック傍受モードを変更するには、本製品を再起動する必要があります。再起動すると、接続済みのネットワーク接続が切断されます。
[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、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。
［**IncomingEndpointsExclusions.item_#**］セクションには、受信トラフィックの除外が含まれています。		
RemoteIp	傍受から除外されるトラフィックのリモートデバイスの IP アドレス。	
DestinationPort	リモートデバイスからのトラフィック傍受から除外される、保護対象デバイス上のポート。	
[OutgoingEndpointsExclusions.item_#] セクションには、送信トラフィックの除外が含まれています。		
RemoteIp	傍受から除外されるトラフィックのリモートデバイスの IP アドレス。	
DestinationPort	保護対象デバイスからのトラフィック傍受から除外される、リモートデバイス上のポート。	
[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。	
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

以下の表では、すべてのアプリケーションタスクに対して管理できるタスクスケジュール設定について説明します。

タスクのスケジュール設定

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。 Monthly – 毎月指定した日時にタスクを実行します。 Weekly – 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 >/< 日 >] [hh]:[mm]:[ss]; [< 日 >|< 曜日 >]; [< 開始周期 >]
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。	既定値：99 分。
RunMissedStartRules	本製品を起動後にミスタスクを実行します。	Yes（既定値）– アプリケーションの起動後に、実行されなかったタスクの実行を有効にします。 No – 本製品を起動後のミスタスクの実行を有効にしません。
UseWorkingTimeout	WorkingTimeout 設定で指定された最大タスク実行時間に達するとタスクを停止します。タスクは完了していなくても停止されます。タスクの次回の起動はスケジュールに従って実行されます。	Yes – タスクの最大実行時間に達したらタスクを停止します。 No（既定値）– 最大タスク実行時間に達したときにタスクを停止しません。
WorkingTimeout	UseWorkingTimeout=yes の場合、アプリケーションがタスクの実行を停止するまでの最大タスク実行時間（分単位）。	既定値：120 分。

補足資料 3：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 は、コマンド / タスクが正常に完了したことを意味します。

1 は、コマンド引数の一般的なエラーを意味します。

2 – 渡された製品設定のエラー。

64 は、Kaspersky Endpoint Security が動作していないことを意味します。

66 – 製品データベースが読み込まれていません（`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 は、製品がポリシーに従って管理しているため、コマンドを実行できないことを意味します。

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 は、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たことを意味します。

73 – `--accept` オプションを使用して確認せずに、アプリケーションの動作に影響するアプリケーションコントロールタスクの設定を行おうとしました。

74 は、Kaspersky Endpoint Security がアップデート後に再起動する必要があることを意味します。

75 は、デバイスを再起動する必要があることを意味します。

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。

78 は、アプリケーションが Light Agent モードで使用されているため、コマンド / タスクを実行できないことを意味します。

79 は、アプリケーションが標準モードで使用されているため、コマンドを実行できないことを意味します。

80 – ネットワークの問題によりアップデートのダウンロード処理に失敗しました。

128 は、不明なエラーを意味します。

65 - その他のすべてのエラー。

補足資料 4：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、リアルタイム保護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 <ファイルの完全パス>`

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 と統合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リアルタイム保護タスクに設定を読み込みます：

   ```
   kesl-control --set-settings 1 --file <ファイルの完全パス>
   ```

補足資料 5：Web コンソールでのポリシーの製品設定

このセクションでは、Web コンソールの［**製品設定**］タブのポリシー設定について説明します。

ホスト脅威対策

ファイル脅威対策

Windows、macOS 、Linux 向け

ファイル脅威対策は、コンピューターのファイルシステムを感染から保護します。既定では、ファイル脅威対策はコンピューターの RAM に常駐し、開いたファイル、保存したファイル、実行されたファイルのすべてをリアルタイムでスキャンします。このコンポーネントは、接続されているドライブを含むすべてのコンピューターのドライブ上のファイルをスキャンします。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、およびヒューリスティック分析を使用してコンピューターを保護します。

コンポーネントは、ユーザーまたはアプリケーションがアクセスしたファイルをスキャンします。悪意のあるファイルが検知された場合、Kaspersky Endpoint Security はファイル操作をブロックします。その後、ファイル脅威対策の設定に応じて、悪意のあるファイルを駆除または削除します。

コンテンツが OneDrive クラウドストレージ上にあるファイルにアクセスしようとすると、Kaspersky Endpoint Security はファイルのコンテンツをダウンロードしてスキャンします。

`Linux` Linux デバイスでは、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スキャン中のファイルへのアクセスのブロック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。

ファイルアンチウイルスの設定

設定	OS	説明
信頼するオブジェクト	`Windows` `macOS` `Linux`	*信頼するオブジェクト*とは、Kaspersky Endpoint Security が特定のオブジェクトについてウイルスなどの脅威のスキャンを実行しないときに、オブジェクトが満たす必要のある一連の条件によって定義されます。スキャン除外により、侵入者がコンピューターやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションを使用できます。こうしたアプリケーションは必ずしも悪意のある目的を持っているわけではありませんが、ハッカーによって悪用される可能性があります。侵入者がコンピューターやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションに関する詳細情報は、カスペルスキー百科事典の Web サイトを参照してください。 Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。
脅威の検知時の処理	`Windows` `macOS` `Linux`	**駆除する。駆除できない場合は削除する**このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルは削除されます。 **駆除する。駆除できない場合はブロックする（OS により異なります）** `Windows` `Linux` このオプションをオンにすると、本製品は、検知した感染したファイルを自動で駆除しようとします。駆除に失敗した場合、ファイルはブロックされます。 **ブロックまたは手動選択（OS により異なります）** `Windows` `Linux` このオプションをオンにすると、本製品は、感染したファイルを駆除または削除することなく、自動的にブロックします。 `macOS` ファイルに感染した悪意のあるオブジェクトの種別に関する情報が通知ウインドウに表示され、実行する処理を選択するよう要求されます。使用可能な処理は、オブジェクトのステータスによって異なる場合があります。 感染したファイルを駆除または削除する前に、本製品は、後でファイルを復元する必要が生じた場合や駆除が可能になった場合に備えて、ファイルのバックアップコピーを作成します。
保護範囲	`Windows` `macOS` `Linux`	ファイル脅威対策によってスキャンされるオブジェクトが含まれています。スキャンオブジェクトには、ハードディスク、リムーバブルドライブ、ネットワークドライブ、フォルダー、ファイル、またはファイル名マスク（複数のファイルを対象に含む）を指定できます。 既定では、ファイル脅威対策はすべてのハードディスク、リムーバブルドライブ、ネットワークドライブで起動したファイルをスキャンします。これらのオブジェクトの保護範囲は変更したり削除することはできません。それぞれのオブジェクト（リムーバブルドライブなど）をスキャンから除外することのみ可能です。 `Linux` Linux デバイスの場合、ファイル脅威対策コンポーネントを使用してスキャン範囲を変更または削除できます。コンポーネントが動作するためには、少なくとも 1 つの保護範囲を指定する必要があります。
File types	`macOS`	**Scan all files**この設定が有効な場合、すべてのファイル（すべての形式と拡張子）が例外なくチェックされます。 **Scan applications and documents by content**この設定を有効にすると、本製品は感染する可能性のあるファイルのみをスキャンします。ファイルで悪意のあるコードをスキャンする前に、ファイルの内部ヘッダーが分析され、ファイルの形式（txt、doc、exe など）が識別されます。また、特定の拡張子を持つファイルも検索します。 **Scan applications and documents by extension**この設定を有効にすると、本製品は感染する可能性のあるファイルのみをスキャンします。ファイル形式はファイルの拡張子に基づいて識別されます。

設定	OS	説明
スキャンの最適化	`Windows` `macOS`	［**スキャンの最適化**］では、ファイルのスキャン中に Kaspersky Endpoint Security のパフォーマンスを向上させる設定が可能です。 • `Windows` `macOS` **新規作成または変更されたファイルのみスキャン**新規ファイルまたは最後にスキャンされたときから変更があったファイルのみスキャンします。このオプションをオンにすると、スキャン時間を短縮できます。このモードは、簡易ファイルと複合ファイルの両方に適用されます。 • `Windows` **駆除できなかった場合はコンテナを停止**：検知されたオブジェクトに対して、本製品に十分な読み取りおよび書き込み権限が付与されていない場合があります。その場合、検知されたオブジェクトの駆除または削除は実行できません。このチェックボックスをオンにすると、本製品は検知されたオブジェクトをブロックし、コンテナを停止します。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検知されたオブジェクトのみをブロックします。 • `macOS` **読み取り専用システムボリュームのスキャンをスキップする**：このチェックボックスをオンにすると、読み取り専用のシステムボリュームはスキャンされません。これにより、スキャン時間を大幅に短縮できます。 • `Windows` **Windows コンテナ内で実行されたファイル操作をスキャンしない**：このチェックボックスをオンにすると、本製品はコンテナの起動時にのみコンテナをスキャンします。チェックボックスをオフにすると、本製品はコンテナをリアルタイムで継続的にスキャンします。
複合ファイルのスキャン	`Windows` `macOS` `Linux`	ウイルスやその他のマルウェアの隠蔽には、アーカイブやデータベースなどの複合ファイルに埋め込む技術が一般的に使用されています。このように隠されたウイルスやその他の脅威を検知するには、複合ファイルを解凍する必要があり、これによりスキャンの速度が低下する場合があります。スキャンする複合ファイル種別を限定することで、スキャンを高速化できます。 • **圧縮ファイル**。これには、ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE およびその他の種類の圧縮ファイルのスキャンが含まれます。本製品は、拡張子だけでなく、形式によっても圧縮ファイルを識別します。圧縮ファイルをスキャンする際、本製品は再帰的な解凍を実行します。これにより、ネストされた圧縮ファイル（圧縮ファイル内の圧縮ファイル）内の脅威を検知できるようになります。 • **配布パッケージと自己解凍型アーカイブ**。サードパーティ 製品のインストールパッケージと自己解凍型アーカイブをスキャンします。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。自己解凍型アーカイブをスキャンするには、［**アーカイブのスキャン**］をオンにします。 • `Windows` `macOS` **Office 形式のファイルと埋め込み OLE オブジェクト**。Microsoft Office ファイル（DOC、DOCX、XLS、PPT など）と、ファイルに埋め込まれた OLE オブジェクト (Excel テーブル、マクロ、メールの添付ファイルなど）をスキャンします。 • `Windows` `Linux` **メールデータベースをスキャン**Microsoft Outlook、Outlook Express、The Bat!、その他のメールクライアントのメールデータベースをスキャンします。 • `Linux` **メール形式のファイルをスキャン**. プレーンテキスト形式のメールメッセージファイルをスキャンします。
次のサイズを超えるアーカイブのバックグラウンド解凍を許可する（MB）	`Windows` `macOS`	このチェックボックスをオンにすると、指定された値よりも大きいサイズの複合ファイルには、これらのファイルをスキャンする前にアクセスできます。この場合、複合ファイルの解凍とスキャンはバックグラウンドで実行されます。 指定された値より小さいサイズの複合ファイルには、これらのファイルを解凍してスキャンした後にのみアクセスできます。 このチェックボックスをオフにすると、すべてのサイズのファイルを解凍してスキャンした後にのみ複合ファイルにアクセスできます。
次のサイズを超えるアーカイブをスキャンしない（MB）	`Windows` `macOS` `Linux`	このチェックボックスをオンにすると、指定されている値を超えるサイズの複合ファイルはスキャンから除外されます。 このチェックボックスをオフにした場合、複合ファイルはサイズに関係なくスキャンされます。 圧縮ファイルから解凍されたサイズの大きいファイルはこのチェックボックスのオンオフに関係なくスキャンされます。
ファイルの最大スキャン時間（秒）	`Linux`	このチェックボックスをオンにすると、指定された時間が経過すると複合ファイルのスキャンを停止します。 値が `0` に設定されている場合、スキャン時間は無制限です。
バックグラウンドスキャン	`Windows`	バックグラウンドスキャンモードでは、Kaspersky Endpoint Security はユーザー向けの通知を表示せずにスキャンを実行します。バックグラウンドスキャンは、その他のスキャン種別（完全スキャンなど）よりも、リソース消費量が少なくなります。このモードでは、Kaspersky Endpoint Security はスタートアップオブジェクト、ブートセクター、システムメモリ、システムパーティションをスキャンします。
コンテキストメニューからのスキャン	`Windows`	Kaspersky Endpoint Security では、個別のファイルに対してウイルスなどのマルウェアを対象とするスキャンをコンテキストメニューから実行できます。 コンテキストメニューからスキャンを実行した時に、Kaspersky Endpoint Security では、OneDrive クラウドストレージ上にコンテンツがあるファイルはスキャンされません。

有害 USB 攻撃ブロック

Windows、Linux 向け

ウイルスの中には、オペレーティングシステムで USB デバイスがキーボードとして検知されるように、USB デバイスのファームウェアを改竄するものがあります。ウイルスはマルウェアなどをダウンロードするためにユーザーのアカウントでコマンドを実行する可能性があります。

有害 USB 攻撃ブロックは、感染した USB デバイスがキーボードの動作を模倣してコンピューターに接続することを防ぎます。

コンピューターに接続された USB デバイスをオペレーティングシステムがキーボードとして識別した場合、製品によって生成された数値コードを、このキーボードまたは使用可能な場合はセキュリティキーボードから入力するようユーザーに要求します（下の図を参照）。この手順をキーボード承認と呼びます。

コードが正しく入力されると、識別パラメータ（キーボードの VID/PID、接続されたポートの番号）が認証キーボードのリストに保存されます。キーボードが再度接続されたときやオペレーティングシステムの再起動後に、認証が繰り返されることはありません。

認証されたキーボードが別のコンピューターの USB ポートに接続されると、このキーボードの認証が再度要求されます。

数値コードが正しく入力されなかった場合、本製品は新しいコードを生成します。数値コードの入力試行回数は指定できます。数値コードの入力を複数回誤ったりキーボードの認証ウィンドウを閉じた場合（下の図を参照）、本製品はキーボードからの入力をブロックします。USB デバイスのブロック時間の経過後もしくはオペレーティングシステムの再起動後に、キーボード認証を再度実行するようユーザーに要求します。

承認されたキーボードの使用は許可され、承認されなかったキーボードの使用はブロックされます。

有害 USB 攻撃ブロックは、既定ではインストールされません。有害 USB 攻撃ブロックが必要な場合は、製品のインストール前にインストールパッケージのプロパティにコンポーネントを追加するか、製品のインストール後に利用可能なコンポーネントを変更できます。



キーボード承認

有害 USB 攻撃ブロックの設定

設定	OS	説明
USB デバイスの最大認証試行回数	Windows Linux	承認コードを指定回数間違って入力すると、USB デバイスを自動的にブロックします。有効な値は 1～10 です。たとえば、認証コードを 5 回まで許可する設定にすると、認証コードの入力を 5 回目に失敗すると本製品は USB デバイスをブロックします。Kaspersky Endpoint Security は、USB デバイスがブロックされている時間を表示します。その時間が経過すると、また認証コードを 5 回まで入力できます。
最大試行回数に達した場合のタイムアウト（分）	Windows Linux	認証コードの入力に指定回数失敗した後の USB デバイスのブロック期間。可能な値：1～180（分）
USB デバイスの認証時にセキュリティキーボードの使用を禁止する	Windows Linux	このトグルスイッチをオンにすると、認証用のコードが入力できない USB デバイスの認証時に、セキュリティキーボードの使用をブロックします。
USB デバイスの認証時にバーコードの使用を禁止する	Windows Linux	このトグルスイッチをオンにすると、 Kaspersky Endpoint Security はバーコードスキャナーの認証の通知にバーコードを表示しません。

リムーバブルドライブのスキャン

Windows、macOS 、Linux 向け

Kaspersky Endpoint Security は、リムーバブルドライブ上にあるファイルでも、実行またはコピーしたすべてのファイルをスキャンします（ファイル脅威対策機能）。ウイルスやその他のマルウェアの拡散を防ぐため、リムーバブルドライブがコンピューターに接続された際に自動でスキャンされるよう設定することができます。Kaspersky Endpoint Security は、検知した感染したファイルをすべて駆除することを自動的に試みます。駆除に失敗した場合、ファイルは削除されます。機械学習やヒューリスティック分析（高レベル）、署名分析を備えたスキャンを実行することでコンピューターの安全を保ちます。Kaspersky Endpoint Security はスキャンの最適化技術の iSwift および iChecker も使用します。これらは常に有効になっており、無効にすることはできません。

リムーバブルドライブスキャンの設定

設定	OS	説明
スキャン種別	Windows Linux	**簡易スキャン**このオプションを選択した場合、リムーバブルドライブが接続されると、感染に対して最も脆弱な特定のファイル形式のファイルのみをスキャンします。複合オブジェクトは解凍しません。 **詳細スキャン**このオプションを選択した場合、リムーバブルドライブが接続されると、Kaspersky Endpoint Security は複合オブジェクト、アーカイブ、配布パッケージ内でネストしたファイルや Office 形式のファイルを含むリムーバブルドライブ上のすべてのファイルをスキャンします。Kaspersky Endpoint Security はメール形式やパスワード保護されたアーカイブのファイルはスキャンしません
ユーザーによるスキャン停止を禁止する	Windows	このチェックボックスをオンにすると、Kaspersky Endpoint Security のローカルインターフェイス内のリムーバブルドライブのスキャンタスクで、［**タスク**］セクションの［**停止**］ボタンおよびリムーバブルドライブのスキャンウィンドウの［**停止**］ボタンが使用できなくなります。
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	Linux	このチェックボックスをオンにすると、Kaspersky Endpoint Security 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へのアクセスをブロックします。
スキャン進捗バーを非表示にする	Windows	このチェックボックスをオンにすると、Kaspersky Endpoint Security はリムーバブルドライブのスキャン進捗バーを非表示にします。アプリケーションはバックグラウンドでスキャンを実行します。 このチェックボックスをオフにすると、リムーバブルドライブのスキャンの進捗が別のウィンドウおよび［**タスク**］セクションに表示されます。
次のサイズを超えるリムーバブルドライブをスキャンしない	Windows	このチェックボックスをオンにすると、Kaspersky Endpoint Security は、指定された最大ドライブサイズ以下のサイズのリムーバブルドライブに対して、選択した処理を実行します。リムーバブルドライブのサイズが設定値を超える場合、Kaspersky Endpoint Security はスキャンをスキップします。 チェックボックスをオフにすると、Kaspersky Endpoint Security は、すべてのサイズのリムーバブルドライブに対して、選択した処理を実行します。

ふるまい検知

Windows、macOS 、Linux 向け

ふるまい検知は、コンピューター上でのアプリケーションの処理に関するデータを取得し、別のコンポーネントのパフォーマンスを向上するために、その情報を提供します。ふるまい検知は、アプリケーションの Behavior Stream Signatures（BSS）を使用します。アプリケーションの動作が BSS のシグネチャと一致する場合、選択された処理が実行されます。Kaspersky Endpoint Security は、Behavior Stream Signatures に基づいて、コンピューターへのプロアクティブディフェンスを実現しています。

さらに、ふるまい検知は、コンピューターのセキュリティを脅かす可能性のあるアプリケーションのプロセスがないかネットワークポートを監視します。本製品は、定義データベースを使用してこのようなプロセスに関する情報を取得します。

脆弱性攻撃ブロックコンポーネントを最適に動作させるには、ふるまい検知コンポーネントを有効にすることをお勧めします。

ふるまい検知の設定

設定	OS	説明
信頼するアプリケーション	`Windows` `macOS` `Linux`	*信頼するアプリケーションのリスト*は、ファイルおよびネットワークの動作（悪意のある動作を含む）やシステムレジストリへのアクセスが Kaspersky Endpoint Security によって監視されないアプリケーションのリストです。既定では、Kaspersky Endpoint Security はすべてのアプリケーションプロセスによってオープン、実行、保存されるオブジェクトを監視し、すべてのアプリケーションとこのようなアプリケーションが生成するネットワークトラフィックの処理を管理します。アプリケーションが信頼するアプリケーションのリストに追加されると、Kaspersky Endpoint Security はアプリケーションのアクティビティの監視を停止します。 Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。
信頼するオブジェクト	`Windows` `macOS` `Linux`	*信頼するオブジェクト*とは、Kaspersky Endpoint Security が特定のオブジェクトについてウイルスなどの脅威のスキャンを実行しないときに、オブジェクトが満たす必要のある一連の条件によって定義されます。スキャン除外により、侵入者がコンピューターやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションを使用できます。こうしたアプリケーションは必ずしも悪意のある目的を持っているわけではありませんが、ハッカーによって悪用される可能性があります。侵入者がコンピューターやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションに関する詳細情報は、カスペルスキー百科事典の Web サイト を参照してください。 Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。
脅威の検知時の処理	`Windows` `macOS` `Linux`	**ファイルの削除またはブロック（OS により異なります）** `Windows` `macOS` このオプションをオンにすると、悪意のある活動を検知した際に、 Kaspersky Endpoint Security は悪意のあるアプリケーションの実行ファイルを削除し、バックアップにファイルのコピーを作成します。 `Linux` 悪意のある活動が検知されると、Kaspersky Endpoint Security は悪意のある活動を実行しているアプリケーションをブロックし、検出された悪意のある活動に関する情報をログに記録します。 **通知する**：`WindowsLinux` このオプションをオンにすると、アプリケーションの悪意のある活動が検知されると、アプリケーションは終了されませんが、悪意のある活動に関する情報がアクティブな脅威のリストに追加されます。 `macOS` 悪意のある活動を検知すると、Kaspersky Endpoint Security は、悪意のある活動が検知された場合に実行する処理を選択するようにユーザーに求めます。使用可能な処理は、オブジェクトのステータスによって異なる場合があります。 **ブロックする**このオプションを選択した場合、悪意のある活動が検知されると、Kaspersky Endpoint Security はそのアプリケーションを終了します。

アンチクリプター

Windows、macOS 、Linux 向け

`Windows` Windows デバイスの場合、コンポーネントは、NTFS ファイルシステムレベルにあり、EFS システムによって暗号化されていないファイルに対する操作のみを監視します。

`Linux` Linux デバイスの場合、コンポーネントは SMB/NFS 経由のネットワークアクセスを使用してローカルディレクトリ内のファイルを分析します。

`macOS` macOS デバイスの場合、コンポーネントは SMB 共有を監視します。

アンチクリプターコンポーネントは、ネットワーク共有内の活動を分析してリモート暗号化から保護します。これらの操作が外部からの暗号化に典型的な Behavior Stream Signatures と一致する場合、選択した処理が実行されます。

`Linux` Linux デバイスでこのコンポーネントを有効にする前に、アンチクリプターに関する情報を必ず確認し、把握しておいてください。

アンチクリプターの設定

設定	OS	説明
信頼するオブジェクト	`Windows` `Linux`	*信頼するオブジェクト*とは、Kaspersky Endpoint Security が特定のオブジェクトについてウイルスなどの脅威のスキャンを実行しないときに、オブジェクトが満たす必要のある一連の条件によって定義されます。スキャン除外により、侵入者がコンピューターやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションを使用できます。こうしたアプリケーションは必ずしも悪意のある目的を持っているわけではありませんが、ハッカーによって悪用される可能性があります。侵入者がコンピューターやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションに関する詳細情報は、カスペルスキー百科事典の Web サイトを参照してください。 Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。
名前または IP アドレスによる除外リスト	`Windows`	**信頼するコンピューター名または IP アドレス**このリストにある、共有フォルダーの暗号化を試行したコンピューターは監視されません。 **マスクによる除外**保護範囲の除外リスト。組織で、共有フォルダーを使用したファイルの交換時にデータ暗号化が使用されている場合、保護範囲からフォルダーを除外することで誤検知の量を減らすことができます。**マスク**を使用します。 • 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。 • 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。 • 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

設定	OS	説明
脅威の検知時の処理	`Windows` `macOS` `Linux`	**通知する**このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、この試みに関する情報がアクティブな脅威のリストに追加され、レポートにエントリが追加されます。 **接続をブロックする時間（分）** `Windows` このオプションを選択した場合、Kaspersky Endpoint Security は共有フォルダーにあるファイルを変更する試用を検知すると、悪意のある活動を開始したセッションのファイル変更に対するアクセスをブロックし、変更されたファイルのバックアップコピーを作成します。 `macOS` `Linux` 共有フォルダー内のファイル変更の試行を検知すると、Kaspersky Endpoint Security は悪意のある活動を実行している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。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*暗号化が検知されました*イベントを作成します。
保護範囲	`Windows` `macOS` `Linux`	*保護範囲*は、Kaspersky Endpoint Security がファイルの動作を監視する共有フォルダーへのパスのリストです。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。既定では、本製品は共有フォルダーを自動的に識別し、すべてのフォルダー内のファイルの動作を監視します。 `macOS` Kaspersky Endpoint Security は macOS デバイスのすべての共有フォルダーを保護します。保護範囲を変更することはできません。 `Windows` `Linux` 保護範囲を選択できます： **保護対象デバイス上のすべてのネットワーク共有フォルダー**本製品は、すべての共有フォルダー内のファイルの動作を監視します。 **指定した共有フォルダーのみ**本製品は、指定された共有フォルダー内でのみ暗号化の試行を監視します。

脆弱性攻撃ブロック

Windows、macOS 、Linux 向け

脆弱性攻撃ブロックは、コンピューター上の脆弱性を悪用して管理者権限を取得したり悪意のある活動を実行しようとするプログラムコードを検知します。たとえば、脆弱性を悪用した攻撃の例としては、バッファーオーバーフロー攻撃などがあります。この攻撃では、脆弱性のあるアプリケーションに大量のデータが送信され、このデータの処理中に、悪意のあるコードが脆弱性のあるアプリケーションによって実行されてしまいます。この攻撃により、不正にマルウェアをインストールされてしまう可能性があります。ユーザー以外の第三者が、脆弱性のあるアプリケーションから実行ファイルを実行しようとすると、Kaspersky Endpoint Security は、このファイルの起動をブロックしてユーザーに通知します。

さらに、脆弱性攻撃ブロックは、コンピューターのセキュリティを脅かす可能性のあるアプリケーションのプロセスがないかネットワークポートを監視します。本製品は、定義データベースを使用してこのようなプロセスに関する情報を取得します。

脆弱性攻撃ブロックコンポーネントが機能するには、ふるまい検知コンポーネントが有効になっている必要があります。脆弱性攻撃ブロックコンポーネントを最適に動作させるには、 ウェブ脅威対策コンポーネントも有効にすることを推奨します。

`Linux` Linux デバイスの場合、システムイベントの読み取り用のアップデート可能なカーネルモジュールも有効にする必要があります。

脆弱性攻撃ブロックの設定

設定	OS	説明
脅威の検知時の処理	`Windows` `macOS` `Linux`	**通知する**この項目を選択すると、脆弱性攻撃の検知時に、その脆弱性攻撃に関する情報を含むエントリがログに記録されて、アクティブな脅威のリストにその脆弱性攻撃に関する情報が追加されます。 **ブロックする**この項目を選択した場合、攻撃が検知されると、その攻撃による操作がブロックされ、攻撃に関する情報がログに記録されます。
システムプロセスのメモリ保護	`Windows`	このオプションをオンにすると、システムプロセスメモリへアクセスしようとする外部プロセスをブロックします。

通信と危険サイト対策

メール脅威対策

Windows、macOS 、Linux 向け
メール脅威対策保護コンポーネントは、受信メールおよび送信メールの添付ファイルをスキャンして、ウイルスやその他の脅威となるアプリケーションを検知します。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、およびヒューリスティック分析を使用してコンピューターを保護します。

メール脅威対策は、受信メッセージだけでなく送信メッセージもスキャンすることができます。本製品は、POP3、SMTP、IMAP、NNTP プロトコルをサポートしています。

> `Linux` Linux デバイス用のアプリケーションは NNTP プロトコルをサポートしていません。

サポート対象のメールクライアント

- `Windows`、`macOS` Microsoft Office Outlook
- `Windows`、`macOS` Mozilla Thunderbird
- `Windows` Windows Mail
- `Windows`、`Linux` MyOffice Mail
- `Windows`、`Linux` R7-Office Organizer
- `macOS` Apple Mail
- `macOS` Canary Mail
- `macOS` Spark
- `macOS` Mimestream
- `macOS` Airmail
- `macOS` Post Box
- `macOS` Boxy Suite 2
- `macOS` Twobird
- `macOS` Shift
- `macOS` Clean Email
- `macOS` eM Client

- macOS Superhuman
- macOS Polymail
- macOS HEY
- macOS Mail+ for Gmail
- macOS Spike mail

Windows メール脅威対策は、メッセージにプロトコルレベルでアクセスできるとは限りません（たとえば、Microsoft Exchange ソリューションを使用する場合）。このため、メール保護には、Microsoft Office Outlook 向けの拡張機能である Kaspersky ASAP Outlook Plugin が含まれています。この拡張機能により、メールクライアントレベルでメッセージをスキャンすることができます。Kaspersky ASAP Outlook Plugin は Outlook 2010、2013、2016、2019 および 2021 の操作をサポートします。

メールクライアントがブラウザーで開いている場合、メール脅威対策はメッセージをスキャンしません。

添付ファイルに悪意のあるファイルが検知されると、Kaspersky Endpoint Security は実行された処理に関する情報をメッセージの件名に追加して、件名を「*[Message has been processed]* <*メッセージの元の件名*>」のように変更します。

メール保護の設定

設定	OS	説明
信頼するオブジェクト	Windows macOS Linux	*信頼するオブジェクト*とは、Kaspersky Endpoint Security が特定のオブジェクトについてウイルスなどの脅威のスキャンを実行しないときに、オブジェクトが満たす必要のある一連の条件によって定義されます。スキャン除外により、侵入者がコンピューターやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションを使用できます。こうしたアプリケーションは必ずしも悪意のある目的を持っているわけではありませんが、ハッカーによって悪用される可能性があります。侵入者がコンピューターやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションに関する詳細情報は、カスペルスキー百科事典の Web サイト を参照してください。 Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。
脅威の検知時の処理	Windows macOS Linux	**駆除する。駆除できない場合は削除する**感染したオブジェクトが送受信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。その後、安全な添付ファイル付きのメッセージがユーザーに提供されます。駆除に失敗した場合、本製品は感染したオブジェクトを削除します。本製品は、実行された処理に関する情報をメッセージの件名に追加します（例：*[メッセージが処理されました]* <*メッセージの件名*>）。 Windows Linux **駆除する。駆除できない場合はブロックする**受信メッセージで感染したオブジェクトが検知された時は、検知されたオブジェクトの駆除を試行します。その後、安全な添付ファイル付きのメッセージがユーザーに提供されます。駆除に失敗した場合は、メッセージの件名に警告が追加されます。その後、元の添付ファイルのあるメッセージがユーザーに提供されます。感染したオブジェクトが送信メッセージで検知された場合、本製品は検知されたオブジェクトの駆除を試みます。オブジェクトを駆除できなかった場合、本製品はメッセージの送信をブロックし、メールクライアント上にエラーメッセージが表示されます。 **ブロックする**受信メッセージで感染したオブジェクトが検出されると、本製品はメッセージの件名に警告を追加します。その後、元の添付ファイルのあるメッセージがユーザーに提供されます。送信メッセージで感染したオブジェクトが検出されると、本製品はメッセージをブロックし、メールクライアントにエラーが表示されます。 Linux Linux デバイスの場合、メール脅威対策コンポーネントは送信メッセージ内の感染したオブジェクトの駆除を試みませんが、メッセージの送信を直ちにブロックします。
POP3、SMTP、NNTP、IMAP トラフィックのスキャン	Windows	POP3、SMTP、NNTP、IMAP プロトコル経由で送信されるメールをメール脅威対策でスキャンします。

設定	OS	説明
Microsoft Outlook アドインに接続	`Windows`	このチェックボックスをオンにすると、POP3、SMTP、NNTP、IMAP プロトコルで送信されるメールのスキャンは、Microsoft Outlook に組み込まれた拡張機能側で有効になります。本製品は、さまざまな段階で Microsoft Outlook からの送受信メッセージをスキャンできます。 • **メール受信時にスキャンする**このチェックボックスをオンにすると、本製品は Microsoft Outlook 経由でメッセージを受信するときにメール脅威対策を使用します。 • **メール閲覧時にスキャンする** • **メール送信時にスキャンする** メールのスキャンに Microsoft Outlook 用機能拡張を使用している場合は、Cached Exchange Modeを使用してください。Exchange キャッシュモードの詳細および使用に関する推奨事項は、マイクロソフトサポート技術情報を参照してください。
添付のアーカイブのスキャン	`Windows` `Linux`	これには、ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE およびその他の種類の圧縮ファイルのスキャンが含まれます。本製品は、拡張子だけでなく、形式によっても圧縮ファイルを識別します。圧縮ファイルをスキャンする際、本製品は再帰的な解凍を実行します。これにより、ネストされた圧縮ファイル（圧縮ファイル内の圧縮ファイル）内の脅威を検知できるようになります。
添付の Office 形式ファイルをスキャン	`Windows` `Linux`	Microsoft Office 形式のファイルをスキャンします（DOC、DOCX、XLS、PPT およびその他の Microsoft 形式のファイル）。Office 形式のファイルには OLE オブジェクトが含まれます。本製品は、このチェックボックスが選択されているかどうかに関係なく、1 MB 未満のオフィス形式の添付ファイルをスキャンします。
次のサイズを超えるアーカイブをスキャンしない（MB）	`Windows` `macOS` `Linux`	このチェックボックスをオンにすると、メール脅威対策では、指定された制限を超える添付圧縮ファイルがスキャン対象から除外されます。このチェックボックスをオフにすると、メール脅威対策はあらゆるサイズの添付圧縮ファイルをスキャンします。
ファイルの最大スキャン時間（秒）	`Windows` `macOS` `Linux`	このチェックボックスをオンにすると、メールに添付ファイルとして送信された圧縮ファイルのスキャン期間が制限されます。
添付ファイルのフィルター	`Windows` `Linux`	添付ファイルのフィルター機能は、メール脅威対策がメールに添付されたファイルに適用する処理を決定します。 添付ファイルのフィルター機能は、送信されるメールには適用されません。 • **添付ファイルを変更しない**このオプションを選択すると、メール脅威対策はメールメッセージに添付ファイルをフィルターしません。 • **選択した種別の添付ファイルの名前を変更する**このオプションを選択すると、メール脅威対策は、指定されたファイルの種別（添付ファイル.doc_ など）の拡張子の最後の文字をアンダースコア文字に置き換えます。したがって、ファイルを開くには、ユーザーはファイルの名前を変更する必要があります。 • **選択した種別の添付ファイルを削除する**このオプションを選択すると、メール脅威対策は指定された種別の添付ファイルをメールメッセージから削除します。 ファイルマスクのリストで、メールメッセージから名前を変更したり削除したりする添付ファイルの種別を指定できます。

ウェブ脅威対策

Windows、macOS 、Linux 向け

ウェブ脅威対策は、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ぎ、悪意のある Web サイトやフィッシングサイトをブロックします。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、およびヒューリスティック分析を使用してコンピューターを保護します。

ウェブ脅威対策コンポーネントは、受信 HTTP、HTTPS、FTP トラフィック、Web サイト、IP アドレスをスキャンします。

`Linux` ウェブ脅威対策は既定で無効になっています。ウェブアンチウイルスを有効にすると、インストールされているサードパーティアプリケーションとオペレーティングシステムのパフォーマンスが低下する可能性があります。Linux デバイスでウェブアンチウイルスを有効にするためのアプリケーションの設定の詳細については、テクニカルサポートのナレッジベースを参照してください。

ウェブアンチウイルスの設定

設定	OS	説明
信頼する Web アドレス	`Windows` `macOS` `Linux`	ウェブ脅威対策が信頼すると判断する Web アドレスのリスト。コンポーネントは、これらのアドレスからの送受信トラフィックについて、脅威をスキャンしません。信頼するアドレスのリストは、既知の Web サイトからのファイルのダウンロードが、ウェブ脅威対策によって妨げられる場合などに使用することができます。 信頼する URL のリストには、Web ページ / Web サイトのアドレスとアドレスマスクの両方を追加できます。Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。
信頼するオブジェクト	`Windows`	*信頼するオブジェクト*とは、Kaspersky Endpoint Security が特定のオブジェクトについてウイルスなどの脅威のスキャンを実行しないときに、オブジェクトが満たす必要のある一連の条件によって定義されます。スキャン除外により、侵入者がコンピューターやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションを使用できます。こうしたアプリケーションは必ずしも悪意のある目的を持っているわけではありませんが、ハッカーによって悪用される可能性があります。侵入者がコンピューターやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションに関する詳細情報は、カスペルスキー百科事典の Web サイトを参照してください。 Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。
脅威の検知時の処理	`Windows` `macOS` `Linux`	**ブロックする** このオプションがオンの場合、Web トラフィック内に感染したオブジェクトを検知すると、ウェブ脅威対策はこのオブジェクトへのアクセスをブロックし、処理に関するメッセージをブラウザー上に表示します。 **許可する、通知する、または手動選択（OS により異なります）** `Windows` このオプションを選択した場合、感染したオブジェクトが Web トラフィックで検知されると、オブジェクトのコンピューターへのダウンロードは許可されますが、感染したオブジェクトに関する情報がアクティブな脅威のリストに追加されます。 `macOS` Web トラフィックオブジェクトに感染したマルウェアの種別の情報が通知に表示され、このオブジェクトに実行する処理を選択するよう要求されます。使用可能な処理は、オブジェクトのステータスによって異なる場合があります。 `Linux` Kaspersky Endpoint Security は、Web トラフィックで感染したオブジェクトが検知されたことをユーザーに通知します。ウェブ脅威対策により、このオブジェクトをデバイスにダウンロードできます。その時点で、アプリケーションは感染した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。

ネットワーク脅威対策

Windows、macOS 、Linux 向け

*ネットワーク脅威対策*コンポーネント（侵入検知システム、Intrusion Detection System、IDS とも呼ばれます）は、ネットワーク攻撃に特徴的な活動がないか受信ネットワークトラフィックを監視します。本製品は、ユーザーのコンピューターへのネットワーク攻撃の試行を検知すると、攻撃しているコンピューターとのネットワーク接続をブロックします。現在知られているタイプのネットワーク攻撃の説明とそれらに対抗する方法は、定義データベースで提供されています。ネットワーク脅威対策が検知するネットワーク攻撃のリストは、定義データベースと製品機能のアップデート時にアップデートされます。

`Linux` ネットワーク脅威対策は既定で無効になっています。ネットワーク脅威対策を有効にすると、インストールされているサードパーティアプリケーションとオペレーティングシステムのパフォーマンスが低下する可能性があります。Linux デバイスでのネットワーク脅威対策を有効にするアプリケーションの設定の詳細については、テクニカルサポートのナレッジベースを参照してください。

ネットワーク脅威対策の設定

設定	OS	説明
信頼する IP アドレス	`Windows` `Linux`	信頼するデバイスの IP アドレスのリスト。ネットワーク脅威対策コンポーネントは、これらのアドレスからのネットワーク動作をブロックしません。 `Windows` ポートおよびプロトコルを指定した IP アドレスを追加することができます。 `Linux` 除外リストに追加できるのは IP アドレスのみです。 また、除外リストに含まれる IP アドレスからのネットワーク攻撃に関する情報は、ログに記録されません。

設定	OS	説明
脅威の検知時の処理	`Windows` `macOS` `Linux`	**ブロックする**脅威が検知されると、ネットワーク脅威対策は攻撃をブロックします。 **攻撃をブロックし、攻撃元の端末をブロックする時間（分）**このオプションを有効にすると、ネットワーク脅威対策は攻撃コンピューターをブロックリストに追加します。つまり、ネットワーク脅威対策は、最初のネットワーク攻撃が試行された後、攻撃コンピューターとのネットワーク接続を一定の時間ブロックします。これにより、同じアドレスからの以降のネットワーク攻撃の可能性に対して、ユーザーのコンピューターが自動的に保護されます。ブロックリストに追加された攻撃元コンピューターをブロックする時間の最小値は1分です。最大値は999分です。 Kaspersky Endpoint Security は、アプリケーションが再起動されたときとネットワーク脅威対策の設定が変更されたときにブロックリストを消去します。
ポートのスキャンおよびネットワークフラッディングを攻撃として扱う	`Windows`	*ポートのスキャン*とは、コンピューターの UDP ポート、TCP ポート、ネットワークサービスをスキャンする攻撃を意味します。これにより、攻撃者がコンピューターの脆弱性を把握して、より悪質な攻撃を仕掛けることができるようになります。また、コンピューターのオペレーティングシステムを識別し、そのオペレーティングシステムに適したネットワーク攻撃を行うためにポートがスキャンされることもあります。 *ネットワークフラッディング*とは、Web サーバーなど、企業のネットワークリソースに対する攻撃を意味します。これは、大量のリクエストを送信し、ネットワークリソースの帯域幅をオーバーロードさせる攻撃です。攻撃されると、ユーザーは企業のネットワークリソースにアクセスできなくなります。 このチェックボックスをオンにすると、Kaspersky Endpoint Security はこれらの攻撃を検知するためネットワークトラフィックを監視します。攻撃が検知されると、ユーザーへの通知に加え、対応するイベントが Kaspersky Security Center に送信されます。また、脅威の対応処理を迅速に行うために必要な、攻撃元のコンピューターに関する情報が提供されます。 一部の許可されるアプリケーションがこのような攻撃と似た動作を行う場合は、これらの検知機能を無効にすることができます。これにより誤検知を減らすことができます。
MAC スプーフィング対策	`Windows`	*MAC スプーフィング攻撃*では、ネットワークデバイス（ネットワークカード）の MAC アドレスを変更します。その結果、攻撃者はデバイスに送信されたデータを別のデバイスにリダイレクトし、このデータにアクセスすることができます。Kaspersky Endpoint Security で MAC スプーフィング攻撃をブロックし、攻撃に関する通知を管理者に送信できます。

ファイアウォール

Windows、macOS 、Linux 向け

ファイアウォールは、インターネットまたはローカルネットワークでの作業中に、コンピューターへの不正な接続をブロックします。ファイアウォールは、コンピューター上のアプリケーションのネットワーク動作も制御します。これにより、個人情報の盗難やその他の攻撃から企業 LAN を保護できます。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、および事前定義された*ネットワークルール*を使用してコンピューターを保護します。

`Linux` Linux デバイスの場合、アプリケーションはファイアウォール管理コンポーネントを使用します。このコンポーネントは、オペレーティングシステムのファイアウォールの設定とルールを管理します。

設定	OS	説明
ネットワークパケットルール	`Windows` `macOS` `Linux`	ネットワークパケットルールのリストのテーブル。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に制限を加えるために使用します。このルールにより、選択したデータプロトコルの、特定のポートを通じた、受信ネットワークトラフィックと送信ネットワークトラフィックが制限されます。 このテーブルには、Microsoft Windows および Linux オペレーティングシステムで動作しているコンピューターのネットワークトラフィックを最適に保護するために、カスペルスキーが推奨する設定済みのネットワークパケットルールがリスト表示されます。 ファイアウォールでは、各ネットワークパケットルールに実行優先度が設定されます。ファイアウォールは、ネットワークパケットルールのリストに表示されているネットワークパケットルールを、上から下に順番に処理します。ネットワーク接続ごとに適用可能な最上位のネットワークパケットルールが検出され、ネットワークの動作を許可またはブロックすることによって、そのルールが適用されます。それぞれのネットワーク接続に対して、適用されたルールよりも優先度が低いネットワークパケットルールはすべてファイアウォールによって無視されます。 ネットワークパケットルールの優先順位は、アプリケーションのネットワークルールよりも高くなります。
使用可能なネットワーク	`Windows` `macOS` `Linux`	このテーブルには、ファイアウォールによって検知されるコンピューターのネットワーク接続に関する情報が表示されます。 既定では、［**パブリックネットワーク**］タイプがインターネットに割り当てられます。インターネットの種別は変更できません。 利用可能なネットワーク接続の種別は次のとおりです： • **パブリックネットワーク**ネットワークは、ウイルス対策アプリケーション、ファイアウォール、またはフィルター（カフェの Wi-Fi など）によって保護されていません。ユーザーがこのようなネットワークに接続されたコンピューターを操作すると、Firewall はこのコンピューターのファイルやプリンターへのアクセスをブロックします。外部ユーザーが、このコンピューターの共有フォルダーからデータにアクセスすることも、このコンピューターのデスクトップにリモートアクセスすることもできません。ファイアウォールは、各アプリケーションのネットワークの動作を、各アプリケーションに設定されたネットワークルールに従ってフィルタリングします。 • **プライベートネットワーク**このコンピューター上のファイルやプリンターへのアクセスが制限されているユーザーのネットワーク（企業 LAN やホームネットワークなど）。 • **信頼するネットワーク**コンピューターが攻撃や不正なデータアクセスの危険にさらされていない安全なネットワーク。このステータスのネットワーク内では、Firewall はすべてのネットワークアクティビティを許可します。
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	`macOS` `Linux`	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。
アプリケーション権限と保護対象のリソース	`Windows`	**アプリケーション**ファイアウォールコンポーネントによって制御されるアプリケーションのテーブル。アプリケーションは信頼グループに割り当てられます。信頼グループは、アプリケーションのネットワーク動作を制御するときに Kaspersky Endpoint Security が使用する権限を定義します。 ポリシーの影響下でコンピューターにインストールされているすべてのアプリケーションの 1 つのリストからアプリケーションを選択し、そのアプリケーションを信頼グループに追加できます。 **ネットワークルール**信頼グループの一部であるアプリケーションのネットワークルールの表。これらのルールに従って、ファイアウォールは、アプリケーションのネットワークの動作を制限します。 この表には、カスペルスキーの専門家が推奨する定義済みネットワークルールが表示されます。これらのネットワークルールは、Windows オペレーティングシステムを実行しているコンピューターのネットワークトラフィックを最適に保護するために追加されました。定義済みネットワークルールを削除することはできません。

セキュリティコントロール

デバイスコントロール

Windows、macOS 、Linux 向け

デバイスコントロールは、コンピューターに内蔵ないし接続されているデバイスへのユーザーアクセスを管理します（例：ハードディスク、カメラ、Wi-Fi モジュール）。これにより、こうしたデバイスが接続されたときにコンピューターを感染から保護し、データの損失や漏洩を防ぐことができます。

デバイスコントロールは、次のレベルでデバイスへのアクセスを許可またはブロックします。

- **デバイス種別**：プリンター、リムーバブルドライブ、CD/DVD ドライブなどの種別。
- **接続バス**：*接続バス*とは、デバイスへのデバイスの接続に使用されるインターフェイスです（例：USB、FireWire）。デバイス種別に［**バスに依存**］モードが選択されている場合、本製品はデバイスが接続されるバスのモード（USB など）に従ってデバイスへのアクセスをコントロールします。
- **信頼するデバイス**：*信頼するデバイス*は、指定されたユーザーまたはユーザーグループが常にフルアクセスできるデバイスです。

  次のデータに基づいて信頼するデバイスを追加できます。

  - `Windows` `macOS` **モデル**各デバイスには製造元 ID（VID）および製品 ID（PID）があります。これらの ID は、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。VID および PID の入力用テンプレート：`VID_1234&PID_5678`。組織内で特定のモデルのデバイスを使用する場合は、モデルでデバイスを追加すると便利です。この方法を使用することで、このモデルのデバイスをすべて追加できます。
  - **ID**各デバイスには固有の識別子があります（ハードウェア ID、または HWID）。これらの ID は、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。デバイス ID の例：`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`。特定のデバイスを複数追加する場合は、ID でデバイスを追加すると便利です。
  - `Windows` `macOS` **モデルマスクによるデバイス**。同一の VID または PID を持つ複数のデバイス（たとえば、製作元が同じデバイス）を使用している場合、マスクを使用してデバイスを信頼リストへ追加できます。`*` 文字は、任意の文字列を置き換えます。`?` 文字は、任意の 1 文字を置き換えます。例：「`VID_05AC&PID_*`」。
  - **ID マスクによるデバイス**：ID が類似する複数のデバイスを使用している場合、マスクを使用してデバイスを信頼リストに追加できます。`*` 文字は、任意の文字列を置き換えます。`?` 文字は、任意の 1 文字を置き換えます。例：「`WDC_C*`」。

`Linux` Linuxデバイスの場合、コンポーネントが実行する処理は、［全般設定］セクションの［検知の設定］サブセクションで選択されたファイル操作の読み取りモードによって異なります。

デバイスコントロールの設定

設定	OS	説明
信頼するデバイス	`Windows` `macOS` `Linux`	信頼するデバイスと、それぞれのデバイスに対してアクセス権が付与されているユーザーのリストです。 Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。

設定	OS	説明
メッセージのテンプレート	Windows Linux	**ユーザーへのメッセージ**ユーザーがブロック対象のデバイスにアクセスしようとしたときに表示されるメッセージのテンプレート。ユーザーが、アクセスがブロックされているデバイスに含まれるファイルに対するファイル操作を試行した場合にも、このメッセージが表示されます。 **管理者へのメッセージ**そのデバイスへのアクセスが誤ってブロックされている場合、またはデバイスの操作が誤ってブロックされている場合に、ユーザーが LAN 管理者に送信するメッセージのテンプレートが含まれています。
一時アクセスの要求を許可する	Windows Linux	このチェックボックスをオンにすると、Kaspersky Endpoint Security のローカルインターフェイスで［**アクセス要求**］が有効になります。このボタンを使用して、ユーザーはブロックされたデバイスへの一時アクセスを要求できます。
操作モード	Linux	Kaspersky Endpoint Security は、デバイスコントロールの設定に従ってアクセスがブロックされているデバイスへのアクセスが試行されたときに、選択した処理を実行します。 • **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が検知されるとイベントを生成します。 • **ブロックする**このオプションをオンにすると、Kaspersky Endpoint Security はデバイスまたはバスに設定されたアクセスモードを適用します。
デバイスと Wi-Fi ネットワーク	Windows macOS Linux	それぞれのアクセスルールのステータスなど、デバイスコントロールの分類に従って、すべての使用可能なデバイス種別のリストが表示されます。
接続バス	Windows Linux	それぞれのアクセスルールのステータスなど、デバイスコントロールの分類に従って、すべての使用可能な接続バスのリストが表示されます。Kaspersky Endpoint Security は、**接続バスに依存**モードが選択されている場合、接続バスの種別に応じてデバイスへのアクセスを許可または拒否します。
アンチブリッジ	Windows	アンチブリッジは、ネットワークブリッジの作成をブロックし、コンピューターで複数のネットワーク接続が同時に確立することを防止します。この機能を使用することで、セキュリティ保護が不十分で接続が許可されていないネットワークから社内ネットワークを保護できます。 アンチブリッジは、デバイスの優先度を参照することで、複数のネットワーク接続の確立をブロックします。デバイスのリスト上の位置が高くなるほど、優先度が高くなります。 現在有効な接続と新しい接続の種別が同じ場合（たとえば、両方とも Wi-Fi など）、Kaspersky Endpoint Security は現在有効な接続をブロックし、新しい接続の確立を許可します。 現在有効な接続と新しい接続の種別が異なる場合（たとえば、1つはネットワークアダプターでもう1つは Wi-Fi など）、Kaspersky Endpoint Security は優先度が低い方の接続をブロックし、優先度が高い方の接続を許可します。 アンチブリッジの使用がサポートされるのは、次の種別のデバイスです：ネットワークアダプター、Wi-Fi、モデム。

ウェブコントロール

Windows、macOS 、Linux 向け

ウェブコントロールでは、ユーザーによる Web リソースへのアクセスが管理されます。これにより、トラフィック消費量を削減し、業務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。

Web サイトへのアクセスルール

ウェブコントロールは、*アクセスルール*を使用して Web サイトへのユーザーアクセスを管理します。次のスキャン領域について Web サイトへのアクセスを構成できます。

- **Web サイトのカテゴリ**：Web サイトは、Kaspersky Security Network クラウドサービス、ヒューリスティック分析、（定義データベースに含まれる）既知の Web サイトのデータベースによってカテゴリ分けされます。［*SNS*］やその他のカテゴリなど、特定のカテゴリへのユーザーアクセスを制限することができます。

- `Windows` **データ種別**：Web サイトのデータへのユーザーのアクセスを制限して、画像を表示できないようにするなどの使い方ができます。Kaspersky Endpoint Security は、ファイルの拡張子ではなくファイル形式に基づいてファイル種別を判定します。

  圧縮ファイル内のファイルはスキャンされません。つまり、たとえば圧縮ファイル内に画像ファイルが含まれていた場合、Kaspersky Endpoint Security はデータ種別を「*アーカイブ*」として識別し、「*グラフィックファイル*」とは識別しません。

- **個別のアドレス**：URL を入力したり、マスクを使用して Web アドレスを指定できます。

Web サイトへのアクセスを管理するために、複数の設定を同時に組み合わせて使用できます。たとえば、Web サイトのカテゴリが「*Web メール*」の場合にのみ「*Office のファイル*」へのアクセスを制限するような使い方ができます。

ウェブコントロールでは、Web サイトへのアクセスルールに関して、次の詳細設定を構成することもできます。

- **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グループ**

  ブラウザーによるインターネットアクセスを制限するときに、IT 部門以外の社内ユーザーを対象にするような使い方ができます。

- **デバイスアクセススケジュール**

  ブラウザーによるインターネットアクセスを制限するときに、対象時間を就業時間中のみに限定するような使い方ができます。

ウェブコントロールの設定

設定	OS	説明
メッセージのテンプレート	`Windows` `Linux`	**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。 **ブロックに関するメッセージ**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適用される際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**企業のネットワークの管理者に送信されるメッセージのテンプレート。Web リソースへのアクセスが誤ってブロックされたとユーザーが判断した場合に使用されます。 メッセージのテンプレートの管理用に特別な変数が用意されています（例：`%USER_NAME%`）。変数を使用すると、単一のメッセージテンプレートを異なるコンピューターで使用できます。
ルールリスト	`Windows` `macOS` `Linux`	Web リソースアクセスルールのリストです。それぞれのルールには優先順位が割り当てられています。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。ある Web サイトが複数のルールの対象に追加されている場合、ウェブコントロールでは、優先順位の最も高いルールに基づいてこの Web サイトへのアクセスを制限します。
既定の動作	`Windows` `macOS` `Linux`	他のルールの対象範囲に含まれない Web リソースへのアクセスルールです。次の設定方法があります： • **ルールリスト以外をすべて許可する** • **ルールリスト以外をすべて禁止する**

設定	OS	説明
ルール適用後にアクティブなブラウザーセッションを終了する	`Windows`	このチェックボックスをオンにすると、ウェブコントロールにより、ポリシーの適用直後に、ブロックされた Web リソースへの接続が終了します。ブラウザーで、Web サイトからのデータのダウンロードがすぐに停止されます。Web サイトを更新したり、禁止されている別の Web サイトに移動したりすると、警告が表示されます。 ウェブコントロールで接続をすぐに終了できるのは、ブラウザーの Web リソースのみです。その他のアプリケーションについては、新しい接続しか制限されません。 チェックボックスをオフにした場合は、ウェブコントロールで、禁止された Web リソースへの新しい接続しか制限されません。アクティブな接続は終了されません。
Web セッションの監視	`Windows`	Kaspersky Endpoint Security は、許可されている Web サイトも含めて、すべての Web サイトへのアクセスに関するデータをログに記録します。Kaspersky Endpoint Security は、イベントを Kaspersky Security Center、Windows イベント ログ、およびレポートに送信します。ユーザーが行うインターネット上での活動を監視するには、イベントの保存に関する設定を指定する必要があります。 監視機能をサポートするブラウザー：Microsoft Edge、Microsoft Internet Explorer、Google Chrome、Yandex Browser、Mozilla Firefox。ユーザーの操作履歴の監視はその他のブラウザーでは動作しません。 ユーザーが行うインターネット上での活動を監視すると、HTTPS トラフィックの復号のためにより多くのコンピューターリソースを消費する可能性があります。

アプリケーションコントロール

Windows、Linux 向け

アプリケーションコントロールは、ユーザーのコンピューター上のアプリケーションの起動を管理します。これにより、アプリケーションを使用するときに企業のセキュリティポリシーを実装できます。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アクセスを制限することにより、コンピューター感染のリスクも減らします。

アプリケーションコントロールコンポーネントは、ルールを使用して保護対象デバイス上のアプリケーションの起動を管理します。ルールには、ルールが適用されたときにアプリケーションコントロールコンポーネントが実行する条件と処理が含まれます。たとえば、アプリケーションが属するカテゴリなどです。*アプリケーションカテゴリ*は、共通点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。

管理者は複数のルールを作成できます。1つのアプリケーションが複数のルールの条件に一致する場合があります。ブロックルールの優先度は、許可ルールの優先度よりも高くなります。Kaspersky Endpoint Security は、アプリケーションが起動されるたびに、ルールに一致するかどうかをチェックします。すべてのアプリケーションコントロールルールに対して、アプリケーションが順次照合されます。

設定	OS	説明
メッセージのテンプレート	Windows	**ユーザーへのメッセージ**：アプリケーションの開始をブロックするアプリケーションコントロールルールが適用される際に表示されるメッセージのテンプレート。 **管理者へのメッセージ**：アプリケーションが誤ってブロックされたとユーザーが考える場合に、ユーザーが企業 LAN 管理者に送信できるメッセージのテンプレート。
操作モード	Windows Linux	次のいずれかのオプションを選択できます： • **ルールリスト以外をすべて許可する**このオプションをオンにすると、すべてのユーザーに対してあらゆるアプリケーションの起動を許可します。ただし、アプリケーションがアプリケーションコントロールのブロックルールで禁止されている場合は除きます。 • **ルールリスト以外をすべて禁止する**このオプションをオンにすると、すべてのユーザーに対してあらゆるアプリケーションの起動をブロックします。ただし、アプリケーションがアプリケーションコントロールの許可ルールで許可されている場合は除きます。
アプリケーションの開始時の処理	Windows Linux	• **ルールを適用**Kaspersky Endpoint Security は選択したモードに従ってアプリケーションの開始を管理します。 • **通知する**Kaspersky Endpoint Security は、アプリケーションの実行試行について通知します。
ポリシーのルールをローカルルールに追加	Linux	このオプションを選択した場合、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、ポリシーで設定されたルールを適用します。
厳密なデジタル署名検証を使用する	Windows	アプリケーションコントロールルールの適用条件として証明書を選択できます。 このチェックボックスをオンにすると、Kaspersky Endpoint Security は、信頼するシステム証明書ストアの証明書で署名されたアプリケーションにのみルールを適用します。このような証明書で署名されたアプリケーションは、さらに、マルウェアのスキャンタスクなどの保護機能によって信頼されていると判断されます。ただし、アプリケーションコントロールルールで別のストアの証明書を指定した場合、そのルールは適用されません。 チェックボックスをオフにすると、Kaspersky Endpoint Security は、Windows の信頼するルート証明書ストアの証明書で署名されたアプリケーションにルールを適用します。このようなアプリケーションは信頼ゾーンに含まれません。保護機能により、このようなアプリケーションの動作が監視されます。
DLL モジュールの読み込みの監視	Windows	このチェックボックスをオンにすると、ユーザーがアプリケーションの起動を試行した際に、DLL モジュールの読み込みを管理します。DLL モジュールの情報およびこの DLL モジュールを読み込んだアプリケーションの情報が、レポートに記録されます。 どの DLL モジュールとドライバーを読み込むかを管理する機能を有効にする場合、［アプリケーションコントロール］で、既定の［**ゴールデンイメージ**］ルールまたは［**ゴールデンイメージ\信頼済み証明書**］KL カテゴリを含み信頼する DLL モジュールとドライバーが Kaspersky Endpoint Security の起動前に読み込まれるように設定した別のルールを有効にしてください。［**ゴールデンイメージ**］ルールが無効なときに DLL モジュールとドライバーの読み込みの管理を有効にすると、オペレーティングシステムが不安定になる場合があります。 Kaspersky Endpoint Security は、［DLL とドライバーを管理］をオンにした後で読み込まれた DLL モジュールとドライバーのみを監視します。チェックボックスをオンにした後、Kaspersky Endpoint Security の起動前に読み込まれるものも含めすべての DLL モジュールとドライバーを確実に監視するため、コンピューターの再起動を推奨します。
ルール	Windows Linux	保護対象デバイスでのアプリケーションの起動をコントロールするために Kaspersky Endpoint Security が使用するアプリケーションコントロールルールです。 アプリケーションコントロールの各モードに追加可能なルールは 5 個までです。
信頼するアップデーター	Windows	このチェックボックスをオンにすると、ルールに含まれるアプリケーションが信頼するアップデーターとみなされます。Kaspersky Endpoint Security は、これらのアプリケーションに対して、新しい実行ファイルの作成と実行を許可します。

システム変更監視

Windows、Linux 向け

このコンポーネントは、サーバー用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合に利用できます。このコンポーネントは、ワークステーション用の Windows で動作するコンピューターに Kaspersky Endpoint Security がインストールされている場合は利用できません。

システム変更監視コンポーネントは、コンピューターのセキュリティ侵害を示す可能性のあるオペレーティングシステムの変更を監視します。そのような変更を検知すると、Kaspersky Endpoint Security は対応するイベントを生成し、管理者に警告します。システム変更監視はリアルタイムモードで動作しますが、オンデマンドでシステム変更チェックを実行することもできます。

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。

`Linux` 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。

システム変更監視設定の設定

設定	OS	説明
リアルタイムシステム変更監視	`Windows`	リアルタイムモードで、システム変更監視は、コンポーネントの範囲（*監視範囲*）に含めたオブジェクトへの変更を追跡します。システム変更監視では、このようなオブジェクトへの不正アクセスをリアルタイムでブロックすることもできます。
システム変更検知時の処理	`Windows`	**ルールを適用**このモードで、システム変更監視は監視範囲内のファイルとレジストリキーに対する操作をブロックし、対応するイベントを生成します。 **ルールをテスト運用（通知）**このモードで、システム変更監視は監視範囲内のファイルとレジストリキーに対する操作を許可し、対応するイベントを生成します。
ファイルとレジストリを監視する	`Windows`	システム変更監視は、ファイル、フォルダー、レジストリへの変更を監視します。
デバイスを監視する	`Windows`	システム変更監視は、外部デバイスの接続と接続解除を監視します。
システム変更チェック	`Windows`	オンデマンドのシステム変更チェックは、手動で実行することも、スケジュールに従って実行することもできるタスクです。*システム変更チェック*タスクを実行するには、コンポーネントの範囲（*監視範囲*）を設定して、ベースラインを作成します。ベースラインとは、システム内のオブジェクトの記録された状態であり、現在の状態と比較する際に参照用に使用されます。
監視範囲	`Linux`	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**の監視範囲が表示されています。
除外リストの範囲	`Linux`	この表には、スキャンの除外範囲が表示されます。テーブル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。
マスクによる除外	`Linux`	名前マスクによってオブジェクトのスキャン除外範囲を設定できます。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。

信頼ゾーン

Windows、macOS 、Linux 向け

*信頼*ゾーンは Kaspersky Endpoint Security が有効なときに監視しないオブジェクトとアプリケーションのリストで、システム管理者が設定します。

管理者は処理されるオブジェクトとコンピューターにインストールされるアプリケーションの特徴を考慮しながら、信頼ゾーンを個別に定義します。Kaspersky Endpoint Security がアクセスをブロックする特定のオブジェクトやアプリケーションが無害であることが確実なときには、オブジェクトやアプリケーションを信頼ゾーンに含めなければならない場合があります。

Kaspersky Endpoint Security は、マスクを使用したファイル名またはフォルダー名の指定をサポートしています。マスクには次のワイルドカード文字を使用できます。

- 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

- 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

信頼ゾーンの設定

設定	OS	説明
Web アドレス	`Windows` `macOS` `Linux`	ウェブ脅威対策が信頼すると判断する Web アドレスのリスト。コンポーネントは、これらのアドレスからの送受信トラフィックについて、脅威をスキャンしません。信頼するアドレスのリストは、既知の Web サイトからのファイルのダウンロードが、ウェブ脅威対策によって妨げられる場合などに使用することができます。 信頼する URL のリストには、Web ページ / Web サイトのアドレスとアドレスマスクの両方を追加できます。
IP アドレス	`Windows` `Linux`	信頼するデバイスの IP アドレスのリスト。ネットワーク脅威対策コンポーネントは、これらのアドレスからのネットワーク動作をブロックしません。 `Windows` ポートおよびプロトコルを指定した IP アドレスを追加することができます。 `Linux` 除外リストに追加できるのは IP アドレスのみです。 また、除外リストに含まれる IP アドレスからのネットワーク攻撃に関する情報は、ログに記録されません。
ネットワークポート	`Windows` `macOS` `Linux`	ウェブコントロール、ファイル脅威対策、ウェブ脅威対策、メール脅威対策、脆弱性攻撃ブロック、およびふるまい検知コンポーネントがデータストリームを監視する既知および登録済みのポートのリスト。このトグルスイッチをオンにすると、ポートは信頼できるものと見なされ、ユーザーデバイス上のこれらのポートを通過するデータは監視されません。
信頼済み証明書	`Windows` `macOS` `Linux`	Kaspersky Endpoint Security が信頼すると判断するルート証明書のリスト。信頼するルート証明書のリストは、暗号化された接続をスキャンする時に使用されます。
信頼するコンピューター名または IP アドレス	`Windows`	ふるまい検知コンポーネントが信頼すると判断するホスト名と IP アドレスのリスト。Kaspersky Endpoint Security は、指定されたデバイスではウイルスやその他の脅威となるアプリケーションをスキャンしません。
ドメイン	`Windows` `Linux`	信頼するドメインのリストウェブ脅威対策、ウェブコントロール、および Cloud Discovery コンポーネント（Windows デバイスのみ）は、これらのドメインとの暗号化された接続を監視しません。 このリスト内のドメインへの接続は、SSL または TLS 経由でアクセスされ、かつ［SSL/TLS 接続をブロック］オプションが有効になっている場合、Windows デバイスからの接続がブロックされます

設定	OS	説明
信頼するマウントポイント	`Linux`	信頼するマウントポイントのリスト。これらは、ファイル脅威対策、アンチクリプター、アプリケーションコントロール、およびふるまい検知コンポーネントによるスキャンから除外されます。 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。
トラフィック読み取りの除外リスト	`Linux`	Kaspersky Endpoint Security がトラフィック読み取りから除外するネットワーク接続のリスト。トラフィック読み取りの除外リストは、ウェブ脅威対策、ネットワーク脅威対策、およびウェブコントロールコンポーネントに影響します。除外される接続は次のパラメータによって定義されます： • 通信方向（受信または送信）。 • リモートデバイスの IP アドレス。送受信トラフィックが読み取りから除外される IP アドレス（トラフィックの方向によって異なります）です。 • 宛先ポート。保護対象デバイス上のポート（受信トラフィック読み取りの除外の場合）またはリモートデバイス上のポート（送信トラフィック読み取りの除外の場合）です。 トラフィック読み取りの除外リストは TCP 接続にのみ適用され、ネットワークパケットルールには影響しません。
Wi-Fi ネットワーク	`macOS`	信頼する Wi-Fi ネットワークのリスト。次の設定を指定できます： • Wi-Fi ネットワーク名 • 暗号化種別 • 認証種別
アプリケーション	`Windows` `macOS` `Linux`	*信頼するアプリケーションのリスト*は、ファイルおよびネットワークの動作（悪意のある動作を含む）やシステムレジストリへのアクセスが Kaspersky Endpoint Security によって監視されないアプリケーションのリストです。既定では、Kaspersky Endpoint Security はすべてのアプリケーションプロセスによってオープン、実行、保存されるオブジェクトを監視し、すべてのアプリケーションとこのようなアプリケーションが生成するネットワークトラフィックの処理を管理します。アプリケーションが信頼するアプリケーションのリストに追加されると、Kaspersky Endpoint Security はアプリケーションのアクティビティの監視を停止します。
マルウェアスキャンの除外リスト	`Windows` `macOS` `Linux`	*信頼するオブジェクト*とは、Kaspersky Endpoint Security が特定のオブジェクトについてウイルスなどの脅威のスキャンを実行しないときに、オブジェクトが満たす必要のある一連の条件によって定義されます。スキャン除外により、侵入者がコンピューターやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションを使用できます。こうしたアプリケーションは必ずしも悪意のある目的を持っているわけではありませんが、ハッカーによって悪用される可能性があります。侵入者がコンピューターやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションに関する詳細情報は、カスペルスキー百科事典の Web サイト を参照してください。
デバイス	`Windows` `Linux`	「*信頼するデバイス*」は、信頼するデバイスの設定で指定されたユーザーが常にフルアクセスできるデバイスです。 信頼するデバイスで作業するには、個々のユーザー、ユーザーグループ、または組織内のすべてのユーザーにアクセス権を付与できます。

全般設定

検知の設定

Windows、macOS 、Linux 向け

このセクションでは、必要に応じて検出を設定する方法について説明します。脅威の検出と防止の有効性は、構成設定が正しいかどうかによって変わります。

設定	OS	説明
その他の種別のオブジェクトの検知	`Windows` `macOS` `Linux`	製品設定にかかわらず、Kaspersky Endpoint Security は常にウイルスやワーム、トロイの木馬や悪意のあるツールを検知してブロックします。これらのプログラムはコンピューターに重大な損害を与える可能性があります。 さらに、次の種類のオブジェクトの検知を有効にすることもできます。 • **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ソフトウェア**こうしたアプリケーションは必ずしも悪意のある目的を持っているわけではありませんが、ハッカーによって悪用される可能性があります。侵入者がコンピューターやユーザーデータに損害を与える目的で悪用する可能性がある正規のアプリケーションに関する詳細情報は、カスペルスキー百科事典の Web サイト を参照してください。 • `Windows` **アドウェア**：アドウェアは、他のプログラムのインターフェイスにバナー広告を表示して、検索クエリを広告 Web サイトにリダイレクトします。 • `Windows` **オートダイヤラー**：オートダイヤラーはモデムを使って密かに電話接続を確立することができます。これらのアプリケーションは、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ソフトウェアでもあります。 • `Windows` **パッカー**：ハッカーは、ウイルス対策ソフトによるマルウェアの検出を逃れるために、特殊なパッカーを使ってマルウェアを圧縮します。カスペルスキーは、ハッカーの間で最もよく使用されるパッカーを特定しました。
特別な駆除	`Windows`	通常、Kaspersky Endpoint Security は、コンピューターが感染する前に検知したマルウェアを終了します。特別な駆除は、すでに活動を開始したマルウェア (アクティブな感染) からコンピューターを保護し、データ損失や脅威の拡散のリスクを最小限に抑えます。 特別な駆除をオンにすると、Kaspersky Endpoint Security は悪意のある活動を検知するとポップアップ通知を表示します。この通知で、Kaspersky Endpoint Security は特別な駆除を実行するようユーザーに通知します。ユーザーがこの方法に同意すると、Kaspersky Endpoint Security はこれらの脅威を無効にして、コンピューターを再起動します。特別な駆除には大量のコンピューターリソースが必要になるため、他のアプリケーション処理速度が低下する可能性があります。 本製品がアクティブな感染の検知を処理している際、オペレーティングシステムの一部が利用できなくなることがあります。特別な駆除が完了し、コンピューターが再起動すると復元されます。 サーバー向けの Windows を実行しているコンピューターに Kaspersky Endpoint Security がインストールされている場合、Kaspersky Endpoint Security は通知を表示しません。そのため、アクティブな脅威を駆除する操作を選択することはできません。脅威を駆除するには、製品設定で特別な駆除を有効にして、マルウェアのスキャンタスクの設定ですぐに特別な駆除を実行するよう設定する必要があります。その後マルウェアのスキャンタスクを開始します。
スキャン中のファイルへのアクセスのブロック	`Linux`	このチェックボックスをオンにすると、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、実行防止処理、リムーバブルドライブスキャンタスクによるスキャンの実行中は、本製品がファイルへのアクセスをブロックします。 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。
オブジェクトの記録設定	`Linux`	**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。 **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をオンにすると、*ObjectNotProcessed* イベントをログに記録します。 **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をオンにすると、*PackedObjectDetected* イベントをログに記録します。

Kaspersky Security Network

Windows、macOS 、Linux 向け

コンピューターをより効果的に保護するために、Kaspersky Endpoint Security は世界中のユーザーから取得されたデータを使用します。Kaspersky Security Network は、こうしたデータの取得を目的に開発されたソリューションです。

KSN 機能は、米国領土内のアプリケーションでは利用できない場合があります。

*Kaspersky Security Network（KSN）*は、カスペルスキー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基盤であり、ファイル、Web リソース、ソフトウェアの評価に関する情報が含まれます。Kaspersky Security Network のデータを利用することで、Kaspersky Endpoint Security が新しい脅威により迅速に対応できるようになり、いくつか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くなります。Kaspersky Security Network に参加すると、KSN サービスから Kaspersky Endpoint Security に、スキャンした Web アドレスの評価に関する情報と、スキャンしたファイルのカテゴリと評価に関する情報が提供されます。KSN の設定について詳しくは、Kaspersky Security Center のヘルプを参照してください。

Kaspersky Security Network の使用は任意です。本製品の初期設定中に、KSN を使用するかどうか尋ねられます。ユーザーは KSN への参加をいつでも開始または終了することができます。

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 に関する声明のテキストが含まれたファイル ksn_<言語 ID>.txt は製品配信キットに含まれています。

カスペルスキーの評価データベースのインフラストラクチャ

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：

- ほとんどのカスペルスキー製品で使用されるのが *Kaspersky Security Network (KSN)* です。KSN の参加者は、カスペルスキーから情報を取得するとともに、ユーザーのコンピューター上で検知されたオブジェクトに関する情報をカスペルスキーに送信します。カスペルスキーに送信された情報は、分析担当者によって分析され、評価データベースと統計情報のデータベースに追加されます。

- *Kaspersky Private Security Network (KPSN)* は、Kaspersky Endpoint Security またはその他のカスペルスキー製品をインストールしているコンピューターのユーザーが、コンピューターからカスペルスキーにデータを送信せずにカスペルスキーの評価データベースや統計情報の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、次のいずれかの理由などにより Kaspersky Security Network に参加できない法人ユーザーの方を対象としています：

  - コンピューター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

Kaspersky Security Network の設定

設定	OS	説明
拡張 KSN モードを使用する	`Windows` `macOS` `Linux`	*拡張 KSN モード*では、本製品からカスペルスキーへ詳細データが送信されます。Kaspersky Endpoint Security は、オプションの設定にかかわらず KSN を使用して脅威を検知します。 `Linux` Linuxデバイスの場合、*Kaspersky Private Security Network (KPSN)* ソリューションを使用している際には表示されません。

設定	OS	説明
クラウドモードを使用	`Windows` `macOS` `Linux`	クラウドモードで動作している場合、Kaspersky Endpoint Security は軽量バージョンの定義データベースを使用します。軽量バージョンの定義データベースを使用しての本製品の動作は、Kaspersky Security Network を使用している場合にサポートされます。軽量バージョンの定義データベースを使用することで、通常バージョンの定義データベースを使用する場合に比べてコンピューターのメモリの使用量が約半分になります。Kaspersky Security Network に参加していないかクラウドモードが無効になっている場合、Kaspersky Endpoint Security は完全版の定義データベースをカスペルスキーのサーバーからダウンロードします。 このチェックボックスをオンにすると、Kaspersky Endpoint Security では軽量なバージョンの定義データベースを使用し、オペレーティングシステムのリソースの負荷を減少させます。 このチェックボックスをオンにした次のアップデートでは、Kaspersky Endpoint Security は軽量なバージョンの定義データベースをダウンロードします。 このチェックボックスをオフにすると、定義データベースの完全版を使用します。 このチェックボックスをオフにした次のアップデートでは、Kaspersky Endpoint Security は定義データベースの全体をダウンロードします。
KSN サーバーが使用できないときのコンピューターのステータス	`Windows`	このドロップダウンリストでは、KSN サーバーが使用できない場合に Kaspersky Security Center に表示するコンピューターのステータスを指定できます。
管理サーバーを KSN プロキシサーバーとして使用する	`Windows` `macOS` `Linux`	このチェックボックスをオンにすると、Kaspersky Endpoint Security は KSN プロキシサービスを使用します。KSN プロキシサービスの設定は管理サーバーのプロパティで編集できます。
KSN プロキシサーバーを使用できない場合は、Kaspersky Security Network サーバーを使用する	`Windows` `macOS` `Linux`	このチェックボックスをオンにすると、KSN Proxy サービスが使用できない場合は、KSN サーバーが使用されます。KSN サーバーは、カスペルスキー側に配置されている場合と、サードパーティ側に配置されている場合（Kaspersky Private Security Network を使用している時）があります。

ユーザー対話

Windows、macOS 、Linux 向け

このセクションでは、アプリケーションインターフェイスとユーザーの操作を設定する方法について説明します。

製品のインターフェイス設定

設定	OS	説明
コンピューターの開始時に Kaspersky Endpoint Security を開始する（推奨）	`Windows` `macOS`	この機能を有効にすると、オペレーティングシステムの読み込み後に Kaspersky Endpoint Security が起動し、セッション中にコンピューターを保護します。 この機能を無効にすると、オペレーティングシステムの読み込み後、ユーザーが手動で起動するまでは Kaspersky Endpoint Security が起動しません。コンピューター保護が無効になるため、ユーザーデータが脅威にさらされる可能性があります。
製品アイコンを表示する	`Windows` `macOS`	クライアントコンピューターの通知領域にアプリケーションアイコンが表示されます。アイコンのコンテキストメニューから Kaspersky Endpoint Security の操作を実行できます。製品アイコンの上の通知も表示されます。
ユーザーにアプリケーションインターフェイスを表示しない	`Windows` `macOS`	このチェックボックスをオンにすると、ユーザはリモートコンピュータからメインウインドウを開くことはできず、インターフェイスは表示されません。 このチェックボックスをオフにすると、ユーザはリモートコンピュータから Kaspersky Endpoint Security のメインウインドウを表示してインターフェイスを使用できます。
アプリケーション動作モニターセクションを非表示	`Windows`	このチェックボックスをオンにすると、クライアントコンピューターの Kaspersky Endpoint Security のメイン ウィンドウでは［**アプリケーション動作モニター**］ボタンを利用できません。*アプリケーション動作モニター*は、ユーザーのコンピューターのアプリケーションの動作に関する情報をリアルタイムで表示するように設計されたツールです。

設定	OS	説明
ローカルでのアップデート管理	macOS	このチェックボックスをオンにすると、ユーザーはリモートコンピューター上の Kaspersky Endpoint Security のアップデートをローカルで管理できます。 このチェックボックスをオフにすると、Kaspersky Security Center の Kaspersky Endpoint Security プラグインを使用した場合のみ、リモートコンピューター上の Kaspersky Endpoint Security のアップデートを管理できるようになります。
ローカルでのライセンス管理	macOS	このチェックボックスをオンにすると、ユーザーはリモートコンピューター上の Kaspersky Endpoint Security のライセンスをローカルで管理できます。 このチェックボックスをオフにすると、Kaspersky Security Center の Kaspersky Endpoint Security プラグインを使用した場合のみ、リモートコンピューター上の Kaspersky Endpoint Security のライセンスを管理できるようになります。
本製品の終了	macOS	このチェックボックスをオンにすると、［**終了**］の項目は製品アイコンのコンテキストメニューに表示されます。リモートコンピュータのユーザーは、使用しているコンピュータの Kaspersky Endpoint Security を終了できるようになります。 このチェックボックスをオフにすると、［**終了**］の項目は製品アイコンのコンテキストメニューに表示されなくなります。リモートコンピュータのユーザーは、使用しているコンピュータの Kaspersky Endpoint Security を終了できません。
ローカルタスクへのアクセス	Windows Linux	このチェックボックスをオンにすると、ローカルタスクが Kaspersky Endpoint Security ローカルインターフェイスに表示されます。その他のポリシー制限がない場合、ユーザーはタスクの設定と実行ができます。ただし、ユーザーはタスク実行スケジュールを設定することはできません。ユーザーはタスクを手動でのみ実行できます。 チェックボックスをオフにすると、ローカルタスクの使用を停止します。このモードでは、スケジュールにのっとったローカルタスクの実行は行われません。Kaspersky Endpoint Security のローカルインターフェイスでタスクの開始や設定ができなくなります。また、コマンドラインの使用時にもタスクの開始や設定ができなくなります。 ファイルまたはフォルダーのスキャンについては、スキャンするファイルまたはフォルダーのコンテキストメニューから［**スキャン**］を選択すれば開始できます。オブジェクトスキャンタスクの既定の設定値で、スキャンタスクが開始します。
グループタスクを表示する	Windows	このチェックボックスをオンにすると、グループタスクが Kaspersky Endpoint Security ローカルインターフェイスに表示されます。ユーザーは製品インターフェイスでタスクのリストを表示できます。 このチェックボックスをオフにすると、空白のタスクリストを表示します。
グループタスクを管理する	Windows Linux	このチェックボックスをオンにすると、Kaspersky コンソール内で指定されたグループタスクを開始および停止できます。ユーザーは製品インターフェイスまたは簡略化した製品インターフェイスでタスクを開始および停止できます。 このチェックボックスをオフにすると、Kaspersky Endpoint Security がスケジュールされたタスクを自動的に開始するか、管理者が Kaspersky Endpoint Security コンソールで手動でタスクを開始します。
コンピューターのステータス	Windows	Kaspersky Endpoint Security がインストールされたクライアントコンピューターについて、ポリシーの適用またはタスクの実行時にエラーが発生した場合に、Web コンソールで表示されるステータスの設定です。*OK*、*警告*および*緊急*のステータスが利用可能です。
アプリケーションのステータスの通知	Windows	システム トレイのアプリケーション イベント通知の設定です。通知領域に通知を表示するイベントカテゴリの横にあるチェックボックスをオンにします。 • **アクティブな脅威** • **コンピューターの再起動が必要** • **定義データベースの問題** • **保護レベルの問題** • **ライセンスの問題** • **適用可能なアップデート** 選択したカテゴリに属するイベントが発生すると、通知領域の製品アイコンが、警告の重要度に応じて または に変わります。
ローカル定義データベースのステータスに関する通知	Windows	製品で使用されている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の通知設定です。Kaspersky Endpoint Security がユーザーに「定義データベースがアップデートされていません」および「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」というメッセージを送信するまでの日数を指定できます。
アプリケーションの起動設定	Linux	製品の起動設定： • **アプリケーションの起動失敗の最大試行回数** • **アプリケーションの起動を待つ時間（分）**指定された待機期間が経過すると、kesl プロセスが再起動されます。

設定	OS	説明
再起動せずに製品アップデートをインストールする	`Windows`	再起動せずに本製品をアップデートすると、製品のバージョンがアップデートされた場合にもサーバーの動作を妨げることがありません。 再起動せずに本製品をアップデートする場合、次の制限事項があります： • バージョン 11.10.0 から、コンピューターを再起動せずにアプリケーションをアップグレードすることができるようになりました。これより前のバージョンのアプリケーションをアップグレードする場合は、コンピューターを再起動する必要があります。 • バージョン 11.11.0 から、コンピューターを再起動せずにパッチをインストールすることができるようになりました。本製品の以前のバージョンにパッチをインストールするには、コンピューターの再起動が必要になる場合があります。 • 本製品の再起動なしのアップデートは、データ暗号化（カスペルスキーの暗号化（FDE）、BitLocker、ファイルレベルの暗号化（FLE））が有効になっているコンピューターでは利用できません。データ暗号化が有効になっているコンピューターで本製品をアップグレードするには、コンピューターを再起動する必要があります。 • 再起動せずに仮想マシン上で本製品をアップグレードすることはできません。仮想マシン上で本製品をアップグレードするには、仮想マシンを再起動する必要があります。 Kaspersky Endpoint Security を 11.10.0 以降のバージョンに再起動せずにアップグレードした後、コンピューターには 2 つの Kaspersky Endpoint Security がインストールされることになります。古いバージョンの製品を手動で削除しないでください。コンピューターが再起動されると、古いバージョンの製品は自動的に削除されます。 パラメータの既定値は、オペレーティングシステムの種類によって異なります。本製品がワークステーションにインストールされている場合、再起動せずに本製品をアップグレードするオプションは無効になります。本製品がサーバーにインストールされている場合、再起動せずに本製品をアップグレードするオプションは有効になります。
リモート管理ソフトウェアとの互換性	`Windows`	Kaspersky Endpoint Security をリモート管理ツール（RAT）と一緒に使用すると問題が発生する場合は、互換性モードを有効にすることができます。この問題は、RAT と製品のセキュアデスクトップ（Secure Desktop）機能に互換性がないことに関連して生じる可能性があります。この機能の目的は、コンピューターのセキュリティレベルを低下させる可能性のある処理を確認することです。この機能により、アプリケーションで他のプロセスから分離された確認ダイアログを表示することができます。この機能では昇格した権限を使用してリクエストの安全を確保します。こうすることで、マルウェアではなくユーザーだけが処理を確認できるようになります。 RAT 互換性モードは、コンピューターのセキュリティレベルを低下させる可能性があります。Kaspersky Endpoint Security と RAT で問題が発生していない場合、互換性モードを有効にすることは推奨しません。この機能は既定で無効になっています。 例：ブラウザーを RemoteApp モードで使用している場合、信頼されていない証明書を使用する Web サイトにアクセスしたときに確認ウィンドウが表示されないことがあります。これは、RemoteApp が本製品のセキュアデスクトップ機能をサポートしていないためです。これにより、ブラウザーが応答しなくなることがあります。RemoteApp モードでブラウザーを正しく動作させるには、互換性モードを有効にする必要があります。他のサードパーティ製ソフトウェアを使用しているときにセキュアデスクトップ機能に問題が発生した場合にも、互換性モードを有効にしてみることができます。

パフォーマンス

Windows、macOS 、Linux 向け

Kaspersky Endpoint Security のパフォーマンスは、電力の消費量やコンピューターリソースの使用率に影響されます。

設定	OS	説明
他のアプリケーションにシステムリソースを優先的に割り当てる	`Windows`	Kaspersky Endpoint Security がコンピューターをスキャンする際にコンピューターのリソースを消費するため、CPU やハードディスクサブシステムの負荷が増加する可能性があります。これにより、他のアプリケーションの動作が遅くなることがあります。パフォーマンスを最適化するために、Kaspersky Endpoint Security には、*他のアプリケーションにリソースを振り分けるモード*が用意されています。このモードでは、CPU の負荷が高い場合に、オペレーティングシステムが Kaspersky Endpoint Security のスキャンタスクスレッドの優先度を下げることができます。これにより、オペレーティングシステムのリソースを他のアプリケーションに再分配することが可能になり、スキャンタスクの CPU 時間が減ります。その結果、Kaspersky Endpoint Security のスキャンに時間がかかるようになります。既定では、製品は他のアプリケーションにリソースを割り当てるように設定されています。
バッテリー使用中はスケジュールタスクを延期またはスキップする	`Windows` `macOS` `Linux`	この機能を有効にすると、Kaspersky Endpoint Security は省電力モードに切り替わります。 `Windows` Kaspersky Endpoint Security がスケジュールされているタスクを*延期します*。必要に応じて、スキャンタスクとアップデートタスクを手動で実行できます。 `macOS` `Linux` Kaspersky Endpoint Security はスケジュールされているタスクを*キャンセルします*。必要に応じて、スキャンタスクとアップデートタスクを手動で実行できます。 省エネモードが有効のときは、コンピューターがバッテリーの電力で動作している場合、以下のタスクがスケジュールされていても実行されません。 • *マルウェアのスキャン* • *定義データベースのアップデート* • *アプリケーション整合性チェック* • *IOC スキャン*
スキャンタスクの CPU 使用率を制限する	`Windows` `macOS` `Linux`	Kaspersky Endpoint Security のパフォーマンスを最適化するには、スキャンタスクによる CPU 使用率を制限できます。使用するオペレーティングシステムによって、CPU 使用率を制限できるタスクは異なる場合があります： • `Windows` `Linux` マルウェアのスキャン • `macOS` `Linux` Critical Areas Scan • `Linux` Inventory • `Linux` コンテナスキャン この機能を有効にすると、スキャンタスクによってすべての CPU コアにかかる平均負荷が、指定された値に近づきます。
スキャンのメモリ使用率を制限する（MB）	`Linux`	スキャンタスク（*マルウェアのスキャン*、*簡易スキャン*、*インベントリ*、*コンテナスキャン*）のメモリ使用量制限を設定できます。
プロセスメモリのスキャンからの除外を設定	`Linux`	プロセスメモリのスキャンの除外リストを設定できます。指定されたプロセスのメモリはスキャンされません。 本製品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を指定します。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。
アプリケーションのメモリ使用量を制限する	`Linux`	本製品の常駐メモリ使用量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。 **計算方法を制限する**： • **無制限**このオプションを選択すると、常駐メモリの使用量は制限されません。 • **正確な値を設定する（%）** • **正確な値を設定する（MB）** • **2 つの値のうち最も低いものを使用する（% または MB）** • **2 つの値のうち最も高いものを使用する（% または MB）** • **自動で制限（推奨）**このオプションを選択すると、常駐メモリの使用量が自動的に制限されます（規定値）。
アプリケーションの安定性監視を有効にする	`Linux`	Kaspersky Endpoint Security のアプリケーションの安定性監視を有効または無効にすることができます。この機能は、異常なアプリケーションの停止回数を追跡し、不安定なアプリケーションのパフォーマンスを管理者に通知します。 このチェックボックスをオンにすると、本製品は Kaspersky Endpoint Security の動作を監視します。 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。*

ネットワークの設定

Windows、macOS 、Linux 向け

インターネットへの接続に使用するプロキシサーバーを構成し、ネットワークポートの監視モードを選択し、暗号化された接続のスキャンを設定できます。

ネットワークの設定

設定	OS	説明
信頼するルート証明書	`Windows` `macOS` `Linux`	信頼するルート証明書のリストです。新しい認証局を導入する場合などに、Kaspersky Endpoint Security を使用してユーザーのコンピューターに信頼済みのルート証明書をインストールすることができます。本製品を使用して、Kaspersky Endpoint Security の証明書ストアに証明書を追加できます。この場合、証明書は Kaspersky Endpoint Security に対してのみ信頼済みと認識されます。言い換えると、ユーザーは新しい証明書を持つ Web サイトにブラウザーでアクセスできます。別のアプリケーションが Web サイトにアクセスしようとすると、証明書の問題により接続エラーが発生します。システムの証明書ストアに追加するには、Active Directory のグループポリシーを使用できます。
プロキシサーバー	`Windows` `macOS` `Linux`	クライアントコンピューターのユーザーによるインターネット接続で使用されるプロキシサーバーの設定です。Kaspersky Endpoint Security では、定義データベースや製品機能のアップデートに使用するものを含む、特定の保護機能にこの設定が使用されます。
プロキシサーバー認証を使用する	`Windows` `macOS` `Linux`	このチェックボックスをオンにすると、アプリケーションはプロキシサーバーに接続するときにユーザー名とパスワードによる認証を使用します。 `Windows` Windows デバイスの場合は、認証種別プを選択する必要があります。 • **NTLM 認証**現在のユーザーアカウントによる NTLM 認証（既定）。 • **ユーザー名とパスワードを指定して NTLM 認証を使用する**手動で指定された資格情報による NTLM 認証。 • **ユーザー名とパスワード**手動で指定された資格情報による認証。 • **自動認証** • **Kerberos 認証**現在のユーザーアカウントによる Kerberos 認証。 • **ユーザー名とパスワードを指定して Kerberos 認証を使用する**手動で指定された資格情報による Kerberos 認証。
ローカルアドレスにはプロキシサーバーを使用しない	`Windows` `macOS`	このチェックボックスをオンにすると、共有フォルダーからアップデートを行う際に、プロキシサーバーは使用されません。
コンポーネントにプロキシサーバーを使用しない	`Linux`	プロキシサーバーを使用しない製品コンポーネントの横にあるチェックボックスをオンにします。 • **Endpoint Detection and Response Expert（オンプレミス）**：KATA サーバーに接続する時は、プロキシサーバを使用しません。 • **KATA Sandbox**：KATA Sandboxとの対話を行うセントラルノードサーバーに接続するときにプロキシサーバーを使用しません。 • **Network Detection and Response (KATA)**：Network Detection and Response サーバーに接続する時は、プロキシサーバを使用しません。
指定した IP アドレスまたは DNS 名にはプロキシを使用しません	`Linux`	この表には、プロキシサーバーを使用してはならない IP アドレスと DNS 名のリストが含まれています。アドレスの指定にマスク（`*` と `?`）が使用できます。 表内のアドレスは、追加、編集、削除できます。
暗号化された接続のスキャン	`Windows` `macOS` `Linux`	この機能により、ウェブ脅威対策、メール脅威対策、ウェブコントロールおよび Cloud Discovery コンポーネントは、暗号化された接続（HTTPS）を監視および処理できるようになります。 `Linux` Linuxデバイスの場合、本製品が証明書を検証する方法を判断する［**証明書検証ポリシー**］を使用できます。 • **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）：インターネットを使用して、証明書の検証に必要な不足しているチェーンを検証およびダウンロードします。
信頼するドメイン	`Windows` `Linux`	Kaspersky Endpoint Security でネットワーク接続をスキャンしない Web アドレスのリストを使用します。この場合 Kaspersky Endpoint Security は、ウェブ脅威対策、メール脅威対策、ウェブコントロールが動作している間は信頼する URL の HTTPS トラフィックはスキャンしません。 ドメイン名または IP アドレスを入力できます。Kaspersky Endpoint Security はドメイン名マスクの入力時に文字「`*`」をサポートします。
従量制接続時に本製品によるデータ通信量を抑制する	`Windows`	このチェックボックスをオンにすると、インターネット接続が制限されているときに本製品のネットワークトラフィックを制限します。高速モバイルインターネット接続は制限するネットワークとして、Wi-Fi 接続は無制限のネットワークとして判断されます。 ネットワークにかかる費用の対策は、Windows 8 以降を実行中のコンピューターで動作します。

設定	OS	説明
Web ページと連携するため Web トラフィック内にスクリプトを埋め込む	Windows	このチェックボックスをオンにすると、Kaspersky Endpoint Security は Web ページと連携するためのスクリプトを Web トラフィック内に埋め込みます。このスクリプトはウェブコントロール機能が正常に動作するために必要です。スクリプトはウェブントロールのイベントの登録を有効にします。 Web ページと連携するスクリプトのトラフィックへの埋め込みは、ウェブコントロールの正常な動作のためカスペルスキーにより推奨されています。
EV 証明書を使用した Web サイトへの暗号化接続を確認する	Windows	EV 証明書（Extended Validation Certificate）は、Web サイトの信頼性を示すためのもので、接続のセキュリティを向上させます。Web サイトで EV 証明書が使用されている場合、ブラウザーのアドレスバーの鍵アイコンでそのことが示されます。また、アドレスバーの全体や一部の色が緑色に変わるブラウザーもあります。 このトグルスイッチをオンにすると、EV 証明書を使用している Web サイトの暗号化された接続を復号化して監視します。 このトグルスイッチをオフにすると、本製品は HTTPS トラフィックの通信内容にアクセスできません。そのため、HTTPS トラフィックは「`https://bing.com`」などの URL のみに基づいて監視されます。 EV 証明書を使用している Web サイトに最初にアクセスするときには、チェックボックスがオンかオフかにかかわらず、接続が復号されます。
SSL 2.0 接続をブロック	Windows	このチェックボックスをオンにすると、SSL 2.0 プロトコルで確立されたネットワーク接続が監視されてブロックされます。 このチェックボックスをオフにすると、SSL 2.0 プロトコルで確立されたネットワーク接続はブロックされません。ただし、このプロトコル経由のネットワークトラフィックが監視されなくなります。
TLS 1.0 接続をブロック	Windows	このチェックボックスをオンにすると、TLS 1.0 プロトコルで確立されたネットワーク接続がブロックされます。 このチェックボックスをオフにすると、TLS 1.0 プロトコルで確立されたネットワーク接続はブロックされません。このプロトコル経由のネットワークトラフィックを監視します。本製品のすべてのコンポーネントは制限されることなく動作します。
SSL 3.0 接続をブロック	Windows	このチェックボックスをオンにすると、SSL 3.0 プロトコルで確立されたネットワーク接続がブロックされます。 このチェックボックスをオフにすると、SSL 3.0 プロトコルで確立されたネットワーク接続はブロックされません。このプロトコル経由のネットワークトラフィックを監視します。本製品のすべてのコンポーネントは制限されることなく動作します。
監視対象ポート	Windows macOS Linux	**すべてのネットワークポートを監視する**このネットワークポート監視モードでは、保護機能（ファイル脅威対策、ウェブ脅威対策、メール脅威対策）はコンピューターで開いているすべてのネットワークポート経由で送信されるデータストリームを監視します。 **選択されたネットワークポートのみを監視する**このネットワークポートの監視モードでは、コンピューターの選択したポートおよび選択したアプリケーションのネットワークの動作を監視します。メールの送信とネットワークトラフィックで通常使用されるネットワークポートのリストは、カスペルスキーの専門家の推奨に従って構成されます。 Mac デバイスでは、選択したポートのみを監視できます。
監視対象アプリケーション	Windows	ポートスキャン設定に関係なく、すべてのポートのすべてのトラフィックが監視されるアプリケーションのリスト。
Firefox が使用する証明書ストアを選択	macOS	**システムルートキーチェーン（推奨）**このオプションをオンにすると、Kaspersky Endpoint Security はシステムルートキーチェーンのルート証明書を使用して、Mozilla Firefox ブラウザで暗号化された HTTPS トラフィックをチェックします。 既定ではこのオプションが選択されます。 **Mozilla Firefox のブラウザー設定の証明書ストア**このオプションをオンにすると、Kaspersky Endpoint Security はブラウザの証明書ストアからの証明書を使用します。 この場合、Kaspersky Endpoint Security 証明書を Mozilla Firefox の証明書ストアに手動で追加する必要があります。詳細は、「カスペルスキー証明書を Mozilla Firefox 証明書ストアに追加する方法」の記事を参照してください。
トラフィック読み取りモード	Linux	**iptables**Kaspersky Endpoint Security は、トラフィックのインターセプトに iptables ユーティリティを使用します。 **eBPF**本製品は、eBPF テクノロジーを使用してトラフィックを傍受します。

コンテナスキャン

Linux 向け

本製品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。本製品は、Docker コンテナ管理システム、CRI-O 環境、Podman および runc ユーティリティとの連携をサポートしています。

コンテナスキャンにはファイル脅威対策コンポーネントを有効にする必要があります。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適用されます。

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。

コンテナスキャン設定

設定	OS	説明
脅威の検知時の処理	Linux	**コンテナをスキップ**感染したオブジェクトを検知した場合、アプリケーションはコンテナに対して操作を実行しません。 **コンテナを停止**感染したオブジェクトを検知した場合、アプリケーションは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**感染したオブジェクトを駆除できなかった場合、アプリケーションはコンテナを停止します。
Docker を使用	Linux	Docker 環境を使用します。環境を使用するには、Docker ソケットのパスまたは URI（ユニバーサルリソース ID）を入力します。
CRI-O を使用	Linux	CRI-O 環境の使用。この環境を使用するには、CRI-O 設定情報ファイルのパスを入力してください。
Podman を使用	Linux	Podman ユーティリティの使用。このユーティリティを使用するには、ユーティリティの実行ファイルへのパスと、コンテナ保管領域のルートディレクトリへのパスを入力します。
runc を使用	Linux	runc ユーティリティの使用。このユーティリティを使用するには、ユーティリティの実行ファイルへのパスと、コンテナ状態保管領域のルートディレクトリへのパスを入力します。

テクニカルサポート

Windows、Linux 向け

コンピューターで発生した Kaspersky Endpoint Security の不具合を解決するため、テクニカルサポートの担当者が、システムに関する情報や、アプリケーションの動作中に発生したイベントに関する情報を必要とする場合があります。この情報はダンプファイルとトレースファイルに保存されています。

*ダンプファイル*には、ダンプファイルの作成時点で Kaspersky Endpoint Security のプロセスが作業していたメモリについてのすべての情報が含まれます。

この*トレースファイル*を使用して、アプリケーションコマンドの実行プロセスを段階的に追跡し、エラーが発生した製品動作の段階を特定することができます。

ダンプファイルとトレースファイルには機密データが含まれている場合があります。データへのアクセスを制御するには、このファイルのセキュリティを個別に確保する必要があります。

ダンプファイルとトレースファイルは、本製品の使用中にコンピューターに保存されます。本製品が削除されると、これらのファイルは完全に削除されます。

コンピューターにセキュリティプロファイルを適用すると、アプリケーションはダンプファイルの書き込みを開始します。不具合が発生した場合、次回アプリケーションを起動すると、テクニカルサポートの情報を読み込むウィンドウが開きます。このウィンドウでは、作成されたダンプファイルに関する情報を確認し、カスペルスキーへの送信を承認できます。

テクニカルサポートの設定

設定	OS	説明
ダンプへの書き込みは有効です	`Windows` `Linux`	ダンプへの書き込みが有効になっている場合、本製品がクラッシュすると、Kaspersky Endpoint Security はダンプファイルを作成します。 `Linux` のダンプファイルは、大量のディスク空き容量を使用します。ハードディスクの空き容量が 4 GB 未満の場合、ダンプを有効にすると、ディスク容量不足につながる可能性があります。
ダンプおよびトレースファイルの保護は有効です	`Windows`	ダンプファイルとトレースファイルの保護が有効な場合、これらのファイルには次のユーザーがアクセスできます： • ダンプファイルには、システム管理者と LAN 管理者、およびダンプファイルとトレースファイルの書き出しを有効にしたユーザーがアクセスできます。 • トレースファイルには、システム管理者と LAN 管理者がアクセスできます。
コードダンプのパス	`Windows` `Linux`	ダンプファイルは、次のフォルダーに保存されています。 • `Windows`：`%ProgramData%\Kaspersky Lab\KES.[AppVersion]\Traces` ダンプファイルに別のフォルダーを設定することはできません。 • `Linux`：`var/opt/kaspersky/kesl/common/dumps` および `var/opt/kaspersky/kesl/common/dumps-user` 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および書き込み権限を持っていることを確認してください。ダンプ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。
トレースフォルダーのパス	`Windows` `Linux`	トレースファイルは、次のフォルダーに保存されています。 • `Windows`：`%ProgramData%\Kaspersky Lab\KES.[AppVersion]\Traces` トレースファイルに別のフォルダーを設定することはできません。 • `Linux`：`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および書き込み権限を持っていることを確認してください。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）	`Linux`	このフィールドでは、アプリケーションのトレース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。
トレースファイルの最大数	`Linux`	このフィールドでは、アプリケーションのトレースファイルの最大数を入力できます。
テクニカルサポートの Web リソースのカスタマイズ	`Windows`	Kaspersky Endpoint Security に不具合が発生した場合に、ユーザーがテクニカルサポートに連絡するために使用できる連絡先情報の表です。サポートの受け方を説明するメッセージテンプレートをユーザー向けに設定することもできます。 既定では、アプリケーションはカスペルスキーの Web サイトへのリンクを表示します。

レポートおよびストレージ

Windows、macOS 、Linux 向け

このセクションでは、Kaspersky Endpoint Security が検出したイベントに関するレポートの作成と保存に関する設定を管理し、バックアップと隔離のオブジェクトの保管領域を設定できます。

レポート

*レポート*には、Kaspersky Endpoint Security の各コンポーネントの動作、データ暗号化イベント、各スキャンタスク、アップデートタスクおよび変更チェックタスクの実行、ならびに製品全体の操作に関する情報が記録されます。

Windows レポートは、フォルダー「C:\ProgramData\Kaspersky Lab\KES.12.4.0\Report」に保存されます。

バックアップ

*バックアップ保管領域*には、脅威の駆除で削除または修正されたファイルのバックアップコピーが保存されています。*バックアップコピー*は、ファイルが駆除または削除される前に作成されるファイルのコピーです。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。

ファイルのバックアップコピーは、次のフォルダーに保存されます。

- Windows：C:\ProgramData\Kaspersky Lab\KES.12.4.0\QB
- Linux：/var/opt/kaspersky/kesl/common/objects-backup/

管理者グループに属するユーザーには、このフォルダーへの完全なアクセス権が付与されます。Kaspersky Endpoint Security のインストールに使用されたユーザーアカウントには、このフォルダーへの限定的なアクセス権が付与されます。

隔離

*隔離*はコンピューター上にある特別なローカル保管領域です。ユーザーがコンピューターに対して危険だと判断したファイルを隔離することができます。隔離されたファイルは暗号化された形式で保存され、デバイスのセキュリティを脅かすことはありません。

レポートと保管領域の設定

設定	OS	説明
レポートを削除するまでの期間（日）	Windows macOS	このチェックボックスをオンにすると、レポートの最長保管期間は指定した期間に制限されます。この期間を経過すると、Kaspersky Endpoint Security は最も古いデータをレポートファイルから自動的に削除します。
レポートファイルのサイズを制限する（MB）	Windows	このチェックボックスをオンにすると、最大レポートファイルサイズは指定した値に制限されます。最大レポートファイルサイズを超過しないように、最大レポートファイルサイズに到達すると、Kaspersky Endpoint Security は最も古いデータをレポートファイルから自動的に削除します。
最近のイベントのみを保存する	macOS	このチェックボックスをオンにすると、Kaspersky Endpoint Security は、タスクが開始されるたびに前回のタスク開始以降に発生した重大でないイベントに関する情報を削除しますが、レポート内の重要なメモ（検知した悪意のあるオブジェクトに関する情報など）は保持されます。
緊急イベント以外も記録する	macOS	このチェックボックスをオンにすると、レポートに情報イベントなど、重要でないイベントを記録します。緊急イベント以外は、保護に影響を与えません。
オブジェクトを削除するまでの期間（日）	Windows macOS Linux	このチェックボックスをオンにすると、ファイルの最長保管期間は指定した期間に制限されます。最大保管期間を経過すると、最も古いファイルがバックアップから削除されます。
バックアップのサイズを制限する（MB）	Windows Linux	このチェックボックスをオンにすると、保管領域の最大サイズは指定した値に制限されます。保管領域の最大サイズを超過しないように、保管領域の最大サイズに到達すると、Kaspersky Endpoint Security は最も古いファイルを保管領域から自動的に削除します。
隔離のサイズを制限する	Windows Linux	**隔離の最大サイズ（MB）** このチェックボックスをオンにすると、隔離の最大サイズは指定した値に制限されます。隔離のサイズの最大値に到達すると、Kaspersky Endpoint Security はイベント［*隔離の保管領域に十分な空き容量がありません*］を Kaspersky Security Center に送信し、イベントをオペレーティングシステムのイベントログに作成します。その間本製品は新しいオブジェクトの隔離を停止します。隔離の中身を手動で空にしてください。 **隔離の容量が次の割合に到達した際に通知する（%）** 隔離のしきい値です。たとえば、「50%」のように隔離のしきい値を設定できます。隔離のサイズがしきい値に到達すると、製品は対応するイベントを Kaspersky Security Center に送信し、イベントをログに記録します。その間本製品は新しいオブジェクトの隔離を継続します。

KSC との連携

このセクションでは、Kaspersky Endpoint Security と Kaspersky Security Center の連携を設定する方法について説明します。

Kaspersky Security Center との連携設定

設定	OS	説明
アクティベーションのプロキシサーバーとして Kaspersky Security Center を使用する	`Windows` `macOS` `Linux`	このチェックボックスをオンにすると、本製品は Kaspersky Security Center 管理サーバーをアクティベーションサーバーへの接続用のプロキシサーバーとして使用します。これは、アクティベーションコードを使用して、インターネットにアクセスできない分離されたネットワークセグメントでアプリケーションをアクティベートする場合に必要です。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場合、インターネット接続は必要ありません。 アプリケーションが Light Agent モードで使用されている場合は適用できません。
管理サーバーへのデータ転送	`Windows` `macOS` `Linux`	管理サーバーへ情報を転送する必要のあるイベントのカテゴリです。管理サーバーのディスク領域を最適化するために、一部のデータの転送を無効にすることができます。 本製品は次のカテゴリのイベントを送信します： • `Windows` **脅威の活動連鎖の情報** • `Windows` `macOS` `Linux` **隔離ファイルの情報**。 • `Windows` `Linux` **バックアップ内のファイルの情報** • `Windows` `Linux` **未処理のファイルの情報** • `Windows` `macOS` `Linux` **インストールされたデバイスの情報**。 • `Windows` `Linux` **起動されたアプリケーションの情報** • `Windows` **ファイル暗号化エラーの情報** • `Windows` **アダプティブアノマリーコントロールルールのステータスに関するレポート** • `Windows` **アダプティブアノマリーコントロールルールの適用に関するレポート**

OS 連携設定

Linux 向け

本製品が適切に機能するには、システムイベント、つまりファイル操作とプロセスの開始を読み取る必要があります。本製品がシステムイベントインターセプターを使用しない場合、リアルタイムスキャンは実行されず、デバイスの保護レベルが低下します。

OS 連携設定

設定	OS	説明
インターセプターメカニズム	`Linux`	本製品で使用されるシステムイベントインターセプターメカニズム： • **fanotify テクノロジー**このオプションを選択すると、本製品はシステムイベントインターセプターのために fanotify テクノロジーを使用します。 • **アップデート可能なカーネルモジュール**このオプションを選択すると、本製品はシステムイベントインターセプターのためにアップデート可能なカーネルモジュールを使用します。
アップデート可能なカーネルモジュールが開始できなかった場合	`Linux`	アップデート可能なカーネルモジュールの起動に失敗した場合のアプリケーションの処理： • **fanotify を使用する**このオプションを選択すると、本製品はシステムイベントインターセプターのために fanotify テクノロジーに切り替わります。 • **システムイベントインターセプターを無効にする（保護レベルが低下します）**本製品がシステムイベントインターセプターを使用しない場合、リアルタイムスキャンは実行されず、デバイスの保護レベルが低下します。 この設定は、［**アップデート可能なカーネルモジュール**］をオンにした場合に使用できます。

設定	OS	説明
テレメトリの送信元	`Linux`	Kaspersky Endpoint Security がテレメトリ収集に使用するソース： • **eBPF のみを使用**eBPF のみが使用されます。 • **既定**eBPF と auditd サービスの両方が使用されます。
auditd の操作モード	`Linux`	このモードでは、auditd サービスは監査イベントを記録し、その後 Detection and Response ソリューションに送信します。 • **排他的**このオプションをオンにすると、auditd サービスを排他的に使用します。サードパーティ製品は監査ストリームに接続できません。 • **非排他的**このオプションをオンにすると、 auditd サービスはシステム監査を使用する別のプロセスからの複数の接続を受け入れることができます。

イベントの設定

Windows、macOS 、Linux 向け

このセクションでは、管理対象デバイスのイベントと一般的なイベントに関する通知を設定できます。通知は、このワークスペース内のユーザーのメールアドレスに送信できます。

製品の実行中は、様々なイベントが発生します。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、本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、修正が必要なコンポーネントのエラーを指摘したりします。

Kaspersky Endpoint Security のイベントは、次の重大度クラスに分類されます。

- *緊急イベント*：コンピューターのセキュリティに重大な脅威をもたらすイベントです（悪意のあるオブジェクトの検出、脆弱性、Kaspersky Endpoint Security の問題）。緊急イベントにはすぐに対応する必要があります。緊急イベントの通知は、無効にしないことを推奨します。

- *機能エラー*：Kaspersky Endpoint Security に不具合が発生した場合（処理エラー、タスク設定エラー）に発生するイベントです。このようなイベントはコンピューターのセキュリティを直接脅かすものではありませんが、Kaspersky Endpoint Security が正しく動作し、デバイスを保護していることを確認するためにユーザーの介入が必要です。

- *警告*：すぐに対処する必要はありませんが、将来的にコンピューターのセキュリティが脅かされる可能性があることを示している可能性があるイベントです。

- *情報イベント*

通知が有効か無効かに関係なく、Kaspersky Endpoint Security はすべてのアプリケーションイベントに関する情報をアプリケーションレポートに記録します。

Kaspersky Endpoint Security のイベントごとに、通知の受信方法を設定できます。

- `Windows` **メールで通知**

- `Windows` **ローカルレポートに保存**

- `Windows` `macOS` **画面で通知**

- `Windows` `Linux` **システムイベントログに保存**

テレメトリの設定

Windows、macOS 、Linux 向け
このセクションでは、管理対象デバイスからテレメトリ収集サーバーへのテレメトリ送信設定を行います。テレメトリとは、保護対象コンピューター上で発生したイベントのリストです。Kaspersky Endpoint Security はテレメトリデータを分析し、同期中に Kaspersky Anti Targeted Attack Platform またはテレメトリ収集サーバーへ送信します。テレメトリイベントはほぼ継続的にサーバーに届きます。次の条件のいずれかが満たされると、Kaspersky Endpoint Security はサーバーとの同期を開始します。

- 同期間隔が経過した。
- バッファ内のイベント数が上限を超えた。

Kaspersky Endpoint Security とサーバー間に接続がない場合は、本製品は新しいイベントをキューに入れます。接続が復元されると、Kaspersky Endpoint Security はキューのイベントを順にサーバーに送信します。サーバーの過負荷を避けるため、イベントの一部がスキップされることがあります。

［組み込みエージェント］セクションで各組み込みエージェントの同期設定を管理し、ネットワーク負荷に応じて最適な値を選択できます。

このセクションでは、次の設定ができます：

- テレメトリの包含および除外ルール。
- KATA サーバー、テレメトリ収集サーバー、または応答サーバーに送信されるテレメトリの収集。

EDR Expert（オンプレミス）のテレメトリ

Windows、macOS 、Linux 向け
EDR Expert（オンプレミス）のテレメトリ設定

設定	OS	説明
EDR Expert（オンプレミス）のテレメトリ	`Windows` `macOS` `Linux`	**インポート**および**エクスポート**EDR Expert (オンプレミス) テレメトリ設定を JSON ファイルにエクスポートできます。これにより、たとえば多数のイベント ID をファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、信頼する URL のリストをバックアップしたり、別のサーバーにリストを移行することができます。
全般的な除外	`Windows` `macOS` `Linux`	送信されるデータを最適化するため、特定のイベント種別に対して除外ルールを設定できます。Kaspersky Endpoint Security は、このルールに該当するテレメトリを収集しません。これによりトラフィックを削減し、信頼するオブジェクトやプロセスからのイベントの処理を回避できます。 **ルール名** **処理**： • **収集しない**このオプションをオンにすると、Kaspersky Endpoint Security はルールの条件を満たすテレメトリを収集しません。 • **IOA を除外**このオプションをオンにすると、Kaspersky Endpoint Security は IOA ルールの適用に基づくテレメトリを収集しません。 *攻撃の痕跡（IOA）*は、標的型攻撃を示す可能性のあるシステム内の疑わしい動作の説明を含むルールです。 **条件**ルールを適用する条件。テレメトリのパラメータ、条件演算子、およびパラメータの値を指定します。既定では、Kaspersky Endpoint Security はルールトリガー条件を論理 AND と組み合わせます。AND および OR 論理演算子を使用して、複数の条件または条件グループを追加できます。
すべてのイベント種別	`Windows` `macOS` `Linux`	カスペルスキーによって既定でテレメトリの収集が定義されているイベント タイプのリスト。 各イベント種別に対してテレメトリを手動で有効または無効にしたり、テレメトリの除外ルールと包含ルールを構成したりできます。

EDR (KATA) / NDR (KATA) テレメトリ

Windows、Linux 向け

パフォーマンスを向上させ、テレメト収集リサーバーへのデータ送信を最適化するために、テレメトリの除外リストを設定できます。たとえば、個々のアプリケーションのネットワーク通信データを送信しないように選択できます。

EDR (KATA) / NDR (KATA) テレメトリ除外設定

設定	OS	説明
除外されるプロセス	`Windows` `Linux`	Kaspersky Endpoint Security は、リストのプロセスに関連するデータを処理しません。 **送信するテレメトリのサイズを最適化**Kaspersky Endpoint Security では、Microsoft SMB プロトコル、WinRM サービス、およびネットワークエージェントの klnagent.exe プロセスについて、データの送信量を最適化したり、コードが 102（基本的な通信）および 8（プロセスのネットワークアクティビティ）のイベントをテレメトリから除外できます。また、すべての種類のネットワークプロトコルについて、ネットワークパケットの種類に関する拡張情報を最適化できます。 Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**および**親プロセス**： • **完全パス**名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。 • **コマンドラインテキスト**ファイルを実行するために使用されるコマンド。 • **説明**RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。 **次のイベント種別に使用する**： • **ファイルの変更** • **ネットワークイベント** • **プロセス：コンソールでの対話的入力** • **モジュールの読み込み** • **レジストリの変更** • **DNS ログ** • **プロセスへのアクセス** • **コード埋め込み** • `Windows` **WMI クエリ** • **パイプ** • LDAP • `Windows` **AMSI**

設定	OS	説明
除外されるネットワークコミュニケーション	`Windows` `Linux`	Kaspersky Endpoint Security は、リストのネットワークコミュニケーションに関連するデータを処理しません。除外ルールでは以下を指定できます。 **ルール名** **通信方向** **プロトコル** **生ソケット** **プロトコル番号** **ローカルアドレス**Kaspersky Endpoint Security がネットワークトラフィックからテレメトリを除外するコンピューターのネットワークアドレス。 **ローカルポートまたは範囲** **リモートアドレス**Kaspersky Endpoint Security がネットワークトラフィックからテレメトリを除外するコンピューターのネットワークアドレス。 **リモートポートまたは範囲** IP アドレスでは IPv4 形式のみがサポートされます。 **選択したアプリケーションにルールを適用**このチェックボックスをオンにすると、Kaspersky Endpoint Security は、リストのアプリケーションの実行ファイルのネットワークトラフィックから EDR テレメトリを除外します。
除外されるファイル操作	`Windows` `Linux`	Kaspersky Endpoint Security は、リストのファイル操作を処理しません。除外ルールでは以下を指定できます。 **ルール名** **ファイル名またはマスク**ファイルにアクセスしたときに Kaspersky Endpoint Security が除外ルールを適用するファイル名またはマスク。Kaspersky Endpoint Security はマスクの入力時の文字「`*`」および「`?`」をサポートします。 **ファイル操作を選択**ルールが適用されるファイル操作の種別。 **以前のパス** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**および**親プロセス**： • **完全パス**名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**ファイルを実行するために使用されるコマンド。 • **説明**RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。

設定	OS	説明
除外される DNS 操作	`Windows` `Linux`	Kaspersky Endpoint Security は、リストの DNS 操作を処理しません。除外ルールでは以下を指定できます。 **ルール名** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**および**親プロセス**： • **完全パス**名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。 • **コマンドラインテキスト**ファイルを実行するために使用されるコマンド。 • **説明**RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。 **DNS 操作**： • **DNS サーバー IP アドレス** • **クエリオプション** • **ステータス** • **ドメイン名** • **設定種別 ID** • **応答データ**クエリに対する DNS 応答の内容。
除外される LDAP 操作	`Windows`	Kaspersky Endpoint Security は、リストの LDAP 操作を処理しません。除外ルールでは以下を指定できます。 **ルール名** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**および**親プロセス**： • **完全パス**名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。 • **コマンドラインテキスト**ファイルを実行するために使用されるコマンド。 • **説明**RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。 **LDAP 操作**： • **LDAP 検索範囲**LDAP検索範囲。次のいずれかの値を取ることができます：ADS_SCOPE_BASE、ADS_SCOPE_ONELEVEL、ADS_SCOPE_SUBTREE。 • **フィルター** • **LDAP オブジェクト検索用の識別名**LDAP ディレクトリ内のレコードの名前。 • **LDAP 操作検索で使用されるオブジェクト属性**クエリ内で戻り値として設定される属性。

設定	OS	説明
除外されるプロセスのアクセスクエリ	`Windows`	Kaspersky Endpoint Security は、リストのプロセスへのアクセス要求を処理しません。除外ルールでは以下を指定できます。 **ルール名** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**、**親プロセス**、**ターゲットプロセスのファイル**、**ソースプロセスのハンドル**および**ターゲットプロセスのハンドル**。 • **完全パス**名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。 • **コマンドラインテキスト**ファイルを実行するために使用されるコマンド。 • **元のファイル名**RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。 **プロセスのアクセスクエリ**： • **操作種別** • **要求されたプロセスへのアクセス** • **コールスタックトレース**

設定	OS	説明
除外されるコード埋め込み	`Windows`	Kaspersky Endpoint Security は、リストのコード埋め込みを処理しません。除外ルールでは以下を指定できます。 **ルール名** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**および**親プロセス**： • **完全パス**名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**ファイルを実行するために使用されるコマンド。 • **説明**RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。 **コード埋め込み**： • **アクセス方法** • **コールスタック**コードの埋め込みに関連する関数の読み取りの時点での API 呼び出しスタック • **変更されたコマンドライン** • **埋め込みアドレス**リモートで実行されたコードが配置されたターゲットプロセスのアドレス空間内のアドレス。 コードの埋め込みが SET_WINDOWS_HOOK および ARG_SPOOFING メソッドを使用して実行された場合、このフィールドは空のままになります。 • **変更されたコマンドライン** • **挿入された DLL 名**インターセプタールーチンを含む DLL の名前と、埋め込み後にコントロールが渡される関数の名前。 SET_WINDOWS_HOOK メソッドを使用してコードの埋め込みが成功した場合、このフィールドが入力されます。 • **挿入された DLL のパス**インターセプタールーチンを含む DLL へのパス。 SET_WINDOWS_HOOK メソッドを使用してコードの埋め込みが成功した場合、このフィールドが入力されます。

設定	OS	説明
除外される WMI クエリ	`Windows`	Kaspersky Endpoint Security は、リストの WMI 要求を処理しません。除外ルールでは以下を指定できます。 **ルール名** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**および**親プロセス**： • **完全パス**名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**ファイルを実行するために使用されるコマンド。 • **説明**RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。 **WMI クエリ**： • **WMI 操作種別** • **リモートクエリ** • **WMI コマンドを実行したコンピューターの名前** • **WMI ユーザーアカウント** • **実行された WMI コマンド** • **WMI 名前空間** • **WMI イベントコンシューマーフィルター** • **作成した WMI イベントコンシューマーの名前** • **WMI イベントコンシューマーのソースコード**
除外されるパイプ操作	`Windows`	Kaspersky Endpoint Security は、リストのパイプ操作を処理しません。除外ルールでは以下を指定できます。 **ルール名** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**および**親プロセス**： • **完全パス**名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**ファイルを実行するために使用されるコマンド。 • **説明**RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。 **パイプ操作**： • **パイプの名前** • **操作種別**

設定	OS	説明
除外されるレジストリ変更	`Windows`	Kaspersky Endpoint Security は、リストのレジストリ変更を処理しません。除外ルールでは以下を指定できます。 **ルール名** Kaspersky Endpoint Security は、ルールトリガー条件を論理 AND と組み合わせます。 **プロセス**および**親プロセス**： • **完全パス**名前と拡張子を含むファイルのフルパス。Kaspersky Endpoint Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。 • **コマンドラインテキスト**ファイルを実行するために使用されるコマンド。 • **説明**RT_VERSION (VersionInfo) リソースからの FileDescription パラメータの値。 • **元のファイル名**RT_VERSION (VersionInfo) リソースからの OriginalFilename パラメータの値。 • **バージョン**RT_VERSION (VersionInfo) リソースからの FileVersion パラメータの値。 • **ファイルのチェックサム**MD5 と SHA256。 ファイルを手動で選択することもできます。本製品は、選択したファイルからフィールドに自動で入力します。 64 ビットオペレーティングシステムでは、プロセスの実行ファイルの 64 ビットバージョンのパラメータを `C:\windows\system32` フォルダーから手動で入力する必要があります。これは、実行ファイルのパラメータフィールドに、`C:\windows\syswow64` フォルダーにある同じ実行ファイルの 32 ビットバージョンのプロパティからデータが入力されるためです。たとえば、`C:\windows\system32\cmd.exe` を選択した場合、プラグインには `C:\windows\syswow64\cmd.exe` のパラメータが表示されます。このような挙動は、オペレーティングシステムの特性によって決まります。 **レジストリ変更**： • **操作種別** • **パス**変更が行われたレジストリキーのパス。 • **値の名前**変更された値の名前（例：RegistrySizeLimit）。 • **値** • **レジストリファイルの完全名**
除外されるデバイスの操作	`Windows`	Kaspersky Endpoint Security は、リストの USB デバイスに関連する操作を処理しません。除外ルールでは以下を指定できます。 **ルール名** **デバイス種別** **デバイス ID** **デバイス名**

KUMA テレメトリ

Windows 向け

既定では、KUMA サーバーへのイベント送信は無効になっています。KUMA を正しく動作させるには、テレメトリ送信を有効にする必要があります。［*Application*］、［*Security*］または［*System*］のいずれかの標準ログからイベントソースを選択できます。また、サードパーティ製のアプリケーションのログを指定することもできます。パフォーマンスを向上させ、KUMA サーバーへのデータ転送を最適化するために、テレメトリに個別のイベントログを手動で追加できます。

KUMA のテレメトリ設定

設定	OS	説明
Windows イベントログ	`Windows`	本製品が KUMA に送信する Windows ログイベントログを 1 つずつ手動で追加するか、設定を含む JSON ファイルをインポートできます。 各イベントログごとに、送信方法を選択できます。 • **すべてのイベントを送信する**このモードでは、本製品は除外ルールに追加されたイベントを除くすべてのイベントを Windows ログから送信します。 • **選択したイベントのみ送信する**このモードでは、本製品は包含ルールに追加されたイベントのみを送信します。 関連するイベント送信モードの除外ルールまたは包含ルールを作成することもできます。ルールを追加するには、Windows イベントログ内のイベントの ID を指定する必要があります。ルール内に複数のイベント ID をリストできます。複数のイベント ID を指定する場合は、区切りとしてカンマを使用します。

組み込みエージェント

Managed Detection and Response

Windows、macOS 、Linux 向け

Kaspersky Endpoint Security は、Managed Detection and Response ソリューションとの連携をサポートしています。*Kaspersky Managed Detection and Response (MDR)* ソリューションはお客様のインフラストラクチャ内のセキュリティインシデントを自動で検知し分析します。MDR はエンドポイントから取得する遠隔測定したデータと機械学習を使用します。MDR はカスペルスキーのエキスパートにインシデントのデータを送信します。エキスパートはインシデントを処理し、新しい項目を定義データベースに追加するなどの対応をします。また、エキスパートたちはインシデントの処理に対して、コンピューターをネットワークから分離するなど、推奨事項を提示することもあります。ソリューションについて詳しくは、Kaspersky Managed Detection and Response のヘルプ を参照してください。

Managed Detection and Response が動作するためには、次の機能を有効にする必要があります：

- Kaspersky Security Network（拡張モード）
- ふるまい検知

これらの機能は必ず有効にしてください。有効になっていないと、遠隔測定したデータを受け取ることができないため、Kaspersky Managed Detection and Response は機能できません。

Managed Detection and Response コンポーネントの設定

設定	OS	説明
MDR 設定ファイル	`Windows` `macOS` `Linux`	BLOB ファイルには、クライアント ID および Kaspersky Managed Detection and Response のライセンスに関する情報が含まれます。BLOB ファイルは MDR 設定ファイルの ZIP アーカイブ内に保存されています。Kaspersky Managed Detection and Response コンソールからこの ZIP アーカイブを取得できます。BLOB ファイルについて詳しくは、Kaspersky Managed Detection and Response のヘルプ を参照してください。

Endpoint Detection and Response Optimum

Windows、macOS 、Linux 向け

Kaspersky Endpoint Security には Kaspersky Endpoint Detection and Response Optimum ソリューション（以降、「EDR Optimum」とも表記）向けの組み込みエージェントが含まれるようになりました。*Kaspersky Endpoint Detection and Response* は、高度なサイバー脅威から企業の IT インフラストラクチャを保護する幅広いソリューションです。ソリューションの機能は、新しい脆弱性攻撃やランサムウェア、ファイルレス攻撃、またシステムシステムツールを悪用する方法などを含む複雑な脅威の検知とそれらへの対応を組み合わせたソリューションです。

Kaspersky Endpoint Detection and Response は、ユーザーデバイス上の潜在的に危険な活動を分析し、*セキュリティ担当者*または*管理者*に攻撃の可能性に関する情報を提供します。これにより、タイムリーな対応措置を講じたり、設定済みの対応処理を自動的に適用したりできます。

Endpoint Detection and Response が動作するためには、次の機能を有効にする必要があります：

- ファイル脅威対策
- ウェブ脅威対策

- メール脅威対策
- 脆弱性攻撃ブロック
- ふるまい検知
- ホスト侵入防止
- 修復エンジン
- アダプティブアノマリーコントロール

コンポーネントのリストは、各種プラットフォームで異なる場合があります。

Endpoint Detection and Response コンポーネントの設定

設定	OS	説明
詳細なシステム動作の記録を有効にする	Windows macOS Linux	この設定は、**遡及的 IOC スキャン**タスクの正確性を確保するのに役立ちます。これは、大量のコンピューター リソースの使用を伴います。
ネットワーク分離	Windows macOS Linux	検知された脅威への対応として、ネットワークからコンピューターを自動的に分離します。 ネットワーク分離がオンになると、本製品はすべてのアクティブな接続を切断し、コンピューターのすべての新規 TCP/IP 接続をブロックします。次の接続のみ有効にします： • ネットワーク分離の除外リストに追加されている接続。 • 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。
次の時間の経過後、分離されたデバイスを自動的にロック解除する（時間）	Windows macOS Linux	ネットワーク分離は、指定した時間の経過後に自動で、または手動で解除することができます。
ネットワーク分離の除外リスト	Windows macOS Linux	ネットワーク分離から除外されるルールのリストです。ネットワーク分離がオンになっても、ルールに一致するネットワーク接続はブロックされません。 *標準のネットワークプロファイル*のリストを使用してネットワーク分離の除外リストを設定できます。既定では、除外リストには DNS/DHCP サーバーおよび DNS/DHCP クライアントロールを持つデバイスの動作が妨げられないようにするルールを含むネットワークプロファイルが含まれています。標準のネットワークプロファイルまたは除外リストの設定は手動で変更できます。 ポリシーのプロパティで指定された除外リストは、脅威の検知時の対応としてネットワーク分離が自動的にオンになった場合にのみ適用されます。コンピューターのプロパティで指定された除外リストは、Kaspersky Security Center のコンソールのコンピューターのプロパティまたはアラートの詳細から手動でネットワーク分離をオンにした場合にのみ適用されます。
実行防止	Windows macOS Linux	実行ファイルやスクリプトを実行したり、Office 形式のファイルを開いたりする動作をコントロールします。たとえば、選択したコンピューター上で安全でないと判断されたアプリケーションの実行を防止することができます。実行防止は、Office ファイルの拡張子のセットおよびスクリプトインタープリターのセットをサポートしています。 実行防止機能を使用するには、実行防止ルールを追加する必要があります。
禁止されたオブジェクトを実行、または開いたときの処理	Windows macOS Linux	**ブロックしイベントログへ追加する**このモードでは、オブジェクトを実行したり、禁止するルールの基準に一致するドキュメントを開いたりする動作がブロックされます。さらに、オブジェクトを実行しようとしたりドキュメントを開いたりしようとした試みに関するイベントをシステムのイベントログおよび Kaspersky Security Center に記録します。 **イベントログに追加する**このモードでは、Kaspersky Endpoint Security はオブジェクトを実行しようとしたり、防止ルールに一致したドキュメントを開いたりしようとした試みに関するイベントをシステムのイベントログと Kaspersky Security Center に記録しますが、これらの動作をブロックしません。既定ではこのモードが選択されます。
実行防止のルール	Windows macOS Linux	*実行防止ルール*とは、オブジェクトの実行のブロックなど、製品がオブジェクトの実行時への対応時に適用する一連の条件です。本製品は、パスや MD5 または SHA256 ハッシュアルゴリズムで計算されたチェックサムからファイルを識別します。

設定	OS	説明
パスの大文字小文字を区別する	`Linux`	このチェックボックスをオンにすると、本製品は実行防止ルールを作成する際に、ルールの作成を大文字と小文字を区別して扱います。
Cloud Sandbox	`Windows` `macOS` `Linux`	*Cloud Sandbox* はコンピューター上のより高度な脅威を検知する技術です。Kaspersky Endpoint Security は、検知したファイルを自動的に Cloud Sandbox に送って分析します。Cloud Sandbox は、これらのファイルを隔離された環境で実行して悪意のあるアクティビティを検出し、これらのファイルの評判を判断します。これらのファイルのデータは Kaspersky Security Network に送られます。このため、Cloud Sandbox が悪意のあるファイルを検知すると、Kaspersky Endpoint Security はこのファイルが検出されたすべてのコンピューター上でこの脅威を除去するための適切な操作を実行します。 分析対象のオブジェクトに関する情報を取得するには、KSN 接続が必要です。

Endpoint Detection and Response Expert（オンプレミス）

Windows、macOS 、Linux 向け

Endpoint Detection and Response Expert バージョン 7.1 以前

Kaspersky Endpoint Security は、Kaspersky Anti Targeted Attack Platform ソリューションの一部として、Kaspersky Endpoint Detection and Response Expert コンポーネント（バージョン 7.1 以前、以下「EDR (KATA)」とも呼ばれます）をサポートしています。*Kaspersky Anti Targeted Attack Platform* は、標的型攻撃、高度な持続的脅威（APT）、ゼロデイ攻撃などの高度な脅威をタイムリーに検知するために設計されたソリューションです。Kaspersky Anti Targeted Attack Platform には、次の 3 つの機能ユニットが含まれています：

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

すべての機能ユニットまたは個別の機能ユニットを別々に購入できます。ソリューションについて詳しくは、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

Kaspersky Endpoint Security は、企業の IT インフラストラクチャにある個別のコンピューターにインストールされ、プロセス、開かれているネットワーク接続や編集されているファイルを継続的に監視します。コンピューターのイベントに関する情報（テレメトリデータ）は Kaspersky Anti Targeted Attack Platform サーバーに送信されます。この場合、Kaspersky Endpoint Security は、本製品が検出した脅威に関する情報およびその脅威の処理結果についての情報を Kaspersky Anti Targeted Attack Platform サーバーに 送信します。

EDR (KATA) および NDR (KATA) 連携は Kaspersky Security Center コンソールで設定します。タスクの実行、隔離されたオブジェクトの管理、レポートの表示やその他の処理を含む組み込みエージェントは、Kaspersky Anti Targeted Attack Platform コンソールを使用して管理されるようになります。

Endpoint Detection and Response Expert バージョン 8.0 以降

Kaspersky Endpoint Security は、Endpoint Detection and Response Expert クラス（バージョン 8.0 以降、以下「EDR Expert（オンプレミス）」とも呼ばれます）のカスペルスキーソリューションをサポートしています。このようなソリューションには、たとえば Kaspersky Symphony XDR などがあります。*Endpoint Detection and Response Expert（オンプレミス）*は、組織がほとんどの種類のサイバーリスクから防御し、最も重要な脅威の拡散シナリオに対応できるようにするエンタープライズ向けサイバーセキュリティソリューションです。

EDR Expert（オンプレミス）は、企業インフラストラクチャから受信したログとテレメトリを分析して攻撃を自動的に検知し、カスペルスキー製品やサードパーティの情報セキュリティ製品からのイベントを含む、EDR Expert（オンプレミス）で収集されたすべてのイベントを統合した調査グラフを使用してインシデントを調査できます。

Endpoint Detection and Response Expert に必要なコンポーネント

Endpoint Detection and Response Expert が動作するためには、次の機能を有効にする必要があります：

- ファイル脅威対策
- ウェブ脅威対策
- メール脅威対策
- 脆弱性攻撃ブロック
- ふるまい検知
- ホスト侵入防止
- AMSI 保護
- バックグラウンドスキャン
- Kaspersky Security Network

コンポーネントのリストは、各種プラットフォームで異なる場合があります。

Endpoint Detection and Response Expert（オンプレミス）コンポーネントの設定

設定	OS	説明

Endpoint Detection and Response Expert ソリューション	`Windows`
	`macOS`
	`Linux`
		Kaspersky Endpoint Security と連携できる Endpoint Detection and Response のエキスパート ソリューションです。
		• **Endpoint Detection and Response Expert（バージョン 7.1 以前）**
		• **Endpoint Detection and Response Expert（バージョン 8.0 以降）**

設定	OS	説明
接続設定	`Windows` `macOS` `Linux`	次の KATA またはテレメトリ収集サーバーの接続設定を管理します。 • **サーバーの接続タイムアウト**Central Node サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の Central Node サーバーに接続を試みます。 • **サーバー証明書**Central Node サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプ を参照してください）。 • **相互認証を使用する**Kaspersky Endpoint Security と Central Node サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、Central Node サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナーを取得して暗号化コンテナーを保護するパスワードを設定します。*暗号化コンテナ*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプ を参照してください）。Central Node を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。 暗号化コンテナはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナを追加することはできません。
サーバーに同期リクエストを送信する間隔（分） *（Endpoint Detection and Response Expert のバージョン 7.1 以前でのみ利用可能）*	`Windows` `macOS` `Linux`	サーバーに送信される同期リクエストの頻度。同期中に、Kaspersky Endpoint Security は変更した製品設定とタスクに関する情報を送信します。
KATA サーバーへの接続 / テレメトリ収集サーバーへの接続	`Windows` `macOS` `Linux`	Kaspersky Anti Targeted Attack Platform サーバーまたはテレメトリ収集サーバーに接続するための IP アドレス（IPv4 または IPv6）とポート番号を入力します。 Central Node サーバー（KATA）またはテレメトリ収集サーバーには、複数のアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスを使用してサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスを使用して接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。 EDR（KATA）ソリューションと EDR Expert（オンプレミス）ソリューションは、異なるアーキテクチャを採用しています。テレメトリの処理には、EDR Expert（オンプレミス）はテレメトリ収集サーバーを使用し、EDR（KATA）は Central Node サーバーを使用します。このため、本製品を EDR Expert（オンプレミス）と連携する場合は、テレメトリ収集サーバーを追加する必要があります。
KATA にテレメトリを送信する / テレメトリ収集サーバーにテレメトリを送信する	`Windows` `macOS` `Linux`	この機能により、選択したソリューションに応じて、テレメトリが KATA サーバーまたはテレメトリ収集サーバーに送信されることを完全に防止できます。例えば、テレメトリを使用する別のソリューションとあわせて Kaspersky Anti Targeted Attack Platform を使用している場合は、KATA (EDR) 向けのテレメトリ送信をオフにすることができます。これにより、これらのソリューションのサーバー負荷を最適化することができます。 Managed Detection and Response ソリューションと KATA (EDR) を導入している場合、MDR テレメトリを使用して KATA (EDR) で脅威応答タスクを作成することができます。
IOA のあるテレメトリのみ送信する *（Endpoint Detection and Response Expert のバージョン 8.0 以降でのみ利用可能）*	`Windows` `Linux`	これにより、テレメトリを最適化し、IOA のあるテレメトリのみを送信できるようになります。 *攻撃の痕跡（IOA）*は、標的型攻撃を示す可能性のあるシステム内の疑わしい動作の説明を含むルールです。本製品は、システム内で進行中の動作をこれらのルールと比較し、標的型攻撃を示唆するイベントをログに記録します。本製品は、このようなイベントをリアルタイムで追跡できるストリーミングスキャンの技術を採用しています。
最大イベント転送遅延時間（秒）	`Windows` `macOS` `Linux`	指定した同期間隔の期間が過ぎると、本製品はイベント送信のためサーバーと同期します。
イベントパッケージの最大数	`Windows`	バッファがイベントでいっぱいになると、本製品はサーバーと同期します。

設定	OS	説明
リクエストの調整を有効にする	`Windows` `macOS` `Linux`	これは、サーバーの負荷の最適化に役立ちます。この機能が有効になっている場合、本製品は送信されるイベントを制限します。イベント数が設定した制限値を超えると、Kaspersky Endpoint Security はイベントの送信を停止します。 **1時間ごとのイベントの最大数**本製品はテレメトリデータストリームを分析し、イベントストリームが設定した時間当たりのイベント数を超えた場合は、イベントの送信を制限します。1時間後にイベントの送信は再開されます。本製品がサーバーにインストールされている場合、テレメトリデータストリームの値は高くなります。サーバーの場合、値を1時間あたり60,000イベントに増やすことを推奨します。 **イベントの制限超過のパーセンテージ**本製品は種別ごと（「レジストリの変更」イベントなど）にイベントを並べ替えます。全体のイベント合計数に対して同じ種別のイベントが占める比率が設定された割合を超えると、本製品はイベントの転送を制限します。その他のイベントが占める全体のイベントの割合がまた大きくなった場合はイベントの送信を再開します。
応答サーバーへの接続 *（Endpoint Detection and Response Expert のバージョン 8.0 以降でのみ利用可能）*	`Windows` `macOS` `Linux`	応答サーバーへの接続設定。応答サーバーの IP アドレス（IPv4、IPv6）とサーバーに接続するポートを指定します。 複数の応答サーバーアのドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスを使用してサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスを使用して接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。
接続設定 *（Endpoint Detection and Response Expert のバージョン 8.0 以降でのみ利用可能）*	`Windows` `macOS` `Linux`	応答サーバーの接続用に以下を設定します： • **サーバーの接続タイムアウト**応答サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別のサーバーに接続を試みます。 • **サーバー証明書**応答サーバーと信頼済みの接続を確立するための TLS 証明書。 • **相互認証を使用する**Kaspersky Endpoint Security と応答サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、応答サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナを取得して暗号化コンテナを保護するパスワードを設定します。*暗号化コンテナ*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。応答サーバーを設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナを読み込む必要があります。 暗号化コンテナはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナを追加することはできません。

Network Detection and Response (KATA)

Windows、Linux 向け

Kaspersky Endpoint Security は、Kaspersky Anti Targeted Attack Platform (EDR (KATA))ソリューションの一部である Kaspersky Network Detection and Response コンポーネントとの連携をサポートします。*Kaspersky Anti Targeted Attack Platform* は、標的型攻撃、高度な持続的脅威（APT）、ゼロデイ攻撃などの高度な脅威をタイムリーに検知するために設計されたソリューションです。Kaspersky Anti Targeted Attack Platform には、次の3つの機能ユニットが含まれています：

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

すべての機能ユニットまたは個別の機能ユニットを別々に購入できます。ソリューションについて詳しくは、Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

Kaspersky Endpoint Security は、企業の IT インフラストラクチャにある個別のコンピューターにインストールされ、プロセス、開かれているネットワーク接続や編集されているファイルを継続的に監視します。コンピューターのイベントに関する情報（テレメトリデータ）は Kaspersky Anti Targeted Attack Platform サーバーに送信されます。この場合、Kaspersky Endpoint Security は、本製品が検出した脅威に関する情報およびその脅威の処理結果についての情報を Kaspersky Anti Targeted Attack Platform サーバーに 送信します。

EDR (KATA) および NDR (KATA) 連携は Kaspersky Security Center コンソールで設定します。タスクの実行、隔離されたオブジェクトの管理、レポートの表示やその他の処理を含む組み込みエージェントは、Kaspersky Anti Targeted Attack Platform コンソールを使用して管理されるようになります。

Network Detection and Response (KATA) が動作するには、次のコンポーネントを有効にする必要があります。

- ファイル脅威対策
- ウェブ脅威対策
- メール脅威対策
- 脆弱性攻撃ブロック
- ふるまい検知
- ホスト侵入防止
- AMSI 保護
- バックグラウンドスキャン
- Kaspersky Security Network

コンポーネントのリストは、各種プラットフォームで異なる場合があります。

Network Detection and Response (KATA) コンポーネントの設定

設定	OS	説明
接続設定（KATA サーバー）	Windows Linux	**サーバーの接続タイムアウト**Central Node サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の Central Node サーバーに接続を試みます。 **サーバー証明書**Central Node サーバーと信頼済みの接続を確立するための TLS 証明書。TLS 証明書は Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。 **相互認証を使用する**Kaspersky Endpoint Security と Central Node サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、Central Node サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナーを取得して暗号化コンテナーを保護するパスワードを設定します。*暗号化コンテナ*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプを参照してください）。Central Node を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。 暗号化コンテナはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナを追加することはできません。
KATA サーバーへの接続	Windows Linux	Kaspersky Anti Targeted Attack Platform サーバーへの接続を設定します。接続する Central Node サーバーの IP アドレス (IPv4 または IPv6) とポートを入力します。 複数の Central Node サーバーアドレスを追加できます。Kaspersky Endpoint Security は、最初の IP アドレスを使用してサーバーに接続しようとします。接続を確立できない場合、リストの 2 番目の IP アドレスを使用して接続しようとします。それでも接続を確立できない場合は、以降同様に次の IP アドレスで接続を試行します。
KATA サーバーに同期リクエストを送信する間隔（分）	Windows Linux	サーバーに送信される同期リクエストの頻度。同期中に、Kaspersky Endpoint Security は変更した製品設定とタスクに関する情報を送信します。
最大イベント転送遅延時間（秒）	Windows Linux	指定した同期間隔の期間が過ぎると、本製品はイベント送信のためサーバーと同期します。

設定	OS	説明
リクエストの調整を有効にする	Windows Linux	これは、サーバーの負荷の最適化に役立ちます。この機能が有効になっている場合、本製品は送信されるイベントを制限します。イベント数が設定した制限値を超えると、Kaspersky Endpoint Security はイベントの送信を停止します。 **1時間ごとのイベントの最大数**本製品はテレメトリデータストリームを分析し、イベントストリームが設定した時間当たりのイベント数を超えた場合は、イベントの送信を制限します。1時間後にイベントの送信は再開されます。本製品がサーバーにインストールされている場合、テレメトリデータストリームの値は高くなります。サーバーの場合、値を1時間あたり60,000イベントに増やすことを推奨します。 **イベントの制限超過の割合（%）**本製品は種別ごと（「レジストリの変更」イベントなど）にイベントを並べ替えます。全体のイベント合計数に対して同じ種別のイベントが占める比率が設定された割合を超えると、本製品はイベントの転送を制限します。その他のイベントが占める全体のイベントの割合がまた大きくなった場合はイベントの送信を再開します。

Sandbox

Windows、Linux 向け

Kaspersky Endpoint Security は、Kaspersky Anti Targeted Attack Platform ソリューションの一部である Kaspersky Sandbox ソリューションおよび Sandbox コンポーネントとの連携をサポートします。*Sandbox* コンポーネントはコンピューター上の高度な脅威を検知し、自動的にブロックします。Sandbox は、オブジェクトのふるまいを分析し、悪意のある操作や、組織の IT インフラストラクチャに向けられた標的型攻撃に特有の動作を検知します。Sandbox は、Microsoft Windows オペレーティングシステムの仮想イメージを配備した特別なサーバー（Sandbox サーバー）上でオブジェクトを分析およびスキャンします。ソリューションについて詳しくは、Kaspersky Sandbox のヘルプおよび Kaspersky Anti Targeted Attack Platform のヘルプを参照してください。

KATA Sandbox コンポーネントでは、自動でファイルをスキャンできるだけでなく、ファイルコンテキストメニューから手動でスキャンすることもできます。

KATA Sandbox を使用するには、Kaspersky Anti Targeted Attack Platform 7.0 以降を導入する必要があります。

Sandbox コンポーネントの設定

設定	OS	説明
連携モード	Windows Linux	**Kaspersky Sandbox**Kaspersky Sandbox ソリューションとの連携本製品によって Kaspersky Sandbox でスキャンするファイルが送信されるのは、自動モードの場合のみです。 **KATA Sandbox**Kaspersky Anti Targeted Attack Platform ソリューションの Sandbox コンポーネントとの連携スキャン用ファイルの送信モードを選択できます： • **手動**ユーザーはコンテキストメニューから手動でスキャン用ファイルを送信します（[**Sandbox に送る**]）。 • **自動**本製品はオブジェクトを自動的に検知し、スキャンのために Sandbox に送信します。 • **複合**本製品は、スキャン対象のオブジェクトを自動的に Sandbox に送信します。必要に応じて、ユーザーはコンテキストメニューから個々のファイルをスキャン対象として送信することもできます。
Sandbox サーバーへの接続	Windows Linux	**Kaspersky Sandbox**Sandbox サーバーの接続設定です。サーバーは配備された Microsoft Windows オペレーティングシステムの仮想イメージを使用してスキャンする必要のあるオブジェクトを実行します。Sandbox サーバーの IP アドレス（IPv4、IPv6 または DNS）とサーバーに接続するポートを指定します。 **KATA Sandbox**：Central Node サーバーの接続設定。Central Node によって、スキャンの最適な設定が選択されて、Sandbox サーバー間の負荷が分散されます。Central Node サーバーの IP アドレス（IPv4、IPv6 または DNS）とサーバーに接続するポートを指定します。

設定	OS	説明
サーバーの接続設定	Windows Linux	**サーバーの接続タイムアウト**Sandbox サーバー（Kaspersky Sandbox 用）または Central Node サーバー（KATA 用）の接続タイムアウト。設定したタイムアウト期間が経過すると、Kaspersky Endpoint Security は要求を次のサーバーに送ります。接続スピードが遅いまたは接続が安定していない場合は、サーバーの接続タイムアウトの時間を長くすることができます。要求のタイムアウトは 0.5 秒以下を推奨します。 **要求のキュー**要求のキューフォルダーのサイズです。Sandbox でスキャンするために複数のオブジェクトを送信する場合、Kaspersky Endpoint Security は要求のキューを作成します。既定では要求のキューフォルダーは 100 MB に制限されています。最大サイズに到達すると、Sandbox は新しい要求のキューへの追加を停止し、関連するイベントを Kaspersky Security Center に送ります。サーバーの設定にお浮いて、要求のキューフォルダーのサイズを設定することができます。 **サーバー TLS 証明書**Sandbox サーバー（Kaspersky Sandbox 用）または Central Node サーバー（KATA 用）との信頼済みの接続を設定するには、TLS 証明書を準備する必要があります。次に、ポリシーを使用してこの証明書をコンピューターに追加する必要があります。また、証明書を Sandbox サーバー（Kaspersky Sandbox 用）または Central Node サーバー（KATA 用）に追加する必要があります。 **相互認証を使用する**（KATA Sandbox のみ）。Kaspersky Endpoint Security と Central Node サーバー間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、Central Node サーバーの設定で相互認証を有効にする必要があります。その後、暗号化コンテナーを取得して暗号化コンテナーを保護するパスワードを設定します。*暗号化コンテナ*とは、証明書と秘密鍵が含まれた PFX アーカイブです。暗号化コンテナーは Kaspersky Anti Targeted Attack Platform コンソールで取得できます（Kaspersky Anti Targeted Attack Platform のヘルプ を参照してください）。Central Node を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナーを読み込む必要があります。
脅威の検知時の処理	Windows Linux	**コピーを隔離に移動し、オブジェクトを削除する**このオプションを選択した場合、Kaspersky Endpoint Security はコンピューターで検知された悪意のあるオブジェクトを削除します。オブジェクトを削除する前に、後でオブジェクトを復元する必要がある場合に備えて、Kaspersky Endpoint Security はそのオブジェクトのバックアップコピーを作成します。バックアップコピーは隔離に移動されます。 **簡易スキャンを実行する**このオプションを選択した場合、Kaspersky Endpoint Security は*Critical Areas Scan*タスクを実行します。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。 **IOC スキャンタスクを作成する**このオプションを選択した場合、Kaspersky Endpoint Security は自動的に *IOC Scan（自動 IOC スキャンタスク）*を作成します。このタスクに対して、実行モード、スキャン範囲、および IOC の検知時の動作（*コピーを隔離に移動し、オブジェクトを削除する*または*簡易スキャンを実行する*）を設定できます。その他の *IOC Scan*タスクの設定を変更するには、タスクの設定に移動してください。
IOC スキャン範囲	Windows Linux	**重要なファイル領域**このオプションを選択した場合、 Kaspersky Endpoint Security は、選択したユーザープロファイルディレクトリや重要なシステムオブジェクトなど、コンピューターの重要なファイル領域でのみ IOC をスキャンします。 **コンピューターのシステムドライブのファイル領域**このオプションを選択した場合、Kaspersky Endpoint Security はコンピューターのシステムドライブで IOC スキャンを実行します。 本製品は、選択したスキャン範囲に関係なく、脅威が検出されたファイルパス内の IOC もスキャンします。
IOC スキャンタスクを実行する	Windows Linux	**手動**都合の良いときに手動で *IOC Scan*タスクを開始できる実行方法です。 **自動**脅威が検知されたときに自動で Kaspersky Endpoint Security が *IOC* スキャンタスクを実行する実行モードです。 Windows **コンピューターを使用していないときにのみ実行する**：スクリーンセーバーが動作しているまたは画面がロックされているときに Kaspersky Endpoint Security が *IOC* スキャンタスクを実行する実行モードです。ユーザーがコンピューターをロック解除すると、Kaspersky Endpoint Security はタスクを一時停止します。このため、タスクの完了まで数日かかることがあります。

KUMA との連携

Windows、Linux 向け

Kaspersky Endpoint Security は、Kaspersky Unified Monitoring and Analysis Platform ソリューションをサポートしています。*Kaspersky Unified Monitoring and Analysis Platform (KUMA)* は、組織の IT インフラストラクチャ向けの SIEM (Security Information and Event Management) ソリューションです。KUMA を使用すると、セキュリティ上の脅威が被害をもたらす前にそれを検知、分析し、緩和することができます。

Kaspersky Endpoint Security は、企業の IT インフラストラクチャにある個別のコンピューターにインストールされ、プロセス、開かれているネットワーク接続や編集されているファイルを継続的に監視します。コンピューターのイベントに関する情報（テレメトリ）は Kaspersky Unified Monitoring and Analysis Platform (KUMA) サーバーに送信されます。

既定では、KUMA サーバーへのイベント送信は無効になっています。KUMA を正しく動作させるため、まず［全般設定］→［テレメトリの設定］セクションで KUMA へのテレメトリ送信を有効にします。

Kaspersky Endpoint Security は、KUMA のエージェントのすべての機能を提供するわけではありません。本製品はマークアップなしでイベントのみを KUMA に送信します。KUMA のすべての機能にアクセスするには、ライセンスを購入し、KUMA 管理者ガイドに従ってソリューションを導入する必要があります。

KUMA コンポーネントの設定

設定	OS	説明
サーバーの接続設定	Windows Linux	**サーバーの接続タイムアウト**KUMA サーバーの応答がタイムアウトするまでの最大値。タイムアウトすると、Kaspersky Endpoint Security は別の KUMA サーバーに接続を試みます。 **サーバー証明書**KUMA サーバーと信頼済みの接続を確立するための TLS 証明書。Kaspersky Unifield Monitoring and Analysis Platform コンソールで TLS 証明書を取得できます（Kaspersky Unified Monitoring and Analysis Platform の手順を参照してください）。 **相互認証を使用する**Kaspersky Endpoint Security と KUMA 間でセキュアな通信を確立する際の相互認証。相互認証を使用するには、KUMA コンソールの TCP コネクター設定で、TLS モード［**Custom PFX**］を選択する必要があります（種別が TCP のコネクターの設定については、Kaspersky Unified Monitoring and Analysis Platform のヘルプを参照してください）。次に、暗号化コンテナを取得し、暗号コンテナを保護するためのパスワードを設定する必要があります。*暗号化コンテナ*とは、証明書と秘密鍵が含まれた PFX アーカイブです。KUMA を設定した後、Kaspersky Endpoint Security の設定でも相互認証を有効にして、パスワード保護された暗号化コンテナを読み込む必要があります。 暗号化コンテナはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナを追加することはできません。
イベント送信時の最大遅延（秒）	Windows Linux	指定した同期間隔の期間が過ぎると、本製品はイベント送信のためサーバーと同期します。
TLS 暗号化を使用する	Windows Linux	この機能を有効にすると、Kaspersky Endpoint Security はTLS 証明書を使用して KUMA サーバーとの信頼済みの接続を確立します。
KUMA サーバーへの接続	Windows Linux	KUMA サーバーの接続設定サーバーへの接続に使用する IP アドレス（IPv4 または IPv6）、接続プロトコル、およびポートを指定します。 複数の KUMA サーバーアドレスを追加できます。Kaspersky Endpoint Security はリストの 1 番目の KUMA サーバーに接続します。接続に失敗した場合、リストの 2 番目の KUMA サーバーに接続します。

Light Agent モード

SVM 検出設定

Windows、Linux 向け

Light Agent を起動すると、その仮想マシンである SVM（Secure Virtual Machine）への接続が確立され、維持されます。Protection Server は SVM 上に導入されます。*Protection Server* は、ファイル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、定義データベースをアップデートし、ライセンスを管理する Kaspersky Security for Virtualization Light Agent ソリューションのコンポーネントです。Light Agent は、スキャンが必要なファイルのフラグメントを SVM に送信します。スキャン結果は、Light Agent がインストールされているすべての仮想マシンで利用できます（SharedCache 技術）。このように、SharedCache 技術によりソリューションの効率が向上し、脅威への対応が迅速化されます。

組織のインフラストラクチャには、Light Agent がインストールされた多数の仮想マシンと、多数の SVM が含まれる場合があります。Integration Server コンポーネントは、ソリューション コンポーネントと仮想インフラストラクチャ間の連携を目的としています。*Integration Server* - Kaspersky Security for Virtualization Light Agent のコンポーネントで、利用可能な SVM のリストを作成してそのデータを Light Agent に送信したり、Light Agent による SVM の検出を管理したり、Light Agent と SVM 間の接続を保護したりします。

SVM 検出設定

設定	OS	説明
Integration Server を使用する	`Windows` `Linux`	Integration Server は、SVM 間で負荷を自動的に分散するので、大規模な仮想インフラストラクチャで役立ちます。 Integration Server の接続設定を入力します。 • Integration Server がインストールされているデバイスの IPv4 形式による IP アドレスまたは完全修飾ドメイン名（FQDN）。 • Integration Server に接続するためのポート番号。既定ではポート 7271 が指定されます。 • Integration Server の管理者のパスワード（管理者アカウントのパスワード）。
SVM アドレスのカスタムリストを使用する	`Windows` `Linux`	Light Agent が接続できる SVM のリストを作成します。SVM の IP アドレス（IPv4 形式）、または完全修飾ドメイン名（FQDN）を指定します。複数の SVM の IP アドレスまたは完全修飾ドメイン名を 1 行に 1 つずつ入力して入力できます。 SVM アドレスのリストで、単一の IP アドレスと一致す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、ソリューションでエラーが発生する可能性があります。

Integration Server 接続設定

Windows、Linux 向け

Integration Server は、Kaspersky Security for Virtualization Light Agent と仮想インフラストラクチャとの通信を可能にするソリューションのコンポーネントです。Integration Server は、接続できる SVM のリストを保持します。Light Agent は、Integration Server との接続を確立し、SVM アドレスのリストを取得します。

Integration Server は、SVM 間で負荷を自動的に分散するので、大規模な仮想インフラストラクチャで役立ちます。Integration Server は、使用可能な SVM に関する情報を取得し、分析して、接続に最適な Protection Server（SVM）のリストを Light Agent に提供します。

Integration Server 接続設定

設定	OS	説明
アドレス	`Windows` `Linux`	Integration Server の IPv4 形式による 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」が指定されていた場合、Integration Server への接続はエラーで終了します。
ポート	`Windows` `Linux`	Integration Server に接続するためのポート番号。 既定ではポート 7271 が指定されます。
Integration Server の認証	`Windows` `Linux`	Integration Server の管理者のパスワード（`admin` アカウントのパスワード）。 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 接続タグ

Windows、Linux 向け

複数の Light Agent を 1 つの SVM に接続することができます。複数の Light Agent の接続のバランスをとるために、SVM 検出設定セクションで SVM の個別のリストを指定することができます。SVM 検出に Integration Server を使用している場合は、タグを使用して、複数の SVM に対する複数の Light Agent の接続のバランスをとることができます。つまり、1 つの Light Agent に対して、タグを使用して、接続する SVM のリストを割り当てることができます。これを行うには、タグを Light Agent に割り当てて、SVM 設定でこのタグを指定する必要があります。SVM 設定でのタグの指定について詳しくは、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください。

例：Kaspersky Endpoint Detection and Response Optimum ソリューションは、指定された仮想マシンホストのインフラストラクチャに導入されます。この場合、`[EDROptimum]` タグを Light Agent に割り当てて、EDR Optimum（EDR Optimum アドオン）ライセンスが追加された SVM に接続することができます。これにより、Light Agent がインストールされている仮想マシンで EDR Optimum 機能を使用できるようになります。EDR Optimum ライセンスのない SVM に Light Agent を接続した場合、Kaspersky Endpoint Detection and Response Optimum 機能は使用できません。

タグを使用して Light Agent を SVM に接続するには、［**接続タグを使用する**］をオンにします。SVM 接続タグを入力します。タグには 255 文字までのテキスト文字列を入力できます。［`;`］以外のすべての文字を使用できます。

SVM 選択アルゴリズム

Windows、Linux 向け

組織のインフラストラクチャには、Light Agent が接続できる SVM が複数導入されている場合があります。仮想インフラストラクチャのネットワークとリソースの負荷を分散するには、Light Agent を複数の SVM に分散させる必要があります。

SVM 選択アルゴリズムの設定

設定	OS	説明
標準の SVM 選択アルゴリズムを使用する	`Windows` `Linux`	このアルゴリズムを使用する場合、インストールおよび起動後、仮想マシン上の Light Agent は、Light Agent に対して *ローカル* な SVM への接続を選択します。SVM をローカルとして識別するために、Light Agent は主に仮想インフラストラクチャ内の SVM の場所を使用します。SVM が Light Agent と同じハイパーバイザーに配置されている場合、Light Agent はそのような SVM をローカルと判断します。一部の仮想インフラストラクチャでは、設定ファイルを使用してローカルの SVM を手動で指定する必要があります。 接続に適したローカルの SVM が見つからない場合、Light Agent は、仮想インフラストラクチャ内の SVM の位置に関係なく、接続されている Light Agent の数が最も少ない SVM を選択します。
拡張 SVM 選択アルゴリズムを使用する	`Windows` `Linux`	拡張アルゴリズムを使用すると、ローカルの SVM の選択条件を手動で指定したり、ローカルの SVM 検出を無効にしたりできます。そのためには、仮想インフラストラクチャ内の SVM パス（ハイパーバイザー、クラスタ、またはデータセンター）を選択する必要があります。つまり、ローカルの SVM を検出する範囲を選択する必要があります。Light Agent は、設定された検出範囲にあるローカルの SVM に接続できない場合、接続の試行を停止します。 拡張アルゴリズムを使用して、Light Agent に対して、ローカルの SVM の検出を無効にすることもできます。この場合、Light Agent は、仮想インフラストラクチャ全体で接続されている Light Agent の数が最も少ない SVM を選択します。

接続の保護

Windows、Linux 向け

Light Agent と Protection Server 間の接続の暗号化を設定できます。これを行うには、SVM の Protection Server 設定および Light Agent 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する必要があります。

接続保護が有効になっている Light Agent は、Light Agent と Protection Server 間のデータチャネルの暗号化が有効になっている SVM にのみ接続できます。接続保護が無効になっている Light Agent は、チャネル暗号化が無効になっているか、Protection Server と Light Agent 間のセキュアでない接続が許可されている SVM にのみ接続できます。

Protection Server での接続の保護の設定について詳しくは、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください。

暗号化を使用して接続を保護すると、Kaspersky Security for Virtualization Light Agent のパフォーマンスに影響する可能性があります。

補足資料 6：外部サービスとの対話設定

Kaspersky Endpoint Security は、外部サービスとの対話に次のネットワーク設定と暗号化設定を使用します：

外部サービスとの対話設定

サービスとプロトコルのネットワークアドレス	説明
activation-v2.kaspersky.com/activationservice/activationservice.svc プロトコル：HTTPS ポート：443	本製品のアクティベーション。
s00.upd.kaspersky.com s01.upd.kaspersky.com s02.upd.kaspersky.com s03.upd.kaspersky.com s04.upd.kaspersky.com s05.upd.kaspersky.com s06.upd.kaspersky.com s07.upd.kaspersky.com s08.upd.kaspersky.com s09.upd.kaspersky.com s10.upd.kaspersky.com s11.upd.kaspersky.com s12.upd.kaspersky.com s13.upd.kaspersky.com s14.upd.kaspersky.com s15.upd.kaspersky.com s16.upd.kaspersky.com s17.upd.kaspersky.com s18.upd.kaspersky.com s19.upd.kaspersky.com プロトコル：HTTPS ポート：443	定義データベースと機能のアップデート

サービスとプロトコルのネットワークアドレス	説明
p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com プロトコル：HTTP ポート：80	定義データベースと機能のアップデート
downloads.upd.kaspersky.com プロトコル：HTTPS ポート：443	• 定義データベースと機能のアップデート • カスペルスキーサーバーへのアクセスの確認。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： 1. Google Public DNS (8.8.8.8) 2. Cloudflare DNS (1.1.1.1) 3. Alibaba Cloud DNS (223.6.6.6) 4. Quad9 DNS (9.9.9.9) 5. CleanBrowsing (185.228.168.168) 本製品は DNS サーバーとの TCP/UDP 接続を確立するため、要求にはドメインアドレスとユーザーの外部 IP アドレスが含まれる場合があります。たとえば、HTTPS で通信する時に Web リソースの証明書を確認するために、この情報が必要になります。パブリック DNS サーバーが使用されている場合、データ処理ルールは、対応するサービスのプライバシーポリシーによって管理されます。
ds.kaspersky.com プロトコル：HTTPS ポート：443	Kaspersky Security Network を使用する

サービスとプロトコルのネットワークアドレス	説明
ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com プロトコル：KSN ポート：443、1443	Kaspersky Security Network を使用する
click.kaspersky.com プロトコル：HTTPS ポート：443	ユーザーインターフェイスからのリンクをたどる。
crl.kaspersky.com ocsp.kaspersky.com プロトコル：HTTP ポート：80	公開鍵基盤（PKI）。 これらのサーバー (crl.kaspersky.com) は公開鍵インフラストラクチャ (PKI) の一部であり、カスペルスキーデジタル署名証明書の有効性ステータスを確認するために必要です。CRL サーバーは失効した証明書のリストを提供します。OCSP サービスを使用すると、特定の証明書のステータスをリアルタイムで照会できます。これらのコンポーネントは、デジタル証明書との対話のセキュリティを維持し、起こりうる攻撃に対する保護を提供します。

カスペルスキー製品との相互運用性

Kaspersky Endpoint Security は、一部のカスペルスキー製品との相互運用性をサポートしています。アプリケーションの相互運用性を最適化するには、このセクションのガイドラインに従ってください。

Kaspersky Security Center Linux

Kaspersky Endpoint Security for Linux と Kaspersky Security Center Linux を併用する場合は、この記事で説明する設定を使用することを推奨します。

推奨設定

本ソフトウェアの機能	推奨される機能の状態	推奨事項
ファイル脅威対策	Enabled	保護の除外を追加します： • /opt/kaspersky/klnagent/sbin/klnagent • /opt/kaspersky/klnagent64/sbin/klnagent • /var/lib/postgresql/<PostgreSQL version>
マルウェアのスキャン	Enabled	
リムーバブルドライブのスキャン	無効	–
ふるまい検知	Enabled	既定の設定を使用します。
ネットワーク脅威対策	Enabled	eBPF のネットワークトラフィックインターセプトモードを選択します NetInterceptorMode=UseEBPF
ウェブ脅威対策	Enabled	既定の設定を使用します。
アンチクリプター	無効	–
コンテナスキャン	無効	–
インベントリ	無効	–

本ソフトウェアの機能	推奨される機能の状態	推奨事項
デバイスコントロール	無効	–
アプリケーションコントロール	無効	–
ファイアウォール	無効	–
ウェブコントロール	無効	–
システム変更監視	Enabled	スキャン範囲を追加します： • /etc • /opt/kaspersky/kesl/ • /opt/kaspersky/ksc64
システム整合性チェック	無効	–
Endpoint Detection and Response Expert（オンプレミス）	Enabled	既定の設定を使用します。
Endpoint Detection and Response Expert（クラウド）	無効	–
Managed Detection and Response	Enabled	既定の設定を使用します。
Network Detection and Response (KATA)	無効	–
KUMA との連携	無効	–
Sandbox	無効	–
対応処理	一部制限事項が適用されます	対応処理では、Kaspersky Endpoint Security for Linux に必要なオブジェクトや、重要なシステムオブジェクトを除外することはできません。対応処理を開始する際は、システムや使用しているアプリケーションに支障をきたさないことを確認してください。
グラフィカルインターフェイス	未設定	–
Kaspersky Endpoint Security for Linux 管理 Web プラグイン	インストール済み	既定の設定を使用します。
Kaspersky Endpoint Security for Linux MMC 管理プラグイン	インストール済み	既定の設定を使用します。
ネットワークエージェント	インストール済み	既定の設定を使用します。
ファイル操作のインターセプト機構	fanotify に基づくシステムインターセプターメカニズム	既定の設定を使用します。
システムイベントテレメトリソース	eBPF+auditd	`TelemetrySource=Default`
脆弱性攻撃ブロック	無効	–
Kaspersky Security Network の使用	Enabled	既定の設定を使用します。
メール脅威対策	Enabled	既定の設定を使用します。
有害 USB 攻撃ブロック	無効	–

本ソフトウェアの機能	推奨される機能の状態	推奨事項
グローバル除外リスト	設定済み	クイックインストールスクリプトを使用して Kaspersky Security Center をインストールする場合は、マウントポイントを除外リストに追加します： `/var/lib/postgresql/<PostgreSQL version>/main` `<PostgreSQL version>` は、使用している PostgreSQL DBMS のバージョン番号です。

Network Detection and Response (KATA)

Kaspersky Endpoint Security for Linux を Network Detection and Response（KATA）と併用する場合は、この記事に記載されている設定を使用することを推奨します。

また、Kaspersky Anti Targeted Attack（KATA）Platformソリューションのドキュメントも確認してください。

Sensor コンポーネントが搭載されたサーバー上のKaspersky Endpoint Security for Linuxの設定

Sensor サーバーの推奨設定

本ソフトウェアの機能	推奨される機能の状態	推奨事項
ファイル脅威対策	Enabled	保護の除外を追加します： • `[container-name:*kata_scanner*]/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*preprocessor_icap*]/tmp/content` • `[container-name:*preprocessor_span*]/tmp/suricata` • `[container-name:*preprocessor_span*]/mnt/kaspersky/nta` • `[container-name:*preprocessor_smtp*]/tmp/` • `[container-name:*preprocessor_pop*]/tmp/` • `[container-name:*sandbox_scan*]/tmp/` • `[container-name:*]/var/log/kaspersky`
マルウェアのスキャン	無効	–
リムーバブルドライブのスキャン	無効	–
ふるまい検知	Enabled	既定の設定を使用します。
ネットワーク脅威対策	無効	–
ウェブ脅威対策	無効	–
アンチクリプター	無効	–
コンテナスキャン	Enabled	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するには、コンテナ監視を有効にします `NamespaceMonitoring=Yes`
インベントリ	無効	–
デバイスコントロール	無効	–
アプリケーションコントロール	無効	–
ファイアウォール	無効	–

本ソフトウェアの機能	推奨される機能の状態	推奨事項
ウェブコントロール	無効	–
システム変更監視	無効	–
システム整合性チェック	無効	–
Endpoint Detection and Response Expert（オンプレミス）	無効	–
Endpoint Detection and Response Expert（クラウド）	無効	–
Managed Detection and Response	無効	–
Network Detection and Response (KATA)	無効	–
KUMA との連携	無効	–
Sandbox	無効	–
対応処理	無効	–
グラフィカルインターフェイス	未設定	–
ネットワークエージェント	インストール済み	既定の設定を使用します。
ファイル操作のインターセプト機構	fanotify に基づくシステムインターセプターメカニズム	既定の設定を使用します。
システムイベントテレメトリソース	eBPF+auditd	`TelemetrySource=Default`
脆弱性攻撃ブロック	無効	–
Kaspersky Security Network の使用	Enabled	既定の設定を使用します。
メール脅威対策	無効	–
有害 USB 攻撃ブロック	無効	–
トレースファイル	–	トレースファイルのディレクトリを、`/var/log/kaspersky` ディレクトリ以外のディレクトリに変更します。たとえば、`/var/log/kesl` ディレクトリを使用します。
グローバル除外リスト	設定済み	次のマウントポイントを除外します： • `/apt_spool` • `/storage` • `/var/lib/postgresql` • `/var/lib/clickhouse` • `/tmp` • `/tmp/*` /tmp および /tmp/* マウントポイントの除外は、バージョン 10.0 以前の NDR (KATA) サーバーに適用されます。 • `/varog/kaspersky` • `/var/opt/kaspersky` • `/data` • `/data/volumes/dumps`

Central Node コンポーネントが搭載されたサーバー上のKaspersky Endpoint Security for Linuxの設定

Central Node サーバーの推奨設定

本ソフトウェアの機能	推奨される機能の状態	推奨事項
ファイル脅威対策	Enabled	保護の除外を追加します： • [container-name:*edr_synchronizer*]/tmp/ • [container-name:*ids_alert_syncer*]/tmp/ • [container-name:kata_product_main_1_kata_scanner]/storage • [container-name:kata_product_main_1_postgresql_server]/var/lib/postgresql • [container-name:kata_product_main_1_clickhouse]/var/lib/clickhouse • [container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool • [container-name:*kata_scanner*]/var/opt/kaspersky/apt-agents • [container-name:*kata_scanner*]/var/lib/nginx/body • [container-name:*kata_scanner*]/apt_spool • [container-name:*kata_scanner*]/tmp/ • [container-name:*kafka*]/tmp/ • [container-name:*ksn_proxy*]/tmp/ • [container-name:*preprocessor_smtp*]/tmp/ • [container-name:*preprocessor_pop*]/tmp/ • [container-name:*preprocessor_icap*]/tmp/ • [container-name:*preprocessor_span*]/tmp/ • [container-name:*sandbox_scan*]/tmp/ • [container-name:*statistics_clickhouse_importer*]/tmp/ • [container-name:*updates_consistency_checker*]/tmp/ • [container-name:*web_backend*]/tmp/ • [container-name:*]/var/opt/kaspersky • /tmp/ • /var/log/kaspersky
マルウェアのスキャン	無効	–
リムーバブルドライブのスキャン	無効	–
ふるまい検知	Enabled	既定の設定を使用します。
ネットワーク脅威対策	無効	–
ウェブ脅威対策	無効	–
アンチクリプター	無効	–
コンテナスキャン	Enabled	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するには、コンテナ監視を有効にします `NamespaceMonitoring=Yes`
インベントリ	無効	–
デバイスコントロール	無効	–
アプリケーションコントロール	無効	–
ファイアウォール	無効	–
ウェブコントロール	無効	–
システム変更監視	無効	–
システム整合性チェック	無効	–
Endpoint Detection and Response Expert（オンプレミス）	無効	–

本ソフトウェアの機能	推奨される機能の状態	推奨事項
Endpoint Detection and Response Expert（クラウド）	無効	–
Managed Detection and Response	無効	–
Network Detection and Response (KATA)	無効	–
KUMA との連携	無効	–
Sandbox	無効	–
対応処理	無効	–
グラフィカルインターフェイス	未設定	–
ネットワークエージェント	インストール済み	既定の設定を使用します。
ファイル操作のインターセプト機構	fanotify に基づくシステムインターセプターメカニズム	既定の設定を使用します。
システムイベントテレメトリソース	eBPF+auditd	`TelemetrySource=Default`
脆弱性攻撃ブロック	無効	–
Kaspersky Security Network の使用	Enabled	既定の設定を使用します。
メール脅威対策	無効	–
有害 USB 攻撃ブロック	無効	–
トレースファイル	–	トレースファイルのディレクトリを、`/var/log/kaspersky` ディレクトリ以外のディレクトリに変更します。たとえば、`/var/log/kesl` ディレクトリを使用します。
グローバル除外リスト	設定済み	マウントポイントを除外リストに追加します： • `/apt_spool` • `/storage` • `/var/lib/postgresql` • `/var/lib/clickhouse` • `/tmp` • `/tmp/*` /tmp および /tmp/* マウントポイントの除外は、バージョン 10.0 以前の NDR (KATA) サーバーに適用されます。 • `/var/log/kaspersky` • `/var/opt/kaspersky` • `/data`

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Endpoint Security for Linux を Kaspersky Unified Monitoring and Analysis Platform と併用する場合は、この記事で説明する設定を使用することを推奨します。

本ソフトウェアの機能	推奨される機能の状態	推奨事項
ファイル脅威対策	Enabled	保護の除外を追加します： • `/opt/kaspersky/kuma` • `/opt/kaspersky/klnagent/sbin/klnagent` • `/opt/kaspersky/klnagent64/sbin/klnagent`
マルウェアのスキャン	無効	–
リムーバブルドライブのスキャン	無効	–
ふるまい検知	Enabled	プロセスをスキャンから除外します `/opt/kaspersky/kuma`
ネットワーク脅威対策	Enabled	侵害されたデバイスのブロックを無効にします `BlockAttackingHosts=No`
ウェブ脅威対策	無効	–
アンチクリプター	無効	–
コンテナスキャン	無効	–
インベントリ	無効	–
デバイスコントロール	無効	–
アプリケーションコントロール	無効	–
ファイアウォール	無効	–
ウェブコントロール	無効	–
システム変更監視	無効	–
システム整合性チェック	無効	–
Endpoint Detection and Response Expert（オンプレミス）	無効	–
Endpoint Detection and Response Expert（クラウド）	無効	–
Managed Detection and Response	無効	–
Network Detection and Response (KATA)	無効	–
KUMA との連携	無効	–
Sandbox	無効	–
対応処理	無効	–
グラフィカルインターフェイス	未設定	–
ネットワークエージェント	インストール済み	既定の設定を使用します。
ファイル操作のインターセプト機構	fanotify に基づくシステムインターセプターメカニズム	既定の設定を使用します。
システムイベントテレメトリソース	eBPF+auditd	`TelemetrySource=Default`
脆弱性攻撃ブロック	無効	–
Kaspersky Security Network の使用	Enabled	既定の設定を使用します。
メール脅威対策	無効	–
有害 USB 攻撃ブロック	無効	–

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、テクニカルサポートサイトにあるセクションの1つです。

ナレッジベースの Kaspersky Endpoint Security のページでは、本製品に関する便利な情報や推奨事項、購入、また本製品のインストールおよび使用に関連したよくある質問（FAQ）と回答に関する情報を参照できます。

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。ナレッジベースの記事に、テクニカルサポートからのニュースが掲載されることもあります。

カスペルスキー製品のフォーラム

特に緊急の対応が必要ではない場合は、カスペルスキー製品のフォーラムをご利用ください。ここでは、カスペルスキーのエキスパートやカスペルスキー製品のユーザーが、さまざまなトピックで意見交換しています。

このフォーラムでは、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。

License

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。

Light Agent

Kaspersky Endpoint Security for Virtualization Light Agent コンポーネント。保護する必要があるすべての仮想マシンにインストールします。

SIEM システム

セキュリティ情報およびイベント管理システム。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。

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

危険とみなされるコンテンツを含む Web アドレスのリスト。このリストは、カスペルスキーによって作成されます。このリストは定期的にアップデートされ、カスペルスキー製品の配信キットに含まれます。

アンチクリプター

ユーザーデータを含むファイルを暗号化することを目的としたランサムウェアの悪意のある処理。暗号化されたファイルは読み取ったり使用したりすることはできません。

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。

駆除

感染しているオブジェクトの処理方法の1つ。駆除の結果、データが完全に復元するかまたは部分的に復元します。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。

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

製品によって現在使用されているライセンス。

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。

製品設定

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）。

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。

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関連であると判断した Web アドレスのリスト。定義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信キットの一部となっています。

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。

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。

ライセンス証明書

カスペルスキーが、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合わせてユーザーに転送するドキュメント。ユーザーに許諾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ファイル legal_notices.txt 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。

AMD64 は Advanced Micro Devices, Inc. の商標または登録商標です。

Amazon は Amazon.com, Inc. またはその関連会社の商標です。

Mac および 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。

文字商標 Bluetooth およびそのロゴは 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。

XenServer は、米国およびその他の国における Cloud Software Group, Inc. またはその子会社の登録商標です。

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。

Grafana ワードマークおよび Grafana ロゴは、米国およびその他の国における Coding Instinct AB の登録商標/サービスマークまたは商標/サービスマークであり、Coding Instinct の許可を得て使用されています。当社は、Coding Instinct または Grafana コミュニティと提携、承認、または後援関係にはありません。

Docker および Docker ロゴはアメリカ合衆国およびその他の国における Docker, Inc. およびその子会社の商標または登録商標です。Docker, Inc.およびその他の関係者は、商標権や本文書で使用される用語の所有者である可能性があります。

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、Intel Corporation またはその子会社の商標です。

Linux はアメリカ合衆国およびその他の国における Linus Torvalds の登録商標です。

Microsoft、Active Directory、Hyper-V、Outlook、Visual C++、Windows は、Microsoft グループ企業の商標です。

OpenStack は、アメリカ合衆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。

Python は Python Software Foundation の商標または登録商標です。

Red Hat、Red Hat Enterprise Linux、CentOS、Fedora 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。

Kubernetes は、米国およびその他の国における The Linux Foundation の登録商標です。

Rocky Linux は、Rocky Enterprise Software Foundation の商標です。

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。

Zabbix は Zabbix SIA の登録商標です。