kaspersky

Kaspersky Endpoint Security for Linux 12.5.0

© 2026 AO Kaspersky Lab

目次

Kaspersky Endpoint Security for Linux
製品情報
主な機能
バージョン 12.5 の新機能
修正された問題
システム要件
製品の購入
他のアプリケーションとの互換性情報
カスペルスキーの各ソリューションにおける機能比較
導入と初期設定
モードと導入スキーム
本製品のインストール環境の準備
システムイベントのインターセプトメカニズムの選択
配布パッケージの準備
Kaspersky Security Center での準備作業
Kaspersky Security Center を使用した本製品のインストール
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インストール
特定のオペレーティングシステムでインストール後に行う追加の設定手順
高速インストールスクリプトを使用した Kaspersky Security Center Linux への移行シナリオ
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
アップグレード後の本製品の設定
本製品のアンインストール
本製品の使用
ライセンス管理
カスペルスキーの別のソリューションに切り替える方法
ライセンスの管理
ライセンスに関する情報の表示
本製品の管理インターフェイス
Kaspersky Security Center を使用した製品の管理
Kaspersky Security Center ポリシー
ポリシーの管理
ポリシー設定のエクスポートとインポート
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
コマンドラインを使用した本製品の管理
Kaspersky Endpoint Security のローカルタスク
タスクの設定の編集
タスクスケジュールの設定
本製品の全般設定の管理
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
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

保護ステータスの監視
リアルタイム保護のステータス
イベントとレポート
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
アプリケーションイベントの表示
レポートの表示
システムパフォーマンスメトリックの取得
アプリケーションの安定性監視
アプリケーションコンポーネントの変更チェック
本製品のアクセスコントロール
事前定義されたロール
ユーザーロールを割り当てる、または取り消す方法
Kaspersky Security Center の RBAC 機能領域
保護対象デバイスの一般的なロールに関する推奨事項
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
アップデート元と配信方式の選択方法
定義データベースのアップデートタスクを設定する方法
Kaspersky Update Utility を使用してアップデートする方法
定義データベースと製品モジュールのアップデートをロールバックする方法
ホスト脅威対策
ファイル脅威対策
保護範囲の作成方法
ファイル脅威の検知時の処理を選択する方法
ファイルスキャンのスマートモードとは
ファイルスキャンを最適化する方法
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
スキャン範囲を作成する方法
スキャンスケジュールを設定する方法
個々のファイルまたはディレクトリをスキャンする方法
オブジェクトスキャンタスクを最適化する方法
簡易スキャン
コンテナスキャン
コンテナ管理ツールとの統合を設定する方法
コンテナとイメージのオンデマンドスキャン範囲の作成方法
コンテナスキャンを最適化する方法
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する方法
コンテナとイメージのオブジェクトスキャンを実行する方法
リムーバブルドライブのスキャン
ふるまい検知
脆弱性攻撃ブロック
アンチクリプター
悪意のある暗号化の検知時に実行する処理の選択方法
保護範囲の作成方法

有害 USB 攻撃ブロック
USB デバイスの認証を設定する方法
オンスクリーンキーボードを使用した USB デバイスの接続を許可する方法
バーコードスキャナーを使用した USB デバイスの接続を許可する方法
通信と危険サイト対策
メール脅威対策
メール脅威が検知された場合の対処法
メール添付ファイルのスキャンを最適化する方法
メール添付ファイルフィルターの用途
ウェブ脅威対策
Web 脅威の検知時に実行する処理を選択する方法
フィッシング対策とは
ネットワーク脅威対策
ネットワーク脅威の検知時に実行する処理を選択する方法
ブロックされたデバイスを管理する方法
ファイアウォール管理
ネットワークパケットルールを作成する方法
ネットワークパケットルールの使用例
ネットワークゾーン（パブリック、ローカル、信頼済み）に IP アドレスを追加する方法
動的ルールとは
Kaspersky Security Center に接続するためのルールを作成する方法
セキュリティコントロール
デバイスコントロール
コマンドラインで信頼するデバイスのリストを管理する方法
デバイスのアクセスモードを設定する方法
デバイスアクセスルールを設定する方法
デバイスコントロールメッセージテンプレートを設定する方法
デバイスへの一時的なアクセスの許可
ウェブコントロール
Web リソースへのアクセスルールを作成する方法
ウェブコントロールのメッセージテンプレートを変更する方法
Web リソースアドレスマスクを作成するためのルール
アプリケーションコントロール
アプリケーションインベントリ
アプリケーションコントロールの動作モードを設定する方法
アプリケーションカテゴリの作成
ゴールデンイメージ
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
システム変更監視
リアルタイムのシステム整合性監視
システム整合性チェック
信頼ゾーン
保護の除外を追加する方法
信頼する URL を追加する方法
コンピューターの信頼する IP アドレスを追加する方法
監視するネットワークポートを選択する方法

- 信頼するルート証明書のリストに証明書を追加する方法
- 信頼するドメインを追加する方法
- マウントポイントを除外する方法
- 信頼するアプリケーションを追加する方法
- 信頼するデバイスを追加する方法

全般設定

- 検知の設定
- Kaspersky Security Network
  - Kaspersky Security Network を有効または無効にする方法
  - アプリケーションのクラウドモードとは
  - KSN プロキシの目的とは
- Kaspersky Security Center ストレージへのデータ転送の設定
- アプリケーション起動の設定方法
- タスク管理の許可設定
- パスワードによる保護
  - カスタム権限について
  - 既定のユーザー権限
- パフォーマンス設定
- ネットワークの設定
  - プロキシ設定の管理方法
  - 本製品がトラフィックをインターセプトする方法
  - 証明書検証ポリシーの設定方法
  - 監視対象ポートの設定方法
  - 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
- ファイル操作のインターセプト
- システムイベントインターセプターの設定
- テレメトリの詳細設定の管理
- バックアップ

高度な脅威と標的型攻撃からの保護

- 対応処理
  - 侵害の兆候の調査
  - 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
  - ファイルを隔離する
  - 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
  - プロセスの開始
  - プロセスの終了
  - オブジェクトの実行防止
  - 隔離の管理
- Endpoint Detection and Response Optimum
  - EDR Optimum 連携を有効にする方法
  - EDR Optimum 連携が稼働中であることを確認する方法
  - Cloud Sandbox

Endpoint Detection and Response Expert（オンプレミス）
EDR Expert（オンプレミス）と正しく統合するための参照イメージを準備する方法
EDR Expert（オンプレミス）との連携を設定する方法
EDR Expert（オンプレミス）との連携が稼働していることを確認する方法
Endpoint Detection and Response Expert（クラウド）
組み込みエージェントと EDR Expert（クラウド）の連携を設定する方法
EDR Expert（クラウド）のテレメトリ送信を最適化する方法
EDR Expert（クラウド）のテレメトリの除外を設定する方法
EDR Expert（クラウド）のイベントフィルターをエクスポートまたはインポートする方法
Kaspersky Anti Targeted Attack Platform
EDR (KATA) との連携の設定方法
NDR (KATA) との連携の設定方法
KATA 連携が正常に動作していることを確認する方法
Sandbox
Sandbox との連携を設定する方法
Sandbox との連携が正常に動作していることを確認する方法
ファイルを Sandbox に手動で送信する方法
Kaspersky Managed Detection and Response
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
KPSN 設定情報ファイルのアップロード
MDR 連携を設定する方法
MDR 統合が有効になっていることを確認する方法
Kaspersky Unified Monitoring and Analysis Platform
KUMA 連携を設定する方法
KUMA 連携が正常に動作していることを確認する方法
仮想環境の保護
SVM 検出を設定する方法
Light Agent が SVM を選択する方法
Light Agent の接続を SVM 間で分散する方法
Light AgentとSVM間の接続の保護
Light Agent のステータスを確認する方法
ベストプラクティス
製品によるリソース消費の最適化
デバイス上のアプリケーションパフォーマンスの分析
ファイル脅威対策とスキャンするタスクに関する推奨事項
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
ふるまい検知に関する推奨事項
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
アプリケーションコンポーネントのリファレンス
Kaspersky Endpoint Security を管理するコマンド
ライセンスを管理するコマンド
ユーザーとロールを管理するためのコマンド

アプリケーションのタスクと設定の管理
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
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
ステータスと保護の監視
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
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
セキュリティコントロール
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
ネットワーク接続の保護
ブロックされたデバイスの管理に使用されるコマンド
ファイアウォールを管理するコマンド
高度な脅威と標的型攻撃からの保護
隔離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
EDR Expert（クラウド）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
Light Agent モードでの製品コマンド
アプリケーションのコマンドラインオプション
アップデートタスク
ホスト脅威対策
ファイル脅威対策タスク
ネットワークディレクトリのスキャンの最適化
マルウェアのスキャン
マルウェアのスキャンタスク
オブジェクトスキャン タスク
簡易スキャンタスク
リムーバブルドライブスキャンタスク
コンテナスキャン
コンテナスキャン設定
コンテナのスキャンタスク
Jenkins との連携
アンチクリプタータスク
ふるまい検知タスク
脆弱性攻撃ブロック

Kaspersky Security Network の使用
Kaspersky Security Network への接続
クラウドモードの有効化または無効化
有害 USB 攻撃ブロックタスク
通信と危険サイト対策
ウェブ脅威対策タスク
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
ネットワーク脅威対策タスク
ファイアウォール管理
ネットワークパケットルールのリストの設定
ネットワークゾーンの設定
セキュリティコントロール
デバイスコントロールタスク
ウェブコントロール
ウェブコントロールタスク
ウェブコントロール設定の表示と編集
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タスク
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
インベントリの設定
インベントリタスク
検知されたアプリケーションのリストの表示
システム変更監視タスク
システム変更チェックタスク
高度な脅威と標的型攻撃からの保護
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）との連携設定
OSMP EDR Expert（オンプレミス）サーバーに接続するための証明書の管理
Kaspersky Endpoint Detection and Response Expert（クラウド）との連携
カスペルスキー Endpoint Detection and Response Expert（クラウド）連携設定
OSMP EDR Expert サーバー（クラウド）の接続証明書の管理
Kaspersky Endpoint Detection and Response（KATA）統合
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
Kaspersky Endpoint Detection and Response (KATA) 連携
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
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 連携の有効化または無効化

Kaspersky Managed Detection and Response 連携の設定
デバイスのネットワーク分離の管理
隔離設定の管理
コマンドラインでの隔離されたファイルの管理
侵害の兆候の調査
実行防止の管理
KUMA 連携の設定
Kaspersky Unified Monitoring and Analysis Platform との連携タスク
KUMA サーバーに接続するための証明書の管理
全般設定
全般的な製品設定
タスクスケジュール
プロキシサーバーの設定
バックアップ設定の構成
ネットワークトラフィックのスキャン設定
グローバル除外の設定
パスワードによる保護の設定
管理コンソールでのアプリケーション設定
定義データベースのアップデート
ホスト脅威対策
ファイル脅威対策
［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
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
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
コンテナの監視
［コンテナスキャン設定］ウィンドウ
コンテナスキャン
［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
リムーバブルドライブのスキャン
ふるまい検知
［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
脆弱性攻撃ブロック
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
アンチクリプター
［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
Kaspersky Security Network
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
有害 USB 攻撃ブロック
通信と危険サイト対策
メール脅威対策
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
ウェブ脅威対策
［信頼する URL］ウィンドウ
［スキャンの設定］ウィンドウ
ネットワーク脅威対策
［除外］ウィンドウ

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
セキュリティコントロール
デバイスコントロール
［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
ウェブコントロール
［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
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］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
インベントリ
［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
システム変更監視
［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

システム整合性チェック
［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
［マスクによる除外］ウィンドウ
ローカルタスク
タスクの管理
高度な脅威と標的型攻撃からの保護
Kaspersky Managed Detection and Response との連携
Kaspersky Endpoint Detection and Response（オンプレミス）との連携
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
Kaspersky Endpoint Detection and Response (KATA) 連携
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
KUMA との連携
［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
隔離
オブジェクトの実行防止
全般設定
プロキシサーバー
プロキシサーバーの除外ウィンドウ
スキャンタスクによる CPU 使用率
バッテリー電源でのタスクの実行
アプリケーションの起動
重要なアップデートを受信したときに自動的に再起動
パスワードによる保護
トレースおよびダンプの設定
アプリケーションが使用する常駐メモリ
暗号化された接続のスキャン
［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
グローバル除外リスト
マウントポイントのパス
プロセスメモリのスキャンからの除外
バックアップ

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
ファイル操作のインターセプト
Kaspersky Security Center 保管領域への情報の送信
システムイベントインターセプター
テレメトリの詳細設定
Light Agent モード
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
既知の問題と制限事項
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
トレースファイルの作成を有効にして設定する方法
ダンプを有効にして設定する方法
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：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
初期設定ファイル
インストールパッケージでの初期設定
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)
KATANDR タスク（ID:31）の既定
補足資料 2：Kaspersky Anti-Virus for Linux Mail Server との対話の設定
補足資料 3：外部サービスとの対話設定
補足資料 4：リムーバブルドライブの簡易スキャンのファイル拡張子
補足資料 5：メッセージテンプレートの変数
補足資料 6：アプリケーションイベント
緊急
警告
情報メッセージ
補足資料 7：リターンコード
補足資料 8：製品データベースを含むアーカイブの準備
補足資料 9：IOC ファイルの要件
法律上の通知
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）コンポーネントとの連携時に提供されるデータ
Kaspersky Endpoint Detection and Response Expert（クラウド）コンポーネントとの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
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 for Linux

参照

Kaspersky Endpoint Security for Linux
バージョン 12.5 の新機能
一般的な導入方式
機能の比較
既知の問題と制限事項

クイックスタート

システム要件
互換性
配布パッケージの準備
インストール環境の準備
アプリケーションの導入
Kaspersky Security Center Linux への移行シナリオ

本製品の使用

アクティベーション
定義データベースのアップデート
Kaspersky Update Utility を使用したアップデート
ファイル脅威対策
信頼ゾーン
リソースの最適化

コマンドラインでの設定

コマンドラインを使用した本製品の管理
管理コマンド
アプリケーションのコマンドラインオプション

サポート

保護ステータスの監視
旧バージョンの製品のアップグレード
テクニカルサポートへの問い合わせ

製品情報

Kaspersky Endpoint Security for Linux は、Linux デバイスに高度で包括的な保護を提供し、さまざまな種類の脅威、ネットワーク攻撃、詐欺行為を防止、検知、対応できるようにします。本製品は、多くのカスペルスキーのマルチプラットフォームソリューションに含まれており、組織の IT インフラストラクチャの課題に合わせて柔軟に設定できます。

保護対象デバイスにインストールされている Kaspersky Endpoint Security は、ローカルで管理することも、Kaspersky Security Center を使用して一元管理することもできます。

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。

主な機能

大規模なサイバー脅威からの保護

高度なテクノロジーに基づく保護は、IT セキュリティの基盤です。Kaspersky Endpoint Security は、ユーザーデバイスのファイルシステムが感染するのを防ぎ、デバイスへのリムーバブルドライブの接続を監視して、リムーバブルドライブのウイルススキャンを実行します。アプリケーションの悪意のある活動を監視し、悪意のあるリモート暗号化からファイルを保護します。ウイルス、トロイの木馬、暗号化プログラム、ハッカー攻撃など、新たな世界的脅威に関する情報を含むデータベースは、定期的に自動でアップデートされます。

通信と危険サイト対策

Kaspersky Endpoint Security は、組織のネットワーク環境を確実に保護します。メール、Web サイト、ダウンロードしたファイルを、開く前にウイルス、ネットワークワーム、その他の脅威がないかスキャンします。このアプリケーションでは、ネットワーク攻撃を示す可能性のある活動について受信ネットワークトラフィックをスキャンし、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、ネットワーク活動をフィルタリングできます。

職場のセキュリティコントロール

Kaspersky Endpoint Security を使用して職場でのアプリケーション、Web リソース、接続デバイスへのユーザーアクセスを制御することで、組織にさらなるセキュリティ層を提供できます。これにより、デバイスを感染から保護し、データの損失や漏洩を防ぐことができます。

高度な脅威や標的型攻撃からの保護

このアプリケーションは、カスペルスキーの Detection and Response ソリューション、具体的には Kaspersky Managed Detection and Response（MDR）および Kaspersky Anti Targeted Attack Platform（KATA）と連携できます。カスペルスキーの SIEM ソリューションである Kaspersky Unified Monitoring and Analysis Platform（KUMA）もサポートされています。Kaspersky Endpoint Security は、ユーザーデバイスで実行中のプロセス、開いているネットワーク接続、および変更中のファイルを監視します。Detection and Response ソリューションとの連携により、エクスプロイト、ランサムウェア、ファイルレス攻撃、ハッカーがデバイスやデータを侵害するために使用する可能性がある正規のシステムツールなどの脅威から保護されます。

仮想環境およびクラウド環境の保護

Kaspersky Endpoint Security は、Kaspersky Security for Virtualization Light Agent ソリューションの一部として、さまざまなサーバー仮想化プラットフォームおよび VDI プラットフォーム上で Linux ゲストオペレーティングシステムが動作する仮想マシンを保護します。オブジェクトのウイルススキャンは、別の仮想マシンにインストールされた特別なコンポーネントである SVM（Secure Virtual Machine）によって実行されます。そのため、このアプリケーションは仮想マシンのリソースではなく SVM のリソースを使用してセキュリティを提供し、スマートな最適化（たとえば、共有キャッシュの使用）と組み合わせることで、IT インフラストラクチャ全体の負荷を最小限に抑えます。

バージョン 12.5 の新機能

Kaspersky Endpoint Security 12.5 for Linux には、次の機能と改良点が導入されています：

- Elbrus CPU を搭載したデバイスへの Kaspersky Endpoint Security 12.5 for Linux のインストールのサポート。本製品では、Elbrus CPU に対して限定的なサポートを提供します。

- Kaspersky Endpoint Detection and Response Expert（クラウド）との連携が実装されました。このクラウドソリューションは、企業資産にインストールされた EPP アプリケーションでは検知できない脅威を含む高度なサイバー脅威から、組織の IT インフラストラクチャを保護するように設計されています。このソリューションは、エンドポイント資産、ネットワークデータ、クラウド環境データなど、幅広い対応ツールとデータソースを活用することで、包括的な可視性、相関分析、自動化を実現します。また、統合されたコンポーネントとエンドツーエンドのワークフローを単一のインターフェイス内で提供することで、統一された検知と対応プロセスを実現し、セキュリティ専門家の効率性を向上させます。

  Kaspersky Endpoint Security for Linux と Kaspersky Endpoint Detection and Response Expert（クラウド）ソリューションとの連携は、本ソリューションが提供開始されるまで一時的に利用できません。本ソリューションの提供開始は 2026 年後半を予定しています。その後、追加のアップグレードを行うことなく、このバージョンの Kaspersky Endpoint Security で連携機能を利用できるようになる予定です。

- Kaspersky Endpoint Security アプリケーションにおける特定の操作のパスワードによる保護。パスワードによる保護を使用すると、付与された権限に応じて、ユーザーが Kaspersky Endpoint Security アプリケーションで実行できる操作を制限できます。アプリケーション設定へのアクセスを制限することで、アプリケーションに対する不正な変更や意図しない変更のリスクを軽減できます。

- デバイスコントロールが改善されました。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、ファイルからインポートできるようになりました。

- 有害 USB 攻撃ブロックコンポーネントの改善。バーコードスキャナーを接続する際に、デバイスのロックを解除するための認証コードを入力する代わりに、画面上のバーコードをスキャンしてスキャナーを認証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（ULKM）の強化：

  - セキュアブートが有効なシステムで、更新可能なカーネルモジュール（ULKM）に基づくシステムイベントのインターセプトがサポートされるようになりました。

  - アプリケーションで、更新可能なカーネルモジュールを使用してイベントをインターセプトできるオペレーティングシステムのサポートが拡張されました。

  - アンチクリプターおよびデバイスコントロールコンポーネント向けに、更新可能なカーネルモジュールのサポートを追加しました。

- Astra Linux Special Edition の閉鎖型ソフトウェア環境モードでのインストールプロセスを改善しました。互換性パックがインストールされている場合、Astra Linux Special Edition オペレーティングシステムを搭載したデバイスに Kaspersky Endpoint Security アプリケーションをインストールした後で、アプリケーションを起動するための追加操作をユーザーが手動で実行する必要がなくなりました。

- アプリケーションのインストール時に、autoinstall.ini 設定情報ファイルを使用して kesl.ini 設定情報ファイルの設定を変更できるようになりました。

- アプリケーションのインストールおよびアンインストール時のエラー診断が改善されました：

  - リターンコードがより詳細になり、潜在的な問題をより明確に把握できるようになりました。

  - アプリケーションのインストールと正常な動作に必要な依存関係（外部ライブラリ、コンポーネント、ユーティリティ、その他のプログラム）の不足に関する新しいメッセージを追加しました。

  - システムディレクトリのアクセス権限が正しく設定されていないことに関する新しいメッセージを追加しました。

  - Kaspersky Security Center に、新しいエラーメッセージと内容が明確化されたエラーメッセージが表示されるようになりました。

  - アプリケーションのインストール中にパッケージマネージャーのエラーを無視できるようになりました。

- アプリケーションは、アプリケーションのデータベースとモジュールの初回アップデート後、インストール中に自動的に再起動するようになりました。アプリケーションのインストール後、最初の 24 時間が経過した後に、重要なアップデートを受信したときにアプリケーションが自動的に再起動するよう設定できるようになりました。アプリケーションの自動再起動は、コマンドラインでアプリケーションの全般設定から、または Web コンソールや管理コンソールを使用してポリシーのプロパティで設定できます。

- Detection and Response ソリューションと連携する場合、kesl.ini 設定情報ファイルの `UseIncreasedXdrEventsCache` 設定を使用してイベントキャッシュを管理できるようになりました。高パフォーマンスと RAM 使用量の間にはトレードオフがあります。

- アプリケーションの停止または再起動時に、kesl.ini 設定情報ファイルの `FastShutdown` 設定を使用して kesl プロセスを高速シャットダウンできるようになりました。これにより、高負荷システムでのアプリケーションのダウンタイムを最小限に抑え、過剰なリソース消費を防止できます。

- イベントキューを処理するふるまい分析コンポーネントのメモリ使用量を、kesl.ini 設定情報ファイルの `ReduceSWMemoryConsumption` 設定を使用して制限できるようになりました。この設定を使用すると、保護レベルに影響が出る可能性があります。必ずドキュメントを確認してください。

- ネットワークアクセスの安定性を向上させました。kesl プロセスが異常終了した場合、Watchdog サーバーは、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の起動時にアプリケーションが追加する Firewall ルールを削除するようになりました。これにより、インターネット接続が失われることを回避し、デバイスのネットワークアクセスを迅速に復元できます。

- 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、複数のスキャンタスクが同時に実行されるのを防止することができるようになりました。このオプションを有効にすると、複数のスキャンタスクが同時に起動された場合、それらはキューに格納されます。

- ファイル脅威対策の除外で、シンボリックリンクを処理できるようになりました。パスが最終的なファイルアドレスに変換されるようになりました。

- アプリケーションを再起動せずに、アプリケーションの全般設定を管理するコマンドを使用して、ダンプファイルディレクトリを有効にして設定できるようになりました。これらのダンプファイル設定は、kesl.ini 設定情報ファイルから削除されました。

- Kaspersky Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Anti Targeted Attack Platform、Kaspersky Unified Monitoring and Analysis Platform ソリューションと連携する場合、パスワードが必須になりました。連携を設定する際に、クライアント証明書のパスワードを指定する必要があります。

- アプリケーションは、Kaspersky Unified Monitoring and Analysis Platform との連携の一環としてテレメトリイベントを送信する際にトラフィックを圧縮できるようになり、帯域幅の節約に役立ちます。

- CentOS 5.2、5.4、6.4、6.6 の 64 ビット版のサポートを含め、サポート対象オペレーティングシステムの一覧を更新しました。

- アプリケーションのインターフェイスが、新たにスペイン語（メキシコ）とポルトガル語（ブラジル）で利用できるようになりました。

旧バージョンの変更点

バージョン 12.4

Kaspersky Embedded Systems Security 12.4 for Linux では、次の新機能と改良点が導入されました：

- 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（オンプレミス） 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）との連携も提供します。連携タスクの名称が *Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携*（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、脅威が拡散する主なシナリオを網羅でき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。Kaspersky Endpoint Detection and Response Expert（オンプレミス）のコンポーネントは、Open Single Management Platform (OSMP) 上に導入されます。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）との連携および Kaspersky Endpoint Detection and Response (KATA) との連携を提供する EDR Expert（オンプレミス）コンポーネントをアクティベートできます。

  - 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）との連携*タスクの設定にある連携モードを選択できます。

- 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構造が見直され、必要な機能をより早く見つけられ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、名前空間で見つかったマウントポイント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

- サポート対象のオペレーティングシステムのリストを更新しました。

バージョン 12.3

Kaspersky Embedded Systems Security 12.3 for Linux では、次の新機能と改良点が導入されました：

- 更新可能なカーネルモジュールに基づいてシステムイベントを傍受するメカニズムを追加しました（Light Agent モードでは利用できません）。デバイスのオペレーティングシステムが fanotify に対応し、更新可能なカーネルモジュールをインストールするためのその他の要件を満たしている場合は、本製品が更新可能なカーネルモジュールを使用するように設定できます。更新可能なカーネルモジュールを使用すると、Kaspersky Endpoint Security による起動されたプロセスのインターセプトを最適化できます。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。

- 更新可能なカーネルモジュールにより、アンチクリプターコンポーネントの機能が向上します（Light Agent モードでは利用できません）。本製品は、より多くの種類のランサムウェアを検知できるようになりました。

- 新しい機能コンポーネント「脆弱性攻撃ブロック」を追加しました（Light Agent モードでは利用できません）。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。

- デバイスコントロールコンポーネントが改善されました。

  - 追加されたデバイスが信頼済みと見なされるユーザーまたはユーザーグループのリストを設定する機能を追加しました。

  - ストレージデバイスへの読み取り専用アクセスを許可する機能を追加しました。

  - また、イベントを通じたユーザー通知を改善し、新しいイベントを追加したほか、プラグインおよびコマンドラインでのイベントテキストを明確化および体系化しました。

- Kaspersky Managed Detection and Response ソリューションとの連携を拡張：
  - これで、デバイスをネットワークから分離できます。
  - ファイルを隔離したり、隔離からファイルを復元したりできます。
  - プロセスを開始または終了できます。
- ライセンスを追加することで、Kaspersky Managed Detection and Response との連携を提供する MDR コンポーネントをアクティベートする機能を追加しました。
- ふるまい検知が改善されました。MDR および EDR (KATA) によるスキャンから処理の除外を有効または無効にできるようになりました。
- プロキシサーバーの除外リストを設定できるようになりました。プロキシサーバーをバイパスする必要がある Kaspersky Endpoint Security を指定したり、プロキシサーバーを使用しないアドレスのリストを作成したりすることもできます。Kaspersky Endpoint Security を仮想環境保護用 Light Agent モードで使用する場合、Kaspersky Security Network、SVM、および Integration Server との接続にプロキシサーバーを使用することはサポートされません。
- トラフィック傍受の除外リストを設定できるようになりました。本製品の管理プラグインまたはコマンドラインを使用して、本製品がトラフィックのインターセプトから除外する接続を指定できるようになりました。
- ファイル脅威対策スキャンを最適化するために、定義データベースログファイルを一時的にスキャンから除外できるようになりました。最後のスキャンから 10 分以内に同じ処理によって定義データベースログファイルが再利用された場合、本製品はそのログファイルのスキャンをスキップします。
- 親ポリシーの設定を継承するときに、親ポリシーとその子ポリシーの除外リスト項目のマージを有効にできるようになりました。
- 管理 Web プラグインを使用して、ポリシーとタスクの除外リストをエクスポートおよびインポートできるようになりました。
- 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で、Kaspersky Security Center 管理コンソールに Kaspersky Endpoint Security の初期設定を構成する機能を追加しました。
- バッテリー電源で動作しているデバイスで、予定されたタスクのキャンセルを設定できるようになりました。
- Kaspersky Endpoint Security が KSN サーバーと対話するときに、KSN プロキシサーバーの使用を有効または無効にする機能を追加しました（Light Agent モードでは利用できません）。KSN プロキシサーバーの使用が有効になっている場合、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。KSN プロキシサーバーの使用が無効になっている場合、Kaspersky Endpoint Security は KSN サーバーと直接対話します。
- コマンドラインでは、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するコマンドを使用できます。
- デバイスで有効なポリシーとポリシープロファイルに関する情報をコマンドラインとグラフィカルインターフェイスに表示する機能を追加しました。
- Perl がインストールされていないデバイスにも本製品をコマンドラインを使用してインストールできるようになりました。

- トラフィックのインターセプトを改善しました。ローカルトラフィック（同じデバイス上のプロセス間のトラフィック）は読み取られなくなりました。

- Kaspersky Managed Detection and Response と連携する場合、KPSN 設定情報ファイルを使用せずにテレメトリを送信するために必要な設定を渡すことができるようになりました。Kaspersky Security Network インフラストラクチャソリューションを使用している場合、または唯一のテナントが root テナントである場合は、Kaspersky Managed Detection and Response との連携に KPSN 設定情報ファイルは必要ありません。

- 製品イベントログ内の大量のイベントのストレージを最適化しました。イベントデータベースを開く操作と閉じる操作、およびイベントを取得する操作が、より高速になりました。

- アプリケーションのグラフィカルインターフェイスを改善しました（アプリケーションを Light Agent モードで使用する場合、グラフィカルインターフェイスはサポートされません）：

  - ウェブコントロールコンポーネントを有効または無効にできるようになりました。

  - グラフィカルインターフェイスのスタイルを刷新しました（新しい配色、すべてのウィンドウの角の丸み）。

- ファイル脅威対策設定およびスキャンタスクの、感染したオブジェクトに適用できる処理の名前を変更しました。

- 64 ビットオペレーティングシステム（eBPF 対応のカーネルバージョン 5.3 以降）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が追加されました。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。オペレーティングシステムが要件を満たしている場合、本製品は Light Agent モードでも eBPF を自動的に使用します。

- すべてのアプリケーション管理インターフェイス（コマンドラインインターフェイス以外）の日時は、RFC 3339 に準拠した統一された形式で表示されます（例：2023-12-25 23:55:59）。

- サポート対象のオペレーティングシステムのリストを更新しました。

バージョン 12.2

Kaspersky Embedded Systems Security 12.2 for Linux では、次の新機能と改良点が導入されました：

- 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) との連携に対応しています。これにより、社内ネットワークが保護され、デバイスで発生するイベントに関する情報（テレメトリ）を、Central Node コンポーネントを備えた Kaspersky Anti Targeted Attack Platform サーバー（以下、NDR サーバーとも表記）に送信できます。

- Kaspersky Anti Targeted Attack Platform ソリューションのコンポーネントである KATA Sandbox との連携に対応しています。これにより、オペレーティングシステムの仮想イメージが展開された特別なサーバーを使用して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や標的型攻撃の兆候を検知できます。

- 情報セキュリティイベントの受信、処理、保存、受信データの分析と相関、受信したイベントの検索、情報セキュリティ脅威の兆候の検知に関する通知の作成などの機能を組み合わせた包括的なソフトウェア Kaspersky Unified Monitoring and Analysis Platform and Analysis Platform との連携に対応しています。

- Kaspersky Endpoint Detection and Response (KATA) との連携における延長機能で、Kaspersky Anti Targeted Attack Platform ソリューションのコンポーネントです：
  - 新しいオブジェクト実行防止機能。
  - 新しいファイル隔離機能。
  - デバイス上のイベントに関する詳細情報（テレメトリ）。
- Endpoint Detection and Response Optimum 連携の延長機能：
  - 新しいオブジェクト実行防止機能。
  - 新しいファイル隔離機能。
  - プロセス名によってプロセスをネットワーク分離から除外できます。
- デバイス上の複雑な脅威を検知できる Cloud Sandbox テクノロジーを使用できます。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。
- 最も頻繁にスキャンされたファイルとアプリケーションに関する統計情報および保護対象デバイスで検出されたマウントポイントのリストを表示できます。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出されたマウントポイントを除外できるようになりました。
- Kaspersky Endpoint Security がオペレーティングシステムのパフォーマンスに与える影響を分析するのに役立つアプリケーションパフォーマンスメトリックを収集できます。
- ファイアウォール管理コンポーネントが改善されました。ネットワークパケットルールに複数の IP アドレスまたは IP アドレス範囲を指定できます。
- オペレーティングシステムのフリーズを追跡するための新しいメカニズム。このメカニズムは、execve 関数などの一部のシステム機能のフリーズをチェックします。3 秒ごとに、wdserver ウォッチドッグサーバープロセスは別の wdserver プロセスを開始し、そこでこれらのシステム関数を呼び出します（execve 関数の呼び出しは、少なくともう 1 つの wdserver プロセスを開始します）。wdserver が応答しないシステム関数を検知すると、ウォッチドッグサーバーの過負荷により kesl プロセスが再起動されます。
- 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管理するときに、ポップアップ通知の表示を構成できます。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、GUI でのポップアップ通知の表示を有効または無効にできるようになりました。
- タスクスケジュールのコマンドラインオプションが改善されました。タスクが許容される最大実行時間に達したときに停止するよう設定できるようになりました。
- Kaspersky Security Center ポリシープロファイルを作成するときの「パッドロック」属性のステータスを変更しました。プロファイルを作成すると、すべての「パッドロック」が既定で開きます。つまり、既定では、プロファイル設定は「ベース」ポリシーの設定を上書きしません。
- 64 ビットオペレーティングシステム（BTF に対応する eBPF を備えたカーネルバージョン 5.3 以降）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が追加されました。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。オペレーティングシステムが指定された要件を満たしている場合、本製品は自動的に eBPF で動作します。

- すべての管理プラグインの日時は、RFC 3339 に準拠した統一された形式で表示されます（例：2023-12-25 23:55:59）。

- サポート対象のオペレーティングシステムのリストを更新しました。

バージョン 12.1

Kaspersky Embedded Systems Security 12.1 for Linux では、次の新機能と改良点が導入されました：

- Kaspersky Endpoint Detection and Response Optimum との連携を設定できるようになりました。これにより、エクスプロイト、ランサムウェア、ファイルレス攻撃、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が保護されます。

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

- Web リソースへのユーザーアクセスを制御する新しい *ウェブコントロール*コンポーネントが追加されました。これにより、トラフィック消費量を削減し、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。

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

- Kaspersky Security Center Web コンソールを使用して Kaspersky Endpoint Security をインストールする手順を改善しました：アプリケーションのインストールパッケージのプロパティで、以前は autoinstall.ini 設定情報ファイルでのみ使用可能だった初期設定を指定できるようになりました。

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

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

- Kaspersky Symphony XDR との連携を設定できるようになりました。Kaspersky Endpoint Security が標準モードで使用されている場合、本製品は「マルウェアのスキャンを開始」と「定義データベースのアップデート」の対応処理を実行できます。

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

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

- サポート対象のオペレーティングシステムのリストを更新しました。

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。

バージョン 12.5 の修正済み問題一覧

識別子	説明
10306343	現在のライセンスのステータスを確認する際に、ライセンスの削除およびインストールに関する通知が誤って生成されていました。
10295949	デバイスコントロールコンポーネントの現在のポリシープロファイルで指定された設定が適用されませんでした。その結果、コンポーネントはポリシーで指定された設定で動作し続けました。
10171454	設定で指定された最初のアップデート元が使用できない場合、アップデートの問題に関するメッセージが誤って表示されていました。
10109293	iptables ネットワークトラフィック傍受モードが選択されている場合（`NetInterceptorMode=UseIPTables`）、特定のネットワークインターフェイスにバインドされたネットワークソケットを開くアプリケーションからのトラフィックが正しく処理されませんでした。
10024219	Kaspersky Security Center 管理コンソールでは、管理対象デバイス上の更新可能なカーネルモジュールのステータスが正しく表示されませんでした。
9995631	アプリケーションによる常駐 RAM 使用量の制限（`MaxMemory` 設定）が、スワップパーティションのないシステムで正しく機能しませんでした。現在は、設定された制限に達すると、Kaspersky Endpoint Security が再起動します。
9937329	*デバイスが接続されました* および *デバイスの接続が切断されました* は、デバイスコントロール（Device_Control）タスクが無効になっているシステムで誤って生成されていました。
9934846	高負荷のシステムでは、アプリケーションが起動しませんでした。アプリケーションから Watchdog サーバーへの接続のタイムアウト時間が延長されました。
9846405	*オブジェクトが処理されていません* イベントは、EFI ブートローダーが設定されているシステムで誤って生成されていました。
9815051	管理対象デバイスで eBPF ネットワークトラフィック傍受モード（`NetInterceptorMode=UseEBPF`）でウェブ脅威対策（Web_Threat_Protection）タスクおよびネットワーク脅威対策（Network_Threat_Protection）タスクを実行している場合、すでに確立されていたネットワーク接続がハングアップすることがありました。このような接続は、データ送信が試行された時点で終了されるようになりました。
9807202	一部の ROSA オペレーティングシステムでは、mkfs.ext2 ユーティリティを使用するとインストール時に問題が発生しました。
9704644	アプリケーションを EDR エージェントモードで使用している場合、デバイスのステータスが正しく表示されませんでした。アプリケーションを EDR エージェントモードで使用している場合のデバイス保護ステータスの値が変更されました。
9643969	eBPF モードでネットワークトラフィックインターセプトを使用している場合、Scylla ホスト間のネットワーク接続に問題が発生することがあります。
9633030	ポリシーで **オブジェクトの実行防止を有効にする** チェックボックスがオフになっている場合に、オブジェクトの実行防止（EDR Expert（オンプレミス））タスクが実行されていました。
9627894	IPv6 が無効になっているオペレーティングシステムで、eBPF テクノロジーに基づくネットワークトラフィック傍受モードが正しく機能しませんでした。
9606448	Kaspersky Security Center 管理サーバーを、カスペルスキーの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してアプリケーションをアクティベートする際に問題が発生しました（ポリシーで **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** チェックボックスがオンになっている場合）。
9508605	Kaspersky Endpoint Detection and Response Expert との連携が有効になっている場合、コンテナ環境を備えたシステムでアプリケーションが大量のメモリを使用していました。
9456741	新しいプロセスの開始を傍受する際にファイルインタープリターを特定できなかったため、アプリケーションがクラッシュしました。

Web プラグインのバージョン 6.1 で修正された問題の一覧

識別子	説明
9558745	Kaspersky Endpoint Security のグラフィカルインターフェイスでの通知の表示を設定するための **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** 設定が、ポリシーのプロパティ（**アプリケーション設定** → **全般設定** → **イベントの設定** → **詳細設定**）に表示されませんでした。
9622658	オブジェクトハッシュによるマルウェアのスキャンからの除外を追加した場合、その除外は保存されませんでした。
9798821	ウェブコントロールルールに個別の Web サイトを追加した場合、ポリシーの変更が保存されませんでした。
9990129	信頼するアプリケーションを追加するフォームに、不要な **コメント** フィールドが表示されていました。
9977884	メール脅威対策コンポーネントの設定に、不要な **セキュリティレベル** トグルスイッチが表示されていました。
9944635	**メールデータベースをスキャン** フラグの名前が重複していました。現在は、次の正しい名前が表示されます：**メールデータベースをスキャン** および **メール形式のファイルをスキャン**。
10010439	ウェブコントロールルールの作成時に、Active Directory のリストからルールに割り当てたユーザーが正しく追加されませんでした。
10218308	ポリシー設定が変更された際に、Kaspersky Security Network のモードがリセットされました。

システム要件

ハードウェアの最小要件

製品をインストールする場合

- 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
- メモリ：
  - 64 ビットオペレーティングシステムの場合：製品が使用できる 2 GB の RAM
  - 32 ビットオペレーティングシステムの場合：製品が使用できる 1 GB の RAM
- 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ースをインストールする場合

- 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モニター。画面のスケーリングが適用されている場合、これらの寸法もスケーリングされます。

Arm アーキテクチャのハードウェア最小要件

製品をインストールする場合

- 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ースをインストールする場合

- 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モニター。画面のスケーリングが適用されている場合、これらの寸法もスケーリングされます。

Elbrus (E2K) アーキテクチャのハードウェア最小要件

製品をインストールする場合

- CPU v3：Elbrus-4S、v4：Elbrus-8S または Elbrus-1S+
- 2 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
- 2 GB 以上のハードディスク空き容量（インストール、一時ファイル、ログファイルの保存などに使用）

グラフィカルユーザーインターフェースをインストールする場合

- 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モニター。画面のスケーリングが適用されている場合、これらの寸法もスケーリングされます。

ソフトウェア要件

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

この記事では、本製品がテストを経て、正しく動作することが保証されているソフトウェアのバージョンを一覧表示します。本製品は他のソフトウェアのバージョンでも動作する可能性がありますが、それらの構成は完全なテストサイクルを経ておらず、サポート保証対象バージョンには含まれていません。

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、gfs2、gvfs、hugetlbfs、mqueue、nfsd、proc、parsecfs、pipefs、pstore、usbfs、rpc_pipefs、securityfs、selinuxfs、sysfs、tracefs。

FUSE 技術経由のマウントポイントに対するファイル脅威対策は、オペレーティングシステムの管理者が追加の手順を実行しない限り制限されます。user_allow_other 設定を /etc/fuse.conf ファイルに追加し、各マウントポイントに allow_root マウントオプションを追加することで、本製品がそれらのマウントポイントでのファイルイベントを監視できるようにすることができます。

64 ビットオペレーティングシステム	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	Elbrus (E2K) アーキテクチャの 64 ビットオペレーティングシステム	32 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（運用アップデート 1.5、1.6、1.7、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) 「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でのみ対応しています。 • CentOS 5.2、5.4、6.4、6.6、7.2、7.3、7.4、7.5、7.6、7.7、7.8、7.9。 Kaspersky Endpoint Security Cloud ソリューションでは、このアプリケーションは CentOS 5.2、5.4、6.4、6.6 デバイス上での実行をサポートしていません。 Kaspersky Security Center Cloud コンソールでは、このアプリケーションは CentOS 5.2、5.4、6.4、6.6 デバイス上での実行をサポートしていません。 • CentOS Stream 8、9、10。 • Debian GNU/Linux 12.8、12.9、12.10、12.11、12.12、12.13 • Debian GNU/Linux 13.1、13.2、13.3 • 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、8.10。 • 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、9.7。 • SberOS 3.4.0、3.5.0、3.6.1。 • SUSE Linux Enterprise Server 12.5、12.6、12.7 • SUSE Linux Enterprise Server 15.4、15.5、15.6、15.7 • Ubuntu® 24.04 LTS • Ubuntu 26.04 LTS • ALT 教育 10、11。 • ALT Workstation 11 • ALT Server 11 • ALT SP Workstation リリース 10	• 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 26.04 LTS • ALT Workstation 11.2 • ALT Server 11.1 • ALT SP Workstation リリース 10 • ALT SP Server リリース 10 • RED OS 8.0	• OS Elbrus 9.3.6。 • Astra Linux Special Edition RUSB.10015-16 (release 2) (operational update 8.1) • Astra Linux Special Edition RUSB.10265-01 (operational update 8.1) • ALT SP Workstation リリース 8、10。 • ALT SP Server リリース 8、10。	• Debian GNU/Linux 12.8、12.9、12.10、12.11、12.12、12.13

64 ビットオペレーティングシステム	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	Elbrus (E2K) アーキテクチャの 64 ビットオペレーティングシステム	32 ビットオペレーティングシステム
• 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 9.5 Workstation • MSVSphere 9.5 Server • MES OS 12 Panel リリース 2025 • MES OS 12 Desktop リリース 2025 • OSnova 3.1 • 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			

Light Agent モードの追加ソフトウェアおよびハードウェア要件

Kaspersky Endpoint Security は、Kaspersky Security for Virtualization Light Agent 6.5 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。

仮想マシン

Kaspersky Endpoint Security のソフトウェアおよびハードウェア要件は、Kaspersky Endpoint Security が Light Agent モードで動作している仮想マシンに対して、次の制限事項付きで適用されます：

- 100 Mbps の帯域幅を持つ仮想化ネットワークインターフェイスが必要です
- Arm デバイスでは、Light Agent モードの Kaspersky Endpoint Security はサポートされません。
- Light Agent モードの本製品は、強制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の Astra Linux Special Edition オペレーティングシステムではサポートされません。

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。

仮想インフラストラクチャに応じて、仮想マシンには次のもの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。
- VMware vSphere インフラストラクチャでは、VMware Tools パッケージ。
- XenServer インフラストラクチャでは、XenTools ソフトウェア。
- HUAWEI FusionSphere インフラストラクチャでは、HUAWEI Tools パッケージ。
- KVM（Kernel-based Virtual Machine）インフラストラクチャでは、QEMU Guest Agent。

サポート対象のターミナルサーバーの種類

- Astra Linux 3.0.5 ターミナルサーバー。

製品の購入

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

本製品のメインファイル

- 32ビットオペレーティングシステムを使用するプロセッサの場合：
  `kesl-12.5.0-<build number>.i386.rpm`
  `kesl_12.5.0-<build number>_i386.deb`
- 64ビットオペレーティングシステムを使用するプロセッサの場合：
  `kesl-12.5.0-<build number>.x86_64.rpm`
  `kesl_12.5.0-<build number>_amd64.deb`
- Arm®プロセッサ、64ビットオペレーティングシステムの場合：
  `kesl-12.5.0-<build number>.aarch64.rpm`
  `kesl_12.5.0-<build number>_arm64.deb`
- Elbrus CPUの場合：
  `kesl-12.5.0-<build number>.e2k.rpm`
  `kesl_12.5.0-<build number>_e2k.deb`

本製品のグラフィカルインターフェイス

- 32ビットオペレーティングシステムを使用するプロセッサの場合：
  `kesl-gui-12.5.0-<build number>.i386.rpm`
  `kesl-gui_12.5.0-<build number>_i386.deb`
- 64ビットオペレーティングシステムを使用するプロセッサの場合：
  `kesl-gui-12.5.0-<build number>.x86_64.rpm`
  `kesl-gui_12.5.0-<build number>_amd64.deb`
- Arm®プロセッサ、64ビットオペレーティングシステムの場合：
  `kesl-gui-12.5.0-<build number>.aarch64.rpm`
  `kesl-gui_12.5.0-<build number>_arm64.deb`
- Elbrus CPUの場合：
  `kesl-gui-12.5.0-<build number>.e2k.rpm`
  `kesl-gui_12.5.0-<build number>_e2k.deb`

サポートが制限されているオペレーティングシステム（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6）に Kaspersky Endpoint Security アプリケーションをインストールするには、OLDのマークが付いた配布パッケージを選択します。

Kaspersky Security Centerを使用した本製品のリモートインストール用アーカイブ

`kesl-12.5.0.<build number>.zip`

このアーカイブには、ユーザー契約書の本文も含まれています。

ユーザー契約書の本文

- `ksn_license.<language ID>`には、Kaspersky Security Networkに関する声明の本文が含まれています。
- `license.<language ID>`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。

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。

他のアプリケーションとの互換性情報

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

Kaspersky Endpoint Security のモードに応じて、表に記載されているバージョンの Kaspersky Security Center を使用して本製品を管理できます。

モード	Kaspersky Security Center のバージョン
標準モードの Kaspersky Endpoint Security	Kaspersky Security Center Windows 14.2、15.1。 MMC 管理プラグインを使用する管理コンソール、および Web 管理プラグインを使用する Kaspersky Security Center Web コンソールによる管理。 Kaspersky Security Center Linux 15.1、15.2、15.3、15.4、16.0、16.1、16.2、16.3。 Web 管理プラグインを使用する Kaspersky Security Center Web コンソールによる管理。
Endpoint Detection and Response Optimum コンポーネントを搭載した標準モードの Kaspersky Endpoint Security	Kaspersky Security Center Windows 15.1。 Kaspersky Security Center Linux 15.3、15.4、16.0、16.1、16.2。
Light Agent モードの Kaspersky Endpoint Security	Kaspersky Security Center Windows 15.1。 Kaspersky Security Center Linux 16.1、16.2、16.3。
EDR Agent モードの Kaspersky Endpoint Security	Kaspersky Security Center Windows 14.2、15.1。 Kaspersky Security Center Linux 15.3、15.4、16.0、16.1、16.2、16.3。

Kaspersky Security for Virtualization Light Agent のサポート対象バージョン

Kaspersky Endpoint Security は、Kaspersky Security for Virtualization Light Agent 6.5 の一部として Light Agent として使用することができます。

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、次のバージョンのKaspersky Anti Targeted Attack Platform に基づくソリューションおよびKaspersky Endpoint Detection and Response Expert（オンプレミス）ソリューションと互換性があります：

- Kaspersky Anti Targeted Attack Platform 6.0、6.1、7.0、7.1（Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA)、および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シナリオを含む）。
- Kaspersky Anti Targeted Attack Platform 8.0（Kaspersky Network Detection and Response (KATA)、および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シナリオを含む）。

  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。
- 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）8.0、8.1（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シナリオを含む）。

  Kaspersky Endpoint Detection and Response Expert（オンプレミス）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（クラウド）との統合のためにサポートされているネットワークエージェントのバージョン

本製品を Kaspersky Endpoint Detection and Response Expert（クラウド）と統合するには、Kaspersky Security Center Cloud コンソールのヘルプに記載されている特定のバージョンの Kaspersky Security Center Cloud コンソール用ネットワークエージェントが必要です。

サードパーティ製のソリューションとの互換性

EDR Agent モードの Kaspersky Endpoint Security は、Dr. Web ウイルス対策製品と連携できます。

カスペルスキーの各ソリューションにおける機能比較

Kaspersky Endpoint Securityは、多くのカスペルスキーのマルチプラットフォームソリューションに含まれています。使用可能なアプリケーション機能は、お客様の地域のサービスプロバイダーから購入したソリューションによって決まります。

機能	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Optimum	Kaspersky Next MXDR Optimum	Kaspersky Next EDR Expert	Kaspersky Next XDR Expert	Kaspersky Hybrid Cloud Security、Desktop	Kaspersky Hybrid Cloud Security Enterprise、Desktop/CPU/Server	Kaspers Cloud S Core/C
ファイル脅威対策	✓	✓	✓	✓	✓	✓	✓	✓	

メール脅威対策	✓	✓	✓	✓	✓	✓	✓	✓	
ウェブ脅威対策	✓	✓	✓	✓	✓	✓	✓	✓	
ネットワーク脅威対策	✓	✓	✓	✓	✓	✓	✓	✓	
ファイアウォール管理	✓	✓	✓	✓	✓	✓	✓	✓	
ふるまい検知	✓	✓	✓	✓	✓	✓	✓	✓	
有害 USB 攻撃ブロック	–	✓	✓	✓	✓	✓	✓	✓	
デバイスコントロール	✓	✓	✓	✓	✓	✓	✓	✓	
リムーバブルドライブのスキャン	✓	✓	✓	✓	✓	✓	✓	✓	
アンチクリプター（共有フォルダー用）	✓	✓	✓	–	✓	✓	–	✓	
コンテナスキャン	–	–	–	–	–	✓	–	✓	
アプリケーションコントロール	✓	✓	✓	✓	✓	✓	✓	✓	
ウェブコントロール	✓	✓	✓	✓	✓	✓	✓	✓	
Kaspersky Unified Monitoring and Analysis Platform との連携	–	–	–	–	–	✓	–	–	
Kaspersky Endpoint Detection and Response Expert（クラウド）との連携	–	–	–	–	✓	✓	–	–	
Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携	–	–	–	–	✓	✓	–	–	

Kaspersky Endpoint Detection and Response Optimum	✓	✓	✓	✓	–	–	–	–	
Kaspersky Managed Detection and Response との連携	–	–	–	✓	–	–	–	–	

導入と初期設定

このシナリオに従って、Kaspersky Endpoint Security を導入し、使用するための準備を行うことができます。

1 本製品の使用モードの選択

カスペルスキーのソリューションをカスペルスキー公式 Web サイトまたは当社のパートナーから購入すると、購入時に指定したメールアドレスにメッセージが届きます。このメッセージには、アクティベーションコードと、ライセンス情報ファイルの入手方法に関する情報が記載されています。組織で、コードを使用したアプリケーションのオンラインアクティベーションがサポートされていない場合、ライセンス情報ファイルが必要になることがあります。

選択したソリューションによって、製品を使用できるモードが決まります：

- Kaspersky Endpoint Security のライセンスをお持ちの場合は、製品を標準モードで使用できます。
- Kaspersky Security for Virtualization Light Agent のライセンスをお持ちの場合は、製品を Light Agent モードで使用できます。
- Kaspersky Endpoint Detection and Response Expert（オンプレミス）のライセンスをお持ちの場合は、アプリケーションを EDR エージェントモードで使用できます。

製品の導入方法は、選択した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。

2 環境の準備

インフラストラクチャに応じて、必要な準備作業を実行します。

3 システムイベントインターセプターメカニズムの選択

デバイスのオペレーティングシステムが fanotify に対応している場合は、インストール中に、システムイベントのインターセプトに使用するメカニズムを選択できます。

4 配布パッケージの準備

製品のインストールに必要なファイルをダウンロードします。必要なファイルは、保護対象デバイスのオペレーティングシステムと製品の導入方法によって異なります。

5 Kaspersky Security Center での準備作業

Kaspersky Security Center で準備作業を実行します。組織のセキュリティ対策を一元管理するには、Kaspersky Security Center の使用を推奨します。Kaspersky Endpoint Security を EDR エージェントモードまたは Light Agent モードで使用する場合にも、Kaspersky Security Center が必要です。

6 本製品のインストール

組織のニーズに合った方法でデバイスに製品をインストールします：

- Kaspersky Security Center を使用した製品のインストール
- コマンドラインを使用したアプリケーションのインストール

7 特定のオペレーティングシステムでのインストール後の追加設定手順

一部の Linux オペレーティングシステムでは、Kaspersky Endpoint Security のインストール後に追加の設定が必要です。

モードと導入スキーム

Kaspersky Endpoint Security は、多くのカスペルスキーのソリューションの一部です。選択したソリューションによって、アプリケーションの動作モードと導入方式が決まります。

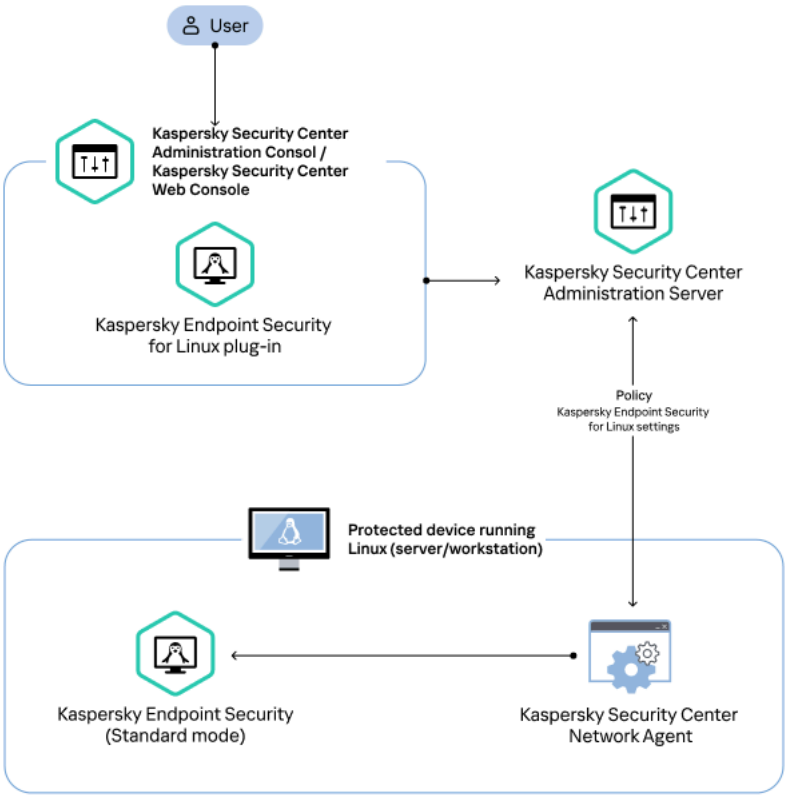
標準モード

本製品の既定のモードです。Kaspersky Endpoint Security は、Linux ワークステーションおよびサーバーに対して、様々な種類の脅威、ネットワーク攻撃、詐欺から包括的に保護します。

このモードでは、アプリケーションは、ファイル脅威対策やふるまい検知などのデバイス保護および制御コンポーネントと、組み込みエージェントを使用して、高度な脅威や標的型攻撃から保護します。

Kaspersky EPP（Endpoint Protection Platform）ソリューションの一部として、このモードで本製品をインストールできます。たとえば、標準モードの Kaspersky Endpoint Security は、Kaspersky Endpoint Security for Business の一部です。

Kaspersky Endpoint Security の主な導入方式は、Kaspersky Security Center を使用した集中導入です。保護対象となる各デバイスに、Kaspersky Endpoint Security と Kaspersky Security Center ネットワークエージェントコンポーネントをインストールする必要があります。このコンポーネントは、デバイスを Kaspersky Security Center 管理サーバーに接続し、Kaspersky Security Center を使用してデバイスを管理できるようにします。



標準モードでの Kaspersky Endpoint Security の導入方式

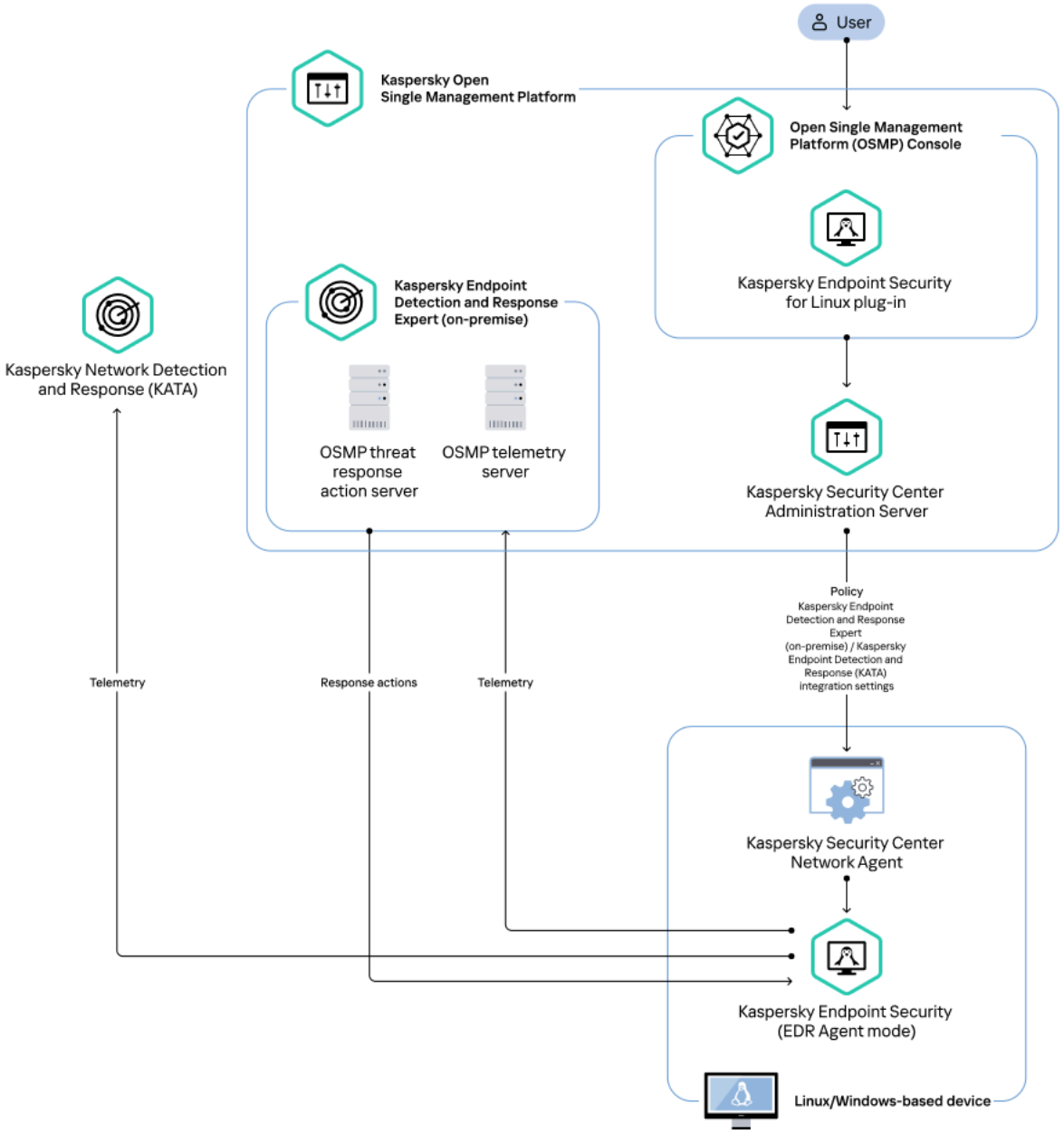
Endpoint Detection and Response Agent（EDR Agent）モード

このモードでは、Kaspersky Detection and Response ソリューションをサードパーティ製アンチウイルスソリューションとともに導入できます。Detection and Response ソリューションには、以下が含まれます：

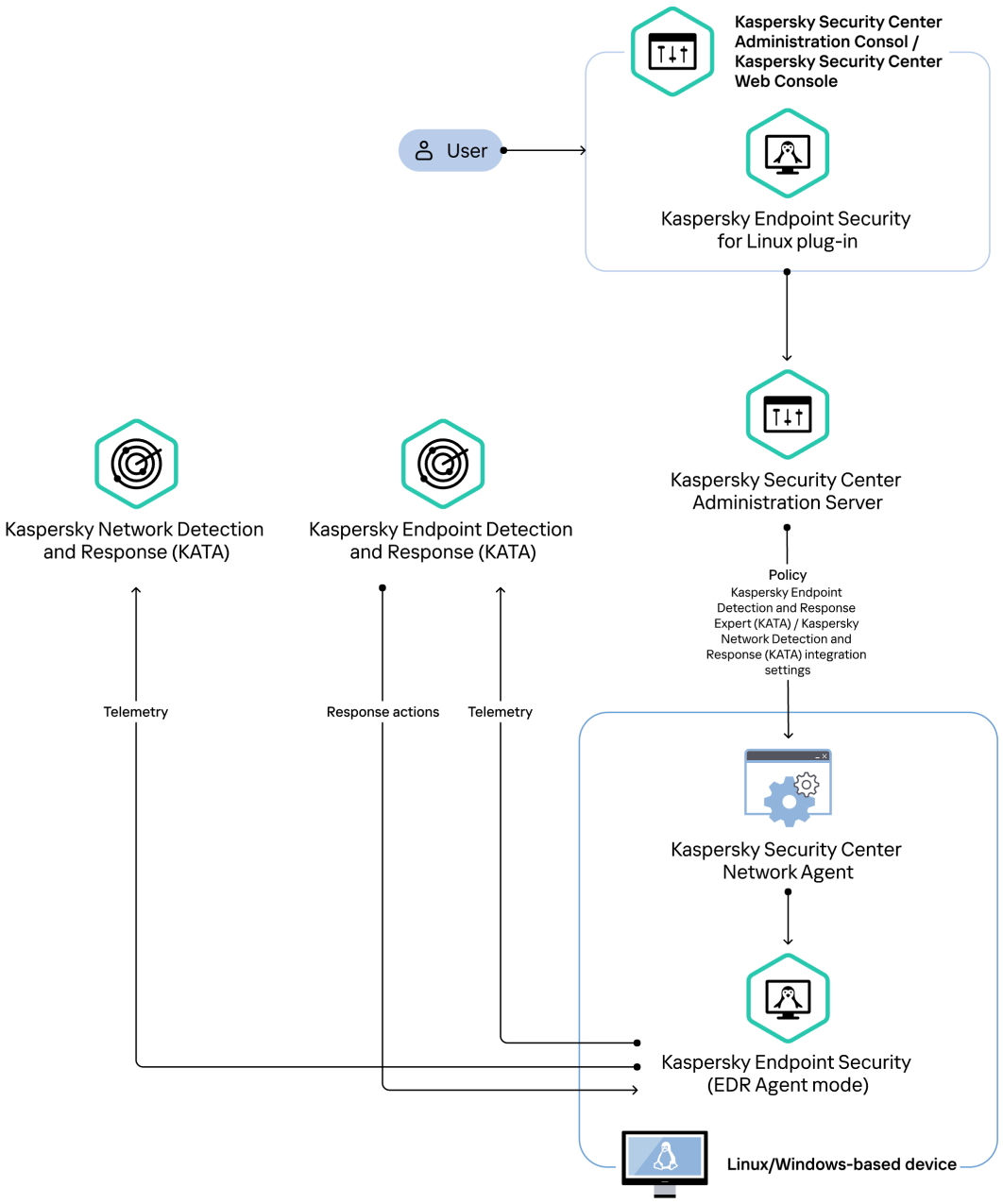
- Open Single Management Platform 上の Kaspersky Endpoint Detection and Response Expert（オンプレミス）（以下、Open Single Management Platform を「OSMP」とも表記）。
- Kaspersky Anti Targeted Attack Platform 上の Kaspersky Endpoint Detection and Response および Kaspersky Network Detection and Response（以下「KATA」ともいいます）。

EDR Agent モードでは、ファイル脅威対策やウェブ脅威対策などの保護および制御コンポーネントは使用できません。サードパーティ製のアンチウイルスアプリケーションがデバイスを保護します。EDR エージェントは、これらのデバイスで実行されているプロセス、開かれ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、Detection and Response ソリューションと連携して、高度な脅威や標的型攻撃から保護します。

Kaspersky Endpoint Security を EDR Agent モードで動作させるには、適切なインフラストラクチャを導入する必要があります。詳細は、選択した Detection and Response ソリューションのヘルプセクションを参照してください。EDR エージェント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。



Kaspersky Endpoint Detection and Response Expert（オンプレミス）と併用する EDR Agent モードの Kaspersky Endpoint Security の導入方式



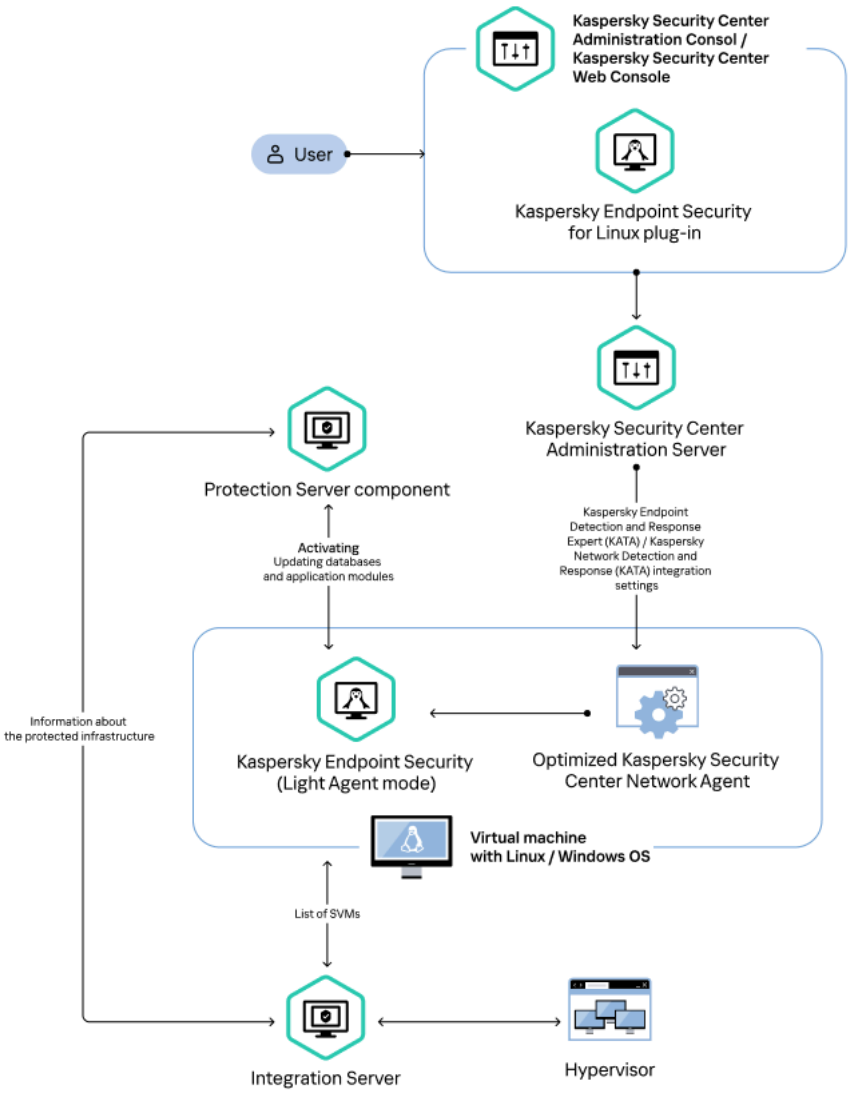
Kaspersky Endpoint Detection and Response および Kaspersky Network Detection and Response と併用する EDR Agent モードの Kaspersky Endpoint Security の導入方式

Light Agent モード

Light Agent モードの 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 Security for Virtualization Light Agent ソリューションの一部です。

このモードでは、標準モードと同じ保護機能および管理コンポーネントを使用できます。違いは、オブジェクトに対するウイルスやその他のマルウェアのスキャン、ライセンスの追加、定義データベースとモジュールのアップデートが、別の仮想マシンである SVM（Secure Virtual Machine）にインストールされた特別なソリューションコンポーネントによって実行される点です。これにより、ハイパーバイザーの負荷を軽減できます。Light Agent モードのアプリケーションは、仮想マシンのリソースではなく SVM のリソースを使用してインフラストラクチャを保護するためです。

Kaspersky Endpoint Security を Light Agent モードで動作させるには、適切なインフラストラクチャを導入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。Light Agent モードの特有の側面の詳細については、既知の問題と制限事項の記事を参照してください。



Light Agent モードの Kaspersky Endpoint Security の導入方式

アプリケーションモードを選択した後、導入シナリオに戻り、環境の準備ステップから続行できます。

本製品のインストール環境の準備

インフラストラクチャの準備

Kaspersky Security Center

Kaspersky Security Center を使用して本製品を集中管理する場合は、インフラストラクチャに Kaspersky Security Center をインストールします。Kaspersky Security Center Windows をすでにインストールしていて、Kaspersky Security Center Linux への移行を予定している場合は、次の手順に従ってください：Kaspersky Security Center Linux へのデータの移行。

EDR Agent モードの Kaspersky Endpoint Security

Kaspersky Endpoint Security を EDR Agent モードで動作させるには、適切なインフラストラクチャを導入する必要があります。詳細は、選択した Detection and Response ソリューションのヘルプセクションを参照してください。

Light Agent モードの Kaspersky Endpoint Security

Kaspersky Endpoint Security を Light Agent モードで実行するには、Kaspersky Security for Virtualization Light Agent ソリューションを導入する必要があります：

1. Kaspersky Security for Virtualization Light Agent ソリューションのコンポーネント、具体的には Integration Server と Protection Server をインストールします。

2. Protection Server を運用できるように準備するため、ソリューションをアクティベートし、Protection Server と Light Agent の定義データベースのアップデートを設定します。

   ソリューションコンポーネントのインストールと設定の詳細については、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください。

3. 保護対象の仮想マシンがLight Agent モードの要件を満たしていることを確認してください。

4. 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 Light Agent モードは、Arm アーキテクチャベースのデバイスおよび Elbrus CPU 搭載デバイスではサポートされていません。

インストールに向けたデバイスの準備

- デバイスが本製品のハードウェアおよびソフトウェア要件を満たしていることを確認してください。

- Kaspersky Endpoint Security を標準モードまたは Light Agent モードでインストールする場合は、デバイスにサードパーティ製のウイルス対策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てください。EDR Agent モードでは、Kaspersky Endpoint Security は Dr. アプリケーションと併用できます。 Web アンチウイルスアプリケーション。

- 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てください。Kaspersky Endpoint Agent for Linux 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ください。

- デバイスに iptables ユーティリティがインストールされていることを確認してください。本製品では、ネットワークトラフィックをインターセプトするために iptables ユーティリティが必要です。

- 次のディレクトリの所有者が root 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、/opt、/usr/bin、/usr/lib、/usr/lib64。これは、本製品の起動と正常な動作に必要です。

- 本製品の実行中は、オペレーティングシステムで使用されるファイルディスクリプタの数が大幅に増加する可能性があります。ディスクリプタ数の制限が十分に高いことを確認してください。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。一般的には、/etc/sysctl.conf ファイルで `fs.file-max=9223372036854775807` を指定して制限を無効にすることを推奨します。この変更を行った後、オペレーティングシステムを再起動してください。

- オペレーティングシステムで `kernel.yama.ptrace_scope=0` が設定されていることを確認してください。`kernel.yama.ptrace_scope` パラメータのその他の値は、Kaspersky Endpoint Security の動作に影響する可能性があります。詳細については、既知の問題点と制限事項セクションを参照してください。

さらに、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するには：

- インストールする kesl-gui パッケージのバージョンは、kesl パッケージのバージョンと一致している必要があります。

- Kaspersky Endpoint Security のグラフィカルインターフェイスを正常に動作させるには、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必要があります。

- デバイスがパッケージマネージャーのリポジトリにアクセスできる場合、本製品のグラフィカルインターフェイスのインストール中に、必要な依存関係がすべて自動的にインストールされます。デバイスがプライベートセグメント内にあり、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：

  1. 参照デバイスで依存関係のリストを確認してください（libice6、libsm6、zlib1g、kesl）。

  2. 次のいずれかの操作を実行します：

     - 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から、パッケージマネージャーを使用してインストールします。

     - グラフィカルインターフェイスのインストール中に、パッケージがデバイスにダウンロードされていることを確認してください。

MMC プラグインのサポートに関する追加要件

Kaspersky Security Center 管理コンソールを使用して本製品を管理する場合は、管理サーバーがインストールされているデバイスに Microsoft® Visual C++® 2015 Redistributable Update 3 RC をインストールしてください（https://www.microsoft.com/en-us/download/details.aspx?id=52685 を参照）。これは、Kaspersky Endpoint Security MMC 管理プラグインの動作に必要です。

特定のオペレーティングシステムに関する追加要件

クローズドソフトウェア環境モードの Astra Linux

互換性パックのインストール

次の場合は、互換性パックをインストールする必要があります：

- クローズドソフトウェア環境モードで本製品をインストールする前。
- 本製品がすでにインストールされている状態で、オペレーティングシステムをクローズドソフトウェア環境モードに切り替える場合。

パッケージをインストール

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

これにより、Astra Linux Special Edition オペレーティングシステム（Arm アーキテクチャ用アップデート 4.7、1.6、1.7、1.8）で、クローズドソフトウェア環境モードにおいてアプリケーションを実行できるようになります。

ptrace の再許可

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ため、Astra Linux のインストール時に ptrace のブロックを解除することを推奨します。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**）。

SUSE Linux Enterprise Server 15

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にアプリケーションをインストールする前に、insserv-compat パッケージをインストールする必要があります。

クローズドソフトウェア環境モードの ALT SP

ALT SP オペレーティングシステムをクローズドソフトウェア環境モードで実行しているデバイスにアプリケーションをインストールする前に、次の操作を実行してください：

1. クローズドソフトウェア環境モードを無効にします：

   ```
   integrity-remover
   ```

2. IMA ポリシーを後で変更するために、kesl グループを作成します：

   ```
   groupadd kesl
   ```

3. 作成したグループの一意の識別子（GID）を確認します：

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

4. 本製品が正常に動作するように、ユーティリティを使用して IMA ポリシーを編集し、kesl グループを 本製品のコンポーネントの整合性チェック の対象から除外します。次の手順に従います：

   a. /usr/share/integrity/policy ファイルをコピーします：

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

b. テキストエディター（vim など）で /etc/integrity/policy ファイルを開いて編集します：

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

c. `dont_measure fsmagic=0xf97cff8c` 行の後（通常、これは `dont_measure` セクションの最後の行です）に、次の行を追加します：

```
dont_measure fgroup=<GID>
```

ここで、`<GID>` 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、これは `dont_appraise` セクションの最後の行です）に、次の行を追加します：

```
dont_appraise fgroup=<GID>
```

ここで、`<GID>` 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. テキストエディター（vim など）で /usr/sbin/integrity-sign ファイルを開いて編集します：

```
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。

アプリケーションの初期設定中は、アプリケーションの定義データベースのアップデートを開始しないでください。

インストールが完了したら、クローズドソフトウェア環境モードを有効にして、本製品を起動するために必要な操作を実行します。

OSnova

Kaspersky Security Center を使用してアプリケーションをインストールおよび管理する場合、アプリケーションをインストールする前に、ネットワークエージェントをインストールできるようにデバイスを準備します：

1. 編集するために /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。

```
#KillUserProcesses=yes
```

2. 編集するために /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。

```
#loginctl terminate-session "$XDG_SESSION_ID"
```

SELinux をサポートするオペレーティングシステム

お使いの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ない場合は、アプリケーションをインストールする前に、パッケージマネージャーに応じて policycoreutils-python または policycoreutils-python-utils パッケージをインストールします。

policycoreutils-python-utils パッケージは、Fedora、Debian、Ubuntu、および RHEL 7 以降の dnf、apt、yum の各パッケージマネージャー向けに提供されています。

policycoreutils-python パッケージは、yum および CentOS/RHEL 7 以前のパッケージマネージャー向けに提供されています。

Kylin OS

Kylin OS デバイスにアプリケーションをインストールする前に、次の操作を実行してください：

1. UKUI（Ubuntu Kylin User Interface）で、Firewallをオフにします。これを行うには、**Kylin Security Center → Firewall とネットワーク保護**セクションに移動し、**Firewall**で、**パブリックネットワーク**と**プライベートネットワーク**の切り替えスイッチを無効にします。

2. UKUI で、アプリケーションネットワーク制御を無効にします。これを行うには、**Kylin Security Center → Firewall とネットワーク保護**セクションに移動し、**アプリケーションネットワーク制御**で**無効**を選択します。

3. UKUI で、アプリケーションソースチェックを無効にします。これを行うには、**Kylin Security Center → アプリケーション保護**セクションに移動し、**アプリケーションソースチェック**で**無効**を選択します。

4. KYSEC セキュリティメカニズムを無効にします。これを行うには、ターミナルで次の操作を実行します：

   a. 現在のステータスを確認します：

   ```
   getstatus
   ```

   b. KYSEC セキュリティメカニズムを無効にします：

   ```
   setstatus disable -p
   ```

   c. KYSEC セキュリティメカニズムが無効になっていることを確認します：

   ```
   getstatus
   ```

5. 組み込みのアンチウイルスアプリケーションをアンインストールします。そのためには、ターミナルで次のコマンドを実行します：

```
sudo dpkg -P pksav
```

6. Qaxsafe アンチウイルスがデバイスにインストールされている場合は、アンインストールする必要があります。次の手順に従います：

   a. 自己保護を無効にします：

      1. タスクバーの通知領域でアプリケーションアイコンを探し、アプリケーションアイコンをダブルクリックしてコンテキストメニューを開きます。

      2. コンテキストメニューで、**設定 → プロテクションセンター**を選択します。

      3. ウィンドウが開きます。そのウィンドウで、**自己保護を有効にする** チェックボックスをオフにし、要求された場合はパスワードを入力します。

   b. Qaxsafe アンチウイルスをアンインストールします。そのためには、ターミナルで次のコマンドを実行します：

```
sudo dpkg -P qaxsafe
```

   c. 残っているファイルをすべて削除します。そのためには、ターミナルで次のコマンドを実行します：

```
sudo rm -rf /opt/qaxsafe
```

fanotify をサポートしていないオペレーティングシステム

アプリケーションのインストールを続行する前に、デバイスに次のものがインストールされていることを確認します：

- 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

役立つ記事

Kylin OS での問題のトラブルシューティング

インストールのために環境を準備した後、導入シナリオに戻り、システムイベントインターセプトメカニズムの選択の手順から続行できます。

システムイベントのインターセプトメカニズムの選択

本製品が正常に機能するには、ファイル操作とプロセスの起動に関するシステムイベントをインターセプトする必要があります。システムイベントのインターセプトは、すべての本製品のモード（標準モード、Light Agent モード、EDR エージェントモード）で必要です。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。

システムイベントのインターセプトメカニズム

本製品では、システムイベントをインターセプトするために、次のメカニズムを使用できます：

- **fanotify に基づくシステムインターセプターメカニズム。***Fanotify* は、ファイルシステム内のイベント（ファイルを開く、読み取る、書き込む、閉じるなど）を監視し、アプリケーションがそれらをリアルタイムでインターセプトできるようにする Linux カーネルのサブシステムです。

- **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。***更新可能なカーネルモジュール*は、fanotify テクノロジーに基づくシステムインターセプトメカニズムと連携して動作します。これにより、システムイベントをuser spaceではなくkernel spaceで処理することで、Kaspersky Endpoint Security によるファイル操作のインターセプトおよびプロセス起動のインターセプトを最適化できます。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。本製品のパフォーマンスは、ファイルおよびプロセスのスキャン結果のキャッシュにより向上します。

  更新可能なカーネルモジュールは、次のタスクおよびコンポーネントにも使用されます：

  - ファイル脅威対策
  - アンチクリプター
  - 脆弱性攻撃ブロック
  - ふるまい検知
  - アプリケーションコントロール
  - オブジェクトの実行防止（Kaspersky Endpoint Detection and Response Expert（オンプレミス）および Kaspersky Endpoint Detection and Response Optimum と統合する場合）

  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 テクノロジーに基づくインターセプトメカニズムでは、指定したマウントポイントでのファイル操作のインターセプトを完全に除外できます。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 がないオペレーティングシステムにおけるファイル脅威対策用のカーネルモジュール。**デバイス上のオペレーティングシステムが fanotify テクノロジーをサポートしていない場合（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6）、本製品はシステムイベントをインターセプトするための特殊なモジュールをコンパイルして使用します。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。

システムイベントのインターセプトメカニズムの選択方法

オペレーティングシステムが fanotify をサポートしている場合、本製品の導入時にシステムイベントのインターセプトメカニズムとして、fanotify のみ、または更新可能なカーネルモジュールと fanotify の組み合わせを選択できます。既定の設定は fanotify です。インストール後、本製品の設定でシステムイベントのインターセプトメカニズムを変更できます。

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。

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 1.6.5、1.6.6）。
- Astra Linux Special Edition RUSB.10015-01（operational update 1.7.3、1.7.4、1.7.6、1.7.7、1.7.8、1.7.9）。
- Astra Linux Special Edition RUSB.10015-01（operational update 1.8.2、1.8.3、1.8.4、1.8.5）。

  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 8.x
- Debian GNU/Linux 12.7、12.8、12.9、12.10、12.11、12.12
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 8.10
- SberLinux 8.10
- SberLinux 9.0.1
- SberLinux 9.1
- SberLinux 9.6
- SberLinux 9.7
- SberOS 3.4
- SberOS 3.5
- Ubuntu 16.04 LTS
- Ubuntu 18.04 LTS
- Ubuntu 20.04 LTS
- 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 11
- ALT Server 11
- ALT Education 11
- 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

32 ビットオペレーティングシステム、Arm アーキテクチャ用のオペレーティングシステム、および Elbrus アーキテクチャ用のオペレーティングシステムはサポートされていません。

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。

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のバージョンは、Kaspersky Endpoint Security のバージョンに依存しません。更新可能なカーネルモジュールの機能は、Kaspersky Endpoint Security の定義データベースとアプリケーションモジュールのアップデートの一環として定期的に拡張されます。したがって、上記のサポート対象オペレーティングシステムのリストは完全ではない場合があります。お使いのデバイスが更新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ことを確認するには、カスペルスキー ULKM ツールを使用してください。

Web コンソールまたは管理コンソールを使用してリモートで確認する方法

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。詳細については、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確認するデバイスを対象に、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。

   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。

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。

デバイスでローカルに確認する方法

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. 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。詳細については、Kaspersky Security Center のヘルプを参照してください。

3. スキャンするデバイスで、Kaspersky ULKM toolユーティリティをローカルに実行します。

```
ulkmtool --check remote
```

4. リターンコードを確認します。

```
echo $?
```

   このユーティリティは、コマンドラインで次のコードを返します：

   0 = Success は、デバイスが更新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。

   1 = NotSupported は、デバイスが更新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。

更新可能なカーネルモジュールのステータスの確認

Kaspersky Security Center Web コンソールまたは管理コンソールで、Kaspersky Endpoint Security がインストールされているデバイスの更新可能なカーネルモジュールのステータスを確認できます。これを行うには、デバイスに割り当てられたタグを確認します：

- *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。

デバイスに割り当てられたタグの表示について詳しくは、Kaspersky Security Center のヘルプを参照してください。

セキュアブートのサポート

更新可能なカーネルモジュールはSecure Bootをサポートしています。Secure Bootが有効になっているオペレーティングシステムで、更新可能なカーネルモジュールに基づくインターセプト機構を使用するには、モジュールの署名に使用されている Kaspersky Endpoint Security の公開証明書をオペレーティングシステムに追加してから、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。

証明書をダウンロード

Ubuntu に証明書を追加する例

1. お使いのオペレーティングシステムでセキュアブートが有効になっていることを確認します：

```
mokutil --sb-state
```

2. mokutil ユーティリティを使用して、ダウンロードした証明書をオペレーティングシステムに追加します：

```
mokutil --import <path to certificate>
```

3. Kaspersky Endpoint Security を再起動します。
4. 次のコマンドを実行して、更新可能なカーネルモジュールが動作しているかどうかを確認します：

```
kesl-control --app-info
```

システムイベントインターセプトメカニズムを選択した後、導入シナリオに戻り、配布パッケージの準備ステップから続行できます。

配布パッケージの準備

*Kaspersky Endpoint Security の配布パッケージ*は、アプリケーションのインストールおよびアップデート用のファイル一式と、ユーザー契約書（使用許諾契約書、プライバシーポリシー、Kaspersky Security Network に関する声明）の本文で構成されています。アプリケーションをローカルで管理および監視しやすくするために、グラフィカルインターフェイスを含む配布パッケージを個別にダウンロードすることもできます。

Kaspersky Security Center を使用して企業ネットワーク内のデバイスに導入するためのインストールパッケージを作成する場合、およびコマンドラインを使用してアプリケーションを導入する場合は、配布パッケージが必要です。

Kaspersky Security Center を使用して導入するには、*アプリケーションのリモートインストール用配布パッケージ*も必要です。この配布パッケージには、アプリケーションのリモート導入に必要なファイルと、ユーザー契約書の本文が含まれています。

> ユーザー契約書の本文は、カスペルスキーの Web サイト（**EULA**セクション）で確認できます。また、アプリケーションのインストール後は、`/opt/kaspersky/kesl/doc/` ディレクトリでも確認できます。

Kaspersky Endpoint Security を手動で導入する場合、または Kaspersky Security Center を使用して導入する場合の配布パッケージは、インストールパッケージの作成ステップで選択できます。

Kaspersky Endpoint Security の導入用配布パッケージを選択する方法

配布パッケージの選択は、次の要素によって異なります：

- Kaspersky Endpoint Security のバージョン：認定済みまたは未認定
- 導入方法：Kaspersky Security Center またはコマンドラインを使用
- OS に応じたパッケージ形式
- オペレーティングシステムのアーキテクチャと CPU の種類
- Kaspersky Endpoint Security の管理方法
- 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の必要性

1. **アプリケーションのバージョンが認定済みか未認定かを確認します**

   - **認定済み**バージョンが必要な場合は、ビジネスアプリケーションのサポートライフサイクルページから配布パッケージ一式をダウンロードします。

     認定済みバージョンには、メインアプリケーションファイルとグラフィカルインターフェイスファイル（`kesl`ディレクトリ）、アプリケーションのリモートインストール用アーカイブ（`remote install`ディレクトリ）、MMC プラグイン（`SCPlugin`）、Web プラグイン（`web plugin`）が含まれています。

     ステップ 3 に進みます。

   - **未認定**バージョンが必要な場合は、次のステップに進みます。

2 導入方法（Kaspersky Security Center を使用するか、コマンドラインを使用するか）を決定します

Kaspersky Security Center を使用した導入の場合は、次のいずれかのソースから配布パッケージをダウンロードします：

- カスペルスキーの Web サイトから
- Kaspersky CompanyAccount をお持ちの場合は、テクニカルサポートにリクエストを送信することにより

コマンドラインを使用した導入の場合は、カスペルスキーの Web サイトから配布パッケージをダウンロードします：

- メインアプリケーションの配布パッケージ（`Distributive`）
- 必要に応じて、グラフィカルユーザーインターフェイス（`Product GUI`）付きの配布パッケージ

カスペルスキーの Web サイトから配布パッケージをダウンロードする場合は、次のファイルが必要になります：

- メインアプリケーションの配布パッケージ（`Distributive`）
- 必要に応じて、グラフィカルユーザーインターフェイス（`Product GUI`）付きの配布パッケージ
- Kaspersky Security Center を使用したアプリケーションのリモートインストール用の配布パッケージ（**追加の配布パッケージ** → `Files for Product remote installation`）
- Kaspersky Security Center ネットワークエージェントの配布パッケージ（Kaspersky Security Center の配布セクション → `Network agent`）

アプリケーションの配布パッケージは、すべての言語版で同じです。Kaspersky Endpoint Security の言語は、アプリケーションの初期設定時に選択します。ローカライズのサポートは、オペレーティングシステムにインストールされている言語によって異なります。

3 保護対象デバイスのオペレーティングシステムに応じてパッケージ形式を決定します

オペレーティングシステム	パッケージ形式
Debian、Ubuntu、Astra Linux、Linux Mint	`.deb`
Red Hat Enterprise Linux、CentOS、Oracle Linux、RED OS、SUSE Linux Enterprise、openSUSE、Rocky Linux、AlmaLinux、ALT シリーズの OS、GosLinux、Rosa シリーズの OS、Amazon Linux 2023	`.rpm`

お使いのオペレーティングシステムが一覧にない場合は、お使いのオペレーティングシステムのドキュメントに従ってパッケージ形式を選択してください。

4 オペレーティングシステムのアーキテクチャと CPU の種類を決定します

CPU の種類とオペレーティングシステムのビット数	配布パッケージ
Arm CPU、64 ビットオペレーティングシステム	`arm64` `aarch64`
Elbrus CPU	`e2k`
その他のプロセッサ、32 ビットオペレーティングシステム	`i386`

CPU の種類とオペレーティングシステムのビット数	配布パッケージ
その他のプロセッサ、64 ビットオペレーティングシステム	x86_64 x64 amd64

サポートが制限されているオペレーティングシステム（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6）に Kaspersky Endpoint Security アプリケーションをインストールするには、OLD のマークが付いた配布パッケージを選択します。

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。

配布パッケージの準備後、導入シナリオに戻り、Kaspersky Security Center での準備操作ステップから続行できます。

Kaspersky Security Center での準備作業

Kaspersky Endpoint Security アプリケーションをインストールする前に、Kaspersky Security Center で次の操作を実行することを推奨します。

1 デバイスの管理グループの設定

Kaspersky Security Center を使用してアプリケーションを管理するには、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管理グループに配置する必要があります。デフォルトでは、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** グループに移動します。

事前に、管理グループへのデバイスの自動配置ルールを設定し、デバイスのタイプごとに個別のグループを作成して、タイプに応じてデバイスをグループに割り当てることを推奨します。これにより、デバイスに応じて異なるアプリケーション設定を適用できます。

デバイスを手動で管理グループに配置することもできます。

❷ 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、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、Kaspersky Security Center に接続するすべてのデバイスにインストールする必要があります。

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。

その結果、ネットワークエージェントがインストールされたデバイスは、それらのデバイスに設定された移動ルールに対応するグループに表示されます。移動ルールを設定していない場合、デバイスは **未割り当てデバイス** グループに表示されます。

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

使用している Kaspersky Security Center 管理コンソールに応じて、Kaspersky Endpoint Security 管理プラグインをインストールします：

- **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。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。

  Kaspersky Endpoint Security MMC プラグインをインストールする方法

  > 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：

  1. **Kaspersky Endpoint Security for Linux** セクションのアプリケーションのダウンロードページ（**ビルド → 管理プラグイン**）から klcfginst.msi ファイルをダウンロードします。

  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、klcfginst.msi ファイルを実行します。

  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を開き、**プロパティ**を選択します。

   - ［**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**］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 管理コンソールを使用して Kaspersky Endpoint Security アプリケーションを管理しており、アプリケーションの複数のバージョンがインストールされている場合は、Kaspersky Endpoint Security アプリケーションのバージョンごとに管理プラグインをインストールする必要があります。そのため、管理する製品のバージョンに合わせて、異なるバージョンの管理プラグインで作成したポリシーも使用できます。また、旧バージョンの管理プラグインで作成したポリシーとタスクを新しいバージョンに変換することもできます。

- **Kaspersky Endpoint Security Web 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。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。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。

  Kaspersky Endpoint Security Web プラグインをインストールする方法

  Web プラグインは、次の方法でインストールできます：

  - 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 コンソールのクイックスタートウィザードについて詳しくは、Kaspersky Security Center ヘルプ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ファイルから配布キットを使用して手動でインストールできます。

  Kaspersky Security Center から Kaspersky Endpoint Security の Web プラグインを手動でインストールするには：

  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. ［**追加**］をクリックします。

     使用可能な管理プラグインのリストが開きます。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。

3. 使用可能なプラグインのリストで、**Kaspersky Endpoint Security <version number> for Linux** Web プラグインを選択します。

4. 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。

5. 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。

新しいプラグインが、インストール済み Web プラグインのリスト（［**設定**］ → ［**Web プラグイン**］）に表示されます。

ファイルから Kaspersky Endpoint Security の Web プラグインを手動でインストールするには：

1. **Kaspersky Endpoint Security for Linux** セクションのアプリケーションのダウンロードページ（**追加の配布パッケージ → Web コンソールプラグイン**）から、Web プラグインを含むアーカイブをダウンロードします。

2. ダウンロードしたアーカイブをローカルで展開します。

3. 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。

4. ［**リストから追加**］ボタンをクリックします。

5. ウィンドウが開きます。このウィンドウで、plugin.zip ファイルへのパスと signature.txt ファイルへのパスを指定します。これらのファイルは、Web プラグインのアーカイブを展開したフォルダーにあります。

6. ［**追加**］をクリックします。

7. 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。

動画：ウィザードを使用した管理 Web プラグインのインストール

動画：隔離されたネットワークでの管理 Web プラグインのインストール

4 Kaspersky Endpoint Security ポリシーの作成

Kaspersky Security Center Web コンソールまたは管理コンソールで、Kaspersky Endpoint Security のポリシーを作成します（使用している Kaspersky Security Center 管理コンソールによって異なります）。

アプリケーションを使用するモードに応じて、次の設定を管理します：

標準モードの場合

管理コンソールのウィザードでポリシーを作成した場合は、アプリケーション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**。Kaspersky Security Center Web コンソールのウィザードでポリシーを作成した場合は、アプリケーションモードの選択をスキップします。

EDR エージェントモードの場合

1. 管理コンソールのウィザードでポリシーを作成した場合は、アプリケーション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**。Kaspersky Security Center Web コンソールのウィザードでポリシーを作成した場合は、アプリケーションモードの選択をスキップします。

2. ウィザードの指示に従って、ポリシーの作成を完了します。

3. 作成したポリシーのプロパティをKaspersky Security Center Web コンソールまたは管理コンソールで開き、デバイスの保護に使用する Detection and Response ソリューションとの統合を有効にします：

   - OSMP プラットフォーム上の Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携では、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。設定は、Kaspersky Security Center Web コンソールで使用できます

   - Kaspersky Anti Targeted Attack Platform 上の Kaspersky Endpoint Detection and Response との連携では、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。設定は、Kaspersky Security Center Web コンソールおよび管理コンソールで使用できます。

   - Kaspersky Anti Targeted Attack Platform 上の Kaspersky Network Detection and Response との統合では、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。設定は、Kaspersky Security Center Web コンソールおよび管理コンソールで使用できます。

Light Agent モードの場合

新規ポリシーウィザードでは：

1. **仮想環境保護用 Light Agent モード**を指定します。

2. SVM 検出設定を管理します：

   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、Light Agent が拡張 SVM 選択アルゴリズムを使用しており、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っている場合、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。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. 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、Integration Server への接続に使用する新しい接続設定（IPv4 アドレスまたは完全修飾ドメイン名（FQDN）とポート）を指定します。

   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。

c. 手動で定義した SVM アドレスのリストを選択した場合は、このポリシーで管理される Light Agent が接続できる SVM のリストを作成します。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。

その他のポリシー設定は、既定値のままにできます。既定の設定により、基本的な保護レベルが提供されます。Kaspersky Endpoint Security のインストール後、組織の要件に従ってポリシーを設定できます。これを行うには、ヘルプのアプリケーションの管理セクションに記載されているコンポーネント設定シナリオを使用できます。

動画：ポリシーの作成

❺ アプリケーションのデータベースとモジュールの集中アップデートの設定

既定では、Kaspersky Endpoint Security は定義データベースがない状態でデバイスにインストールされます。本製品は、定義データベースがデバイスにダウンロードされた後にのみ機能するようになります。本製品のインストール直後に保護が開始されるようにするには、定義データベースの集中アップデートを設定します。

Kaspersky Security Center Web コンソールまたは管理コンソール（使用している Kaspersky Security Center 管理コンソールに応じて異なります）で、以下を実行します：

1. 管理サーバーのタスク *管理サーバーのリポジトリへのアップデートのダウンロード* を開始します。このタスクは、管理サーバークイックスタートウィザードによって自動的に作成されます。

   このタスクは、Kaspersky Endpoint Security のアップデートパッケージを管理サーバー上のアップデートディレクトリにダウンロードします。

2. Kaspersky Endpoint Security アプリケーション用に、アップデート種別のグループタスクを作成します。タスク設定で、以下を指定します：

   - アップデート元：Kaspersky Security Center。
   - タスクスケジュール：少なくとも 1 日 1 回。このタスクは 1 日に 4 ～ 6 回実行することを推奨します。

動画：定義データベースの集中アップデートの設定

6 ライセンスの追加とアクティベーションタスクの作成

標準モードで本製品をアクティベートするには、本製品にライセンスを追加する必要があります。ライセンスでカバーされていないコンポーネントがある場合、別のライセンスが必要になる場合があります：

EDR エージェントモードで Kaspersky Endpoint Security をアクティベートするには、EDR Expert（オンプレミス）のライセンスが必要です。

インフラストラクチャと組織の要件に応じて、アクティベーション方法を選択できます：

- 本製品がすべてのデバイスに同じ機能セットでインストールされている場合は、ライセンスの自動配布を使用します。配布するライセンスは、まず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 Kaspersky Security Center のライセンス保管領域に追加する必要があります。詳細については、Kaspersky Security Center ヘルプを参照してください。

- 本製品の機能セットがデバイスごとに異なる場合、アクティベーションには異なるライセンスが必要です。この場合、保護対象デバイスを異なる管理グループに配置し、各管理グループにライセンスを追加するためのグループタスクを設定します。

Light Agent モードの Kaspersky Endpoint Security は、SVM に接続した後、Protection Server からライセンスの情報を受信します。Light Agent モードの Kaspersky Endpoint Security を個別にアクティベートする必要はありません。

動画：アクティベーションコードで本製品をアクティベートする

動画：ライセンス情報ファイルで本製品をアクティベートする

Kaspersky Security Center の準備が完了したら、導入シナリオに戻り、本製品のインストールステップから続行できます。

Kaspersky Security Center を使用した本製品のインストール

インストールに関する特別な留意事項：

- Elbrus CPU を搭載したデバイスでは、Kaspersky Endpoint Security の EDR Agent モードおよび Light Agent モードはサポートされていません。
- Arm デバイスでは、Light Agent モードの Kaspersky Endpoint Security はサポートされません。

Kaspersky Security Center を使用して本製品をインストールする場合の推奨シナリオには、次の手順が含まれます：

Kaspersky Endpoint Security は、Kaspersky Security Center から クイックスタートウィザードおよび保護導入ウィザードを使用してインストールすることもできます。

1 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には、次のものが含まれます：

- メインの配布パッケージ
- 本製品のリモートインストール用の配布パッケージ
- 本製品のグラフィカルインターフェイスを含む配布パッケージ
- 初期設定（インストール時に適用）

次の方法でインストールパッケージを作成できます：

- **カスペルスキーのサーバーでホストされている配布パッケージを使用する**。Kaspersky Security Center では、指定した配布パッケージからインストールパッケージが自動的に作成されます。

  動画：Kaspersky Security Center でのインストールパッケージの自動作成

> サポートが制限されているオペレーティングシステム（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6）に Kaspersky Endpoint Security アプリケーションをインストールするには、`for legacy OS` のマークが付いた配布パッケージを選択します。

- **手動で、配布パッケージの準備手順で準備したファイルを使用する**。設定情報ファイルを使用して初期設定を指定する場合、または作成したインストールパッケージを異なるオペレーティングシステムや異なるパッケージマネージャーで使用する場合は、この方法を推奨します。

動画：Kaspersky Security Center でのインストールパッケージの手動作成

事前にダウンロードした製品データベースをインストールパッケージに追加できます。統合データベースを含むインストールパッケージを使用している場合、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。

インストールパッケージは何度でも使用できます。

インストールパッケージを手動で準備する方法

1. Kaspersky Endpoint Security のリモートインストール用ファイルを含む圧縮ファイルをローカルで解凍します。

2. メインのアプリケーションファイルを含むパッケージを同じディレクトリに配置します。

   作成したインストールパッケージを異なるオペレーティングシステム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オペレーティングシステムとパッケージマネージャーに対応する配布パッケージをディレクトリに配置します。

3. 本製品のグラフィカルインターフェイスを使用する場合は、グラフィカルインターフェイスのパッケージを同じディレクトリに配置します。

   作成したインストールパッケージのプロパティ、またはautoinstall.ini 設定情報ファイルで該当する設定（`USE_GUI=Yes`）を編集し、グラフィカルインターフェイスの使用を有効にします。既定では、グラフィカルインターフェイスはインストールされません。

   > Kaspersky Endpoint Security を Light Agent モードで使用する場合、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。

4. 設定情報ファイルを使用して本製品の初期設定を行う場合は、autoinstall.ini 設定情報ファイルを開き、必要に応じて編集します。autoinstall.ini ファイルは、Kaspersky Endpoint Security のリモートインストール用ファイルを含む圧縮ファイルを解凍したフォルダー内にあります。

   a. 既定では、本製品は標準モードで使用されます。

      本製品を EDR Agent モードで使用するには、`ENDPOINT_AGENT_MODE=Yes` を設定します。

      本製品を Light Agent モードで使用するには、`KSVLA_MODE=Yes` を設定します。

      > 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。

b. 本製品を Light Agent モードでインストールするには：

- 一時仮想マシンの作成元となるテンプレートに本製品をインストールする場合は、`VDI_MODE=Yes` を設定します。この設定により VDI 保護モードが有効になり、一時仮想マシン上での本製品のパフォーマンスが最適化されます。

- 保護する仮想マシンの仮想インフラストラクチャ内での役割（サーバーまたはワークステーション）を指定します（`SERVER_MODE=Yes|No`）。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。

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、後から本製品の初期設定を変更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。

Web コンソールでのインストールパッケージの作成

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：

- **検出と製品の導入 → 導入と割り当て → インストールパッケージ**。

- ［**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. Web コンソールを使用している場合は、インストールパッケージの作成方法を選択します：

- **インストールパッケージをファイルから作成する**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。

- **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**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 コンソールを使用している場合、インストールパッケージはカスペルスキーのサーバーでホストされている配布パッケージから作成されます。

4. パッケージの作成方法に応じて：

- 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圧縮ファイル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、［**ダウンロードしてインストールパッケージを作成**］をクリックします。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。

7. 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。

- 本製品を EDR Agent モードでインストールする場合は、［**使用モード**］設定で［**Endpoint Detection and Response Agent**］を選択します。

- 本製品を Light Agent モードでインストールする場合は、次の設定を指定します：

  使用モードで、［**仮想環境を保護する Light Agent**］を選択します。

  VDI 保護モードを有効にするVDI 保護モードを有効にするには、このチェックボックスをオンにします。本製品を一時的な仮想マシンの作成に使用する仮想マシンテンプレートにインストールする場合は、こちらを推奨します。既定では、このチェックボックスはオフです。

  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）。

- 必要に応じて、その他の初期設定を管理します。

  インストールパッケージに含まれる本製品のすべての初期設定について詳しくは、付録 1を参照してください。

管理コンソールでのインストールパッケージの作成

準備したファイルを使用してインストールパッケージを作成するには：

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. kesl.kud ファイルへのパスを指定します。このファイルは、配布パッケージの準備の手順で本製品をインストールするためのファイルを含む圧縮ファイル（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。

   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すべての条件を読んで同意したことを確認します。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. 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待ってから、ウィザードを終了します。

8. インストールパッケージのプロパティを開き、［**製品設定**］タブに移動します。

- 本製品を EDR Agent モードでインストールする場合は、［**アプリケーションモード**］設定で［**Endpoint Detection and Response Agent**］を選択します。

- 本製品を Light Agent モードでインストールする場合は、次の設定を指定します：

  アプリケーションモード［**仮想環境保護用 Light Agent**］を選択します。

VDI 保護モードを有効にするVDI 保護モードを有効にするには、このチェックボックスをオンにします。本製品を一時的な仮想マシンの作成に使用する仮想マシンテンプレートにインストールする場合は、こちらを推奨します。既定では、このチェックボックスはオフです。

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です。

Light Agent モードでは使用できません：

- 本製品の定義データベースのアップデート元の設定とアップデートの開始
- プロキシサーバーの設定
- 本製品のアクティベーション

Light Agent モードの本製品は、SVM への接続後に Protection Server から定義データベースのアップデートとライセンスの情報を受信します。Kaspersky Endpoint Security を別途アクティベートしたり、定義データベースのアップデートを設定したりする必要はありません。

- 必要に応じて、その他の初期設定を管理します。

  インストールパッケージに含まれる本製品のすべての初期設定について詳しくは、付録1を参照してください。

後で、作成したインストールパッケージのプロパティの［**製品設定**］セクションで、本製品の初期設定を実行することもできます。

ウィザードにより、カスペルスキーのサーバーから取得した配布パッケージに基づいてインストールパッケージが作成されます。

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. ［**その他の操作**］ →［**カスペルスキー製品の現在のバージョンを表示**］ボタンをクリックします。
3. リストから Kaspersky Endpoint Security の配布パッケージを選択し、［**ダウンロードしてインストールパッケージを作成**］ボタンをクリックします。
4. 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。

   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すべての条件を読んで同意したことを確認します。確認するには、確認ウィンドウで両方のチェックボックスをオンにし、［**すべて同意する**］ボタンをクリックします。
5. 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。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。
6. インストールパッケージのプロパティを開き、［**製品設定**］セクションに移動します。

   - 本製品を EDR Agent モードでインストールする場合は、［**アプリケーションモード**］設定で［**Endpoint Detection and Response Agent**］を選択します。
   - 本製品を Light Agent モードでインストールする場合は、次の設定を指定します：

     アプリケーションモード［**仮想環境保護用 Light Agent**］を選択します。

     VDI 保護モードを有効にするVDI 保護モードを有効にするには、このチェックボックスをオンにします。本製品を一時的な仮想マシンの作成に使用する仮想マシンテンプレートにインストールする場合は、こちらを推奨します。既定では、このチェックボックスはオフです。

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です。

Light Agent モードでは、次の設定は使用できません：

- 本製品の定義データベースのアップデート元の設定とアップデートの開始
- プロキシサーバーの設定
- 本製品のアクティベーション

Light Agent モードの本製品は、SVM への接続後に Protection Server から定義データベースのアップデートとライセンスの情報を受信します。Kaspersky Endpoint Security を別途アクティベートしたり、定義データベースのアップデートを設定したりする必要はありません。

- 必要に応じて、その他の初期設定を管理します。

  インストールパッケージに含まれる本製品のすべての初期設定について詳しくは、付録1を参照してください。

後で、作成したインストールパッケージのプロパティの［**製品設定**］セクションで、本製品の初期設定を実行することもできます。

2 社内ネットワーク内のデバイスへの本製品のインストール

Kaspersky Security Center を使用して、アプリケーションのリモートインストールタスクにより本製品をインストールできます。

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。

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で指定した設定、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に従って自動的に実行されます。

ビデオ：Kaspersky Endpoint Security のインストール、定義データベースのアップデート、パフォーマンスの確認

❸ 本製品の定義データベースのアップデート

本製品を標準モードまたは EDR Agent モードでインストールした場合は、Web コンソールまたは管理コンソール（使用している Kaspersky Security Center の管理コンソールに応じて異なります）で、「本製品の定義データベースとモジュールの一元的なアップデートの設定」ステップで作成した［*Update*］グループタスクを実行します。Kaspersky Endpoint Security の定義データベースのアップデートについて詳しくは、「本製品の定義データベースとモジュールのアップデート」セクションを参照してください。

❹ 本製品の状態チェック

これにより、Kaspersky Endpoint Security がインストールおよびアクティベートされ、本製品のデータベースがアップデートされています。インストール後、本製品は自動的に起動します。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
- 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。

本製品を使用する準備ができていることを確認します。

Web コンソールでデバイスの保護ステータスを確認する方法

1. Web コンソールのメインウィンドウで、［**アセット管理**］ → ［**アセット（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。下位グループを選択するには、ウィンドウ上部の **階層を表示** ボタンをクリックします。

   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. デバイスの名前をクリックします。

   管理対象デバイスのプロパティウィンドウが開きます。

4. ［**全般**］タブで、［**プロテクション**］セクションを選択します。［**デバイスステータス**］フィールドに［*OK*］と表示されている必要があります。

   ［**デバイスステータス**］フィールドに、システムディレクトリに対する権限が不十分であるという情報が表示される場合は、このデバイス上でローカルに次のディレクトリの権限を確認してください：/var/opt/kaspersky、/var/log/kaspersky、/opt/kaspersky。所有者が root であり、これらのディレクトリへの書き込みアクセス権が所有者にのみ付与されていることを確認してください。

5. ［**アプリケーション**］タブに移動します。

6. 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。

7. ［**情報**］セクションの［**全般**］タブで、［**定義データベース**］を確認します。本製品の定義データベースが最新の状態であることを確認してください。

8. ［**全般**］タブの［**ライセンス**］セクションに移動し、本製品がアクティベートされていることを確認してください。

9. 本製品を EDR Agent モードでインストールした場合は、［**全般**］タブの［**コンポーネント**］セクションに移動し、「Kaspersky Endpoint Security ポリシーの作成」ステップで設定した統合のステータスが［*実行中*］であることを確認してください。

10. 本製品を Light Agent モードでインストールした場合は、［**全般**］タブの［**コンポーネント**］セクションに移動し、［**仮想環境保護用 Light Agent モード**］行のステータスが［*実行中*］と表示されていることを確認してください。これは、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。

管理コンソールでデバイスの保護ステータスを確認する方法

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。

   管理対象デバイスのプロパティウィンドウが開きます。

4. ［**保護**］セクションを選択します。［**デバイスステータス**］フィールドに［*OK/ネットワーク上で表示可能*］と表示されている必要があります。

   ［**デバイスステータス**］フィールドに、システムディレクトリに対する権限が不十分であるという情報が表示される場合は、このデバイス上でローカルに次のディレクトリの権限を確認してください：/var/opt/kaspersky、/var/log/kaspersky、/opt/kaspersky。所有者が root であり、これらのディレクトリへの書き込みアクセス権が所有者にのみ付与されていることを確認してください。

5. ［**アプリケーション**］セクションに移動します。

6. デバイスにインストールされているアプリケーションのリストで、Kaspersky Endpoint Security を選択し、ダブルクリックして本製品のプロパティウィンドウを開きます。

7. ［**全般**］セクションの［**定義データベース**］フィールドを確認します。本製品の定義データベースが最新の状態であることを確認してください。

8. ［**ライセンス**］セクションに移動し、本製品がアクティベートされていることを確認してください。

9. 本製品を EDR Agent モードでインストールした場合は、［**コンポーネント**］セクションに移動し、「Kaspersky Endpoint Security ポリシーの作成」ステップで設定した統合のステータスが［*実行中*］であることを確認してください。

10. 本製品を Light Agent モードでインストールした場合は、［**コンポーネント**］セクションに移動し、［**仮想環境保護用 Light Agent モード**］行のステータスが［*実行中*］と表示されていることを確認してください。これは、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。

役立つ記事

タスクが実行されない場合、またはポリシーが適用されない場合の対処方法

デバイスのステータスが次の場合の対処方法：「ポリシー設定が無効です。ポリシーが適用されていません。」

エラー：「アプリケーションは現在のバージョンの Kaspersky Security Center Web コンソールでサポートされていないか、アプリケーションの Web プラグインがインストールされていません」

GUI のインストール時に発生する問題のトラブルシューティング

インストールエラーコードの説明

Kaspersky Endpoint Security のインストール後に発生するエラー

Kaspersky Endpoint Security のインストールが完了したら、導入シナリオに戻り、「特定のオペレーティングシステムにおけるインストール後の追加設定手順」の手順から続行できます。

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

インストールに関する特別な留意事項：

- Elbrus CPU を搭載したデバイスでは、Kaspersky Endpoint Security の EDR Agent モードおよび Light Agent モードはサポートされていません。
- Arm デバイスでは、Light Agent モードの Kaspersky Endpoint Security はサポートされません。
- 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するには、root 権限が必要です。
- 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。
- 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。

コマンドラインを使用してアプリケーションをインストールする場合の推奨シナリオは、次の手順で構成されます：

1 Kaspersky Endpoint Security アプリケーションのインストール

インストールを開始する前に、ダウンロードしたアプリケーションのメインファイルを含むパッケージを、デバイスの /tmp ディレクトリに配置してください。

RPM パッケージからアプリケーションをインストールする方法

32 ビットオペレーティングシステムの場合

```
yum install kesl-12.5.0-<build number>.i386.rpm
```

64 ビットオペレーティングシステムの場合

```
yum install kesl-12.5.0-<build number>.x86_64.rpm
```

64 ビット ALT オペレーティングシステムの場合

```
apt-get install kesl-12.5.0-<build number>.x86_64.rpm
```

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の場合

```
yum install kesl-12.5.0-<build number>.aarch64.rpm
```

Arm アーキテクチャの 64 ビット ALT オペレーティングシステムの場合

```
apt-get install kesl-12.5.0-<build number>.aarch64.rpm
```

Elbrus アーキテクチャの 64 ビットオペレーティングシステムの場合

```
yum install kesl-12.5.0-<build number>.2ek.rpm
```

Elbrus アーキテクチャの 64 ビット ALT オペレーティングシステムの場合

```
apt-get install kesl-12.5.0-<build number>.2ek.rpm
```

サポートが限定されている 64 ビットオペレーティングシステムの場合（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6）

```
rpm -i kesl-12.5.0-<build number>.x86_64.rpm
```

CentOS 5.2、CentOS 5.4、CentOS 6.4、または CentOS 6.6 にアプリケーションをインストールするには、Web サイトから OLD と記載された配布パッケージをダウンロードする必要があります。

DEB パッケージからアプリケーションをインストールする方法

32 ビットオペレーティングシステムの場合

```
apt-get install ./kesl_12.5.0-<build number>_i386.deb
```

64 ビットオペレーティングシステムの場合

```
apt-get install ./kesl_12.5.0-<build number>_amd64.deb
```

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の場合

```
apt-get install ./kesl_12.5.0-<build number>_arm64.deb
```

Elbrus アーキテクチャの 64 ビットオペレーティングシステムの場合

```
apt-get install ./kesl_12.5.0-<build number>_2ek.deb
```

❷ 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使用してアプリケーションを管理する場合は、アプリケーションと同じデバイスにグラフィカルインターフェイスをインストールする必要があります。

アプリケーションのグラフィカルインターフェイスに関する特記事項：

- Kaspersky Endpoint Security 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は、グラフィカルインターフェイスをインストールできません。
- アプリケーションを Light Agent モードで使用している場合、グラフィカルユーザーインターフェイスはサポートされません。

インストールを開始する前に、ダウンロードしたアプリケーションのグラフィカルインターフェイスのファイルを含むパッケージを、デバイスの /tmp ディレクトリに配置してください。

RPM パッケージから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する方法

32 ビットオペレーティングシステムの場合

```
yum install kesl-gui-12.5.0-<build number>.i386.rpm
```

64 ビットオペレーティングシステムの場合

```
yum install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

64 ビット ALT オペレーティングシステムの場合

```
apt-get install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

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の場合

```
yum install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

Arm アーキテクチャの 64 ビット ALT オペレーティングシステムの場合

```
apt-get install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

Elbrus アーキテクチャの 64 ビットオペレーティングシステムの場合

```
yum install kesl-gui-12.5.0-<build number>.2ek.rpm
```

Elbrus アーキテクチャの 64 ビット ALT オペレーティングシステムの場合

```
apt-get install kesl-gui-12.5.0-<build number>.2ek.rpm
```

サポートが限定されている 64 ビットオペレーティングシステムの場合（CentOS 6.4、CentOS 6.6）

```
rpm -i kesl-gui-12.5.0-<build number>.x86_64.rpm
```

CentOS 6.4 または CentOS 6.6 にアプリケーションをインストールするには、Web サイトから OLD と記載された配布パッケージをダウンロードする必要があります。

DEB パッケージから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する方法

32 ビットオペレーティングシステムの場合

```
apt-get install ./kesl-gui_12.5.0-<build number>_i386.deb
```

64 ビットオペレーティングシステムの場合

```
apt-get install ./kesl-gui_12.5.0-<build number>_amd64.deb
```

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の場合

```
apt-get install ./kesl-gui_12.5.0-<build number>_arm64.deb
```

Elbrus アーキテクチャの 64 ビットオペレーティングシステムの場合

```
apt-get install ./kesl-gui_12.5.0-<build number>_2ek.deb
```

3 本製品の初期設定

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。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。

本製品の初期設定を対話形式で実行する方法。

ステップ 1：ウィザードの開始

初期セットアップウィザードを開始します

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

ウィザードのプロンプトで、Kaspersky Endpoint Security の初期設定の値を手順に従って指定します。

デバイスにネットワークエージェントがインストールされており、本製品を標準モードまたは EDR Agent モードでインストールする場合、本製品のデータベースのアップデートおよび本製品のアクティベーションに関連する初期セットアップウィザードのステップをスキップできます。

ステップ 2：標準モードまたは Light Agent モードの選択

Light Agent モードで本製品を使用するには、 yes と入力します。

標準モードで本製品を使用するには、 no と入力します。

本製品を EDR Agent モードで使用する場合は、このステップで no と入力し、次のステップで EDR Agent モードを選択する必要があります。

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。

ステップ 3：モードの選択：標準または Endpoint Detection and Response Agent

ステップ 2で本製品を標準モードで使用することを選択した場合、このステップが表示されます。

EDR Agent モードで本製品を使用するには、yes と入力します。

標準モードで本製品を使用するには、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。

ステップ 4：Kaspersky Endpoint Detection and Response Expert（クラウド）との連携

ステップ 3で本製品を標準モードで使用することを選択した場合、このステップが表示されます。

Kaspersky Endpoint Detection and Response Expert（クラウド）との連携を使用するには、yes と入力します。

カスペルスキー Endpoint Detection and Response Expert（オンプレミス）との連携を使用するには、no と入力します。

ステップ 5：仮想マシンのロールの選択

ステップ 2で本製品を Light Agent モードで使用することを選択した場合、このステップが表示されます。

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。

ステップ 6：VDI 保護モードの有効化

ステップ 2で本製品を Light Agent モードで使用することを選択した場合、このステップが表示されます。

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。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。

ステップ 7：ロケールの選択

このステップでは、ウィザードによって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とおりに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。

ステップ 8：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の内容を確認します。

ステップ 9：使用許諾契約書への同意

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。

ステップ 10：プライバシーポリシーへの同意

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。

ステップ 11：Kaspersky Security Network の使用

このステップでは、Kaspersky Security Network の利用規約に同意するかどうかを指定します：

- Kaspersky Security Network に関する声明の条項に同意する場合は、 yes （または y）と入力します。これにより、拡張 KSN モードが有効になります。
- Kaspersky Security Network に関する声明の条項に同意しない場合は、 no （または n）と入力します。

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。

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 Security Network が有効になっている場合、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 は軽量版のマルウェア定義データベースを使用します。

ステップ 12： 特権グループからのユーザーの削除

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

［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。

ステップ 13： ユーザーへの Administrator ロールの割り当て

このステップでは、ウィザードから管理者ロール（admin）の付与を求められます。

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。

ステップ 14： システムイベントインターセプターメカニズムの設定

OS が更新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、本製品は更新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。OS がこれらの要件を満たしていない場合でも fanotify テクノロジーに対応している場合、本製品は fanotify を使用してシステムイベントをインターセプトします。OS が fanotify テクノロジーに対応していない場合、本製品はファイル脅威対策のためにシステムイベントをインターセプトする特殊なカーネルモジュールをコンパイルして使用します。必要なパッケージがすべてインストールされている場合、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。

- 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。

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。

ステップ 15： 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 アクセス制御システムがインストールされている場合に表示されます。

SELinux を Kaspersky Endpoint Security と連携するよう自動設定するには、 yes と入力します。本製品で SELinux を自動設定できない場合（たとえば、semanage ユーティリティが存在しない場合など）、ウィザード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 システムの自動設定を実行しない場合は、 no と入力します。

既定では、ウィザードにより yes が提示されます。

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手動で設定できます。

ステップ 16： アップデート元の設定

このステップは、Kaspersky Endpoint Security を標準モードまたは EDR Agent モードでインストールしている場合に表示されます。

定義データベースと機能のアップデート元を指定します。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。カスタムアップデート元のアドレスは、ローカルディレクトリ（例：/home/databases）またはリモートの HTTP サーバーまたは HTTPS サーバー（例：http://example.com/databases/）として指定できます。

ステップ 17：プロキシサーバーの設定

このステップは、Kaspersky Endpoint Security を標準モードまたは EDR Agent モードでインストールしている場合に表示されます。

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>://]<address of 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>@]<address of proxy server>:<port> - プロキシサーバーへの接続に認証が必要な場合。IPv6 アドレスを指定する場合は、角括弧で囲んで入力してください。

> 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。

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。

ステップ 18： 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、Kaspersky Endpoint Security を標準モードまたは EDR Agent モードでインストールしている場合に表示されます。

このステップでは、ウィザードにより、インストール直後にクライアントデバイスで本製品の定義データベースのアップデートタスクを実行するよう提示されます。

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。

既定では、ウィザードにより yes が提示されます。

［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。

ステップ 19： 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、Kaspersky Endpoint Security を標準モードまたは EDR Agent モードでインストールしている場合に表示されます。

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。

ステップ 20： 本製品のアクティベーション

このステップは、Kaspersky Endpoint Security を標準モードまたは EDR Agent モードでインストールしている場合に表示されます。

インストール直後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するか、ライセンス情報ファイルへ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。

自動モードで初期設定を実行する方法

1. 初期設定を含む設定情報ファイルを作成します。Kaspersky Security Center を使用した本製品のリモートインストールに使用される autoinstall.ini 設定情報ファイルから設定をコピーし、必要に応じて変更できます。

2. 設定情報ファイルで、次の必須設定を指定します：

   - 使用許諾契約書（EULA）とプライバシーポリシーへの同意：

     `EULA_AGREED=Yes`

     `PRIVACY_POLICY_AGREED=Yes`

     使用許諾契約書およびプライバシーポリシーの条件は、本製品の配布キットに含まれている license.<language ID> ファイルで確認できます：

     使用許諾契約書およびプライバシーポリシーの条件に同意しない場合、インストールプロセスは中止されます。

   - 既定では、Kaspersky Security Network アプリケーションは標準モードで使用されます。

本製品を EDR Agent モードで使用するには、次の設定を指定します：

```
ENDPOINT_AGENT_MODE=Yes
```

本製品を Light Agent モードで使用するには、次の設定を指定します：

```
KSVLA_MODE=Yes
```

- Kaspersky Security Network を使用するKaspersky Security Network の利用規約に同意するかどうかを指定します：

  ```
  USE_KSN=Yes|No
  ```

  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。Kaspersky Security Network に関する声明の条件に同意すると、拡張 KSN モードが有効になります。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 Security Network が有効になっている場合、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 は軽量版のマルウェア定義データベースを使用します。

- 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する設定：

  ```
  GROUP_CLEAN=Yes|No
  ```

3. 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を選択します。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インターセプトする場合は、次の値を設定します：

   ```
   INTERCEPTOR_MODE=UseUpdatableKernelModule
   ```

   既定では、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。

4. 本製品を標準モードまたは EDR Agent モードでインストールする場合は、次の設定を指定します：

   - プロキシサーバー設定。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：

     - `PROXY_SERVER=[<connection protocol>://]<address of proxy server>:<port>` - プロキシサーバーへの接続に認証が不要な場合。

     - `PROXY_SERVER=[<connection protocol>://][<user name>:<password>@]<address of proxy server>:<port>` - プロキシサーバーへの接続に認証が必要な場合。IPv6 アドレスを指定する場合は、角括弧で囲んで入力してください。

     > 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かどうかを指定します：

     ```
     USE_GUI=Yes|No
     ```

5. 本製品を Light Agent モードでインストールする場合は、次の設定を指定します：

   - 保護対象仮想マシンのロール：

     - `SERVER_MODE=Yes`：保護対象仮想マシンがサーバーとして使用される場合。

     - `SERVER_MODE=No`：保護対象仮想マシンがワークステーションとして使用される場合。

   - 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。一時仮想マシンの作成元とな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、次の値を設定します：

     `VDI_MODE=Yes`

6. 初期セットアップウィザードを開始します：

```
/opt/kaspersky/kesl/bin/kesl-setup.pl --autoinstall=<initial configuration file>
```

   ここで、`<initial configuration file>` 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。

リターンコードの確認

```
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。

4 本製品の状態チェック

これにより、Kaspersky Endpoint Security がインストールおよびアクティベートされ、本製品のデータベースがアップデートされています。インストール後、本製品は自動的に起動します。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

- 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。

標準モードにおけるデバイスの保護ステータスの確認

デバイスの保護ステータスを確認するには、次のコマンドを実行します：

```
kesl-control --app-info [--json]
```

ここで、 `--json` は、データを JSON 形式で出力することを意味します。 `--json` 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。

次の点を確認します：

- アプリケーションがアクティベートされていること（**アプリケーションのライセンスの情報** 行）。
- 定義データベースが最新であること（**定義データベースを読み込み済み** 行および **定義データベースの前回の公開日時** 行）。
- ファイル脅威対策が有効になっていること（**ファイル脅威対策** 行）。
- **アプリケーションのステータス** 行に OK が表示されていること。

  アプリケーションのステータス 行に、システムディレクトリに対する権限が不十分であるという情報が表示されている場合は、このデバイス上で次のディレクトリの権限をローカルで確認してください：/var/opt/kaspersky、/var/log/kaspersky、/opt/kaspersky。所有者が root であり、これらのディレクトリへの書き込みアクセス権が所有者にのみ付与されていることを確認してください。

EDR Agent モードにおけるデバイスの保護ステータスの確認

デバイスの保護ステータスを確認するには、次のコマンドを実行します：

```
kesl-control --app-info [--json]
```

ここで、 `--json` は、データを JSON 形式で出力することを意味します。 `--json` 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。

次の点を確認します：

- 本製品がアクティベートされていること（**EDR Expert（オンプレミス）のライセンスの情報** 行）
- 定義データベースが最新であること（**定義データベースを読み込み済み** 行および **定義データベースの前回の公開日時** 行）。
- アプリケーションが EDR エージェントモードで使用されていること（**Endpoint Detection and Response Agent モード** 行）。
- ポリシーで設定した連携について、「利用可能で実行中」ステータスが表示されていること。
- **アプリケーションのステータス** 行に OK が表示されていること。

  アプリケーションのステータス 行に、システムディレクトリに対する権限が不十分であるという情報が表示されている場合は、このデバイス上で次のディレクトリの権限をローカルで確認してください：/var/opt/kaspersky、/var/log/kaspersky、/opt/kaspersky。所有者が root であり、これらのディレクトリへの書き込みアクセス権が所有者にのみ付与されていることを確認してください。

Light Agent モードにおけるデバイスの保護ステータスの確認

1. 次のコマンドを実行します：

   ```
   kesl-control --ksvla-info
   ```

   アプリケーションが Light Agent モードで使用されていること（**仮想環境保護用 Light Agent モード** 行）。

2. ポリシーで、接続可能な SVM を検出するために Integration Server を選択している場合は、次のコマンドを実行します：

   ```
   kesl-control --viis-info
   ```

   Light Agent が Integration Server に接続されていること（**Integration Server への接続ステータス** 行）。

3. 次のコマンドを実行します：

   ```
   kesl-control --svm-info
   ```

   Light Agent が SVM に接続されていることを確認してください：接続が確立されている SVM に関する情報が表示されます。

4. 次のコマンドを実行します：

   ```
   kesl-control --app-info [--json]
   ```

   ここで、`--json` は、データを JSON 形式で出力することを意味します。`--json` 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。

   次の点を確認します：

   - Light Agent が、Kaspersky Security for Virtualization Light Agent のアクティベーションに使用されたライセンスに関する情報を受信していること（**アプリケーションのライセンスの情報** 行）。
   - 定義データベースが最新であること（**定義データベースを読み込み済み** 行および **定義データベースの前回の公開日時** 行）。
   - **アプリケーションのステータス** 行に OK が表示されていること。

     アプリケーションのステータス 行に、システムディレクトリに対する権限が不十分であるという情報が表示されている場合は、このデバイス上で次のディレクトリの権限をローカルで確認してください：/var/opt/kaspersky、/var/log/kaspersky、/opt/kaspersky。所有者が root であり、これらのディレクトリへの書き込みアクセス権が所有者にのみ付与されていることを確認してください。

役立つ記事

タスクが実行されない場合、またはポリシーが適用されない場合の対処方法

デバイスのステータスが次の場合の対処方法：「ポリシー設定が無効です。ポリシーが適用されていません。」

エラー：「アプリケーションは現在のバージョンの Kaspersky Security Center Web コンソールでサポートされていないか、アプリケーションの Web プラグインがインストールされていません」

GUI のインストール時に発生する問題のトラブルシューティング

インストールエラーコードの説明

Kaspersky Endpoint Security のインストール後に発生するエラー

Kaspersky Endpoint Security のインストールが完了したら、導入シナリオに戻り、「特定のオペレーティングシステムにおけるインストール後の追加設定手順」の手順から続行できます。

特定のオペレーティングシステムでインストール後に行う追加の設定手順

Kaspersky Endpoint Security のインストール用に環境を準備し、本製品をインストールした後、一部のオペレーティングシステムでは追加の設定が必要です。

本製品での動作のための SELinux の手動設定

お使いのオペレーティングシステムで SELinux アクセス制御システムが `Enforcing` モードで使用されている場合、既定では、インストール中に本製品で動作するよう自動的に設定されます。

本製品で 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）、ウィザード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。この場合、または自動設定を拒否した場合は、本製品の初期設定が完了した後、Kaspersky Endpoint Security と連携して動作するように SELinux システムを手動で設定します。

この設定には root 権限が必要です。

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 が有効になっている場合は、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、設定情報ファイル /etc/selinux/config で `SELINUX=permissive` を設定し、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「targeted」ポリシーではなくカスタム SELinux ポリシーを使用する場合は、SELinux ポリシーに従って、元の Kaspersky Endpoint Security 実行ファイルのそれぞれにラベルを割り当てます。

   ```
   semanage fcontext -a -t bin_t <executable file>
   restorecon -v <executable file>
   ```

ここで、`<executable file>` は次のとおりです：

- /var/opt/kaspersky/kesl/<ビルド番号_*>/opt/kaspersky/kesl/libexec/kesl
- /var/opt/kaspersky/kesl/<ビルド番号_*>/opt/kaspersky/kesl/bin/kesl-control
- /var/opt/kaspersky/kesl/<ビルド番号_*>/opt/kaspersky/kesl/libexec/kesl-gui
- /var/opt/kaspersky/kesl/<ビルド番号_*>/opt/kaspersky/kesl/shared/kesl
- /var/opt/kaspersky/kesl/<ビルド番号_*>/opt/kaspersky/kesl/bin/response

4. 次のタスクを実行します：

ファイル脅威対策 タスクを実行する

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

簡易スキャンタスクを実行する

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

> 今後実行する予定の Kaspersky Endpoint Security のタスクをすべて実行することを推奨します。

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。

audit.log ファイルを表示します

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

7. audit.log ファイルにエラーがある場合は、エラーを修正するために、ブロック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、今後実行する予定のすべてのタスクを再度開始します。

ブロック 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読み込みます：

```
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 Enforcing 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。

レスポンスアクション用の SELinux の設定

オペレーティングシステムで SELinux を `Enforcing` モードで使用する予定の場合、Detection and Response ソリューションとの連携時に対応アクションを実行するには、SELinux の設定を追加で管理する必要があります。

> この SELinux の設定には root 権限が必要です。

対応アクション用に SELinux を設定するには：

1. SELinux を Permissive モードに切り替えます：
   - SELinux が有効になっている場合は、次のコマンドを実行します：

     SELinux を Permissive モードに切り替えます

     ```
     setenforce Permissive
     ```

   - SELinux が無効になっている場合は、設定情報ファイル /etc/selinux/config で `SELINUX=permissive` を設定し、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. Detection and Response ソリューションとの連携の一環として使用する対応アクションを実行するには、すべてのタスクを実行します。
4. SELinux で［メモリダンプの取得］タスクおよび［プロセスメモリダンプの取得］タスクを使用してフォレンジック情報を収集するには、タスクで指定されている SMB サーバーへのアクセスを Kaspersky Endpoint Security に許可してください。
5. audit.log ファイルにエラーがないことを確認します。

   audit.log ファイルを表示します

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

6. audit.log ファイルにエラーが存在する場合は、ブロック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読み込み、エラーを修正してから、対応アクションのタスクを再度実行します。

   ブロック 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読み込みます：

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

7. SELinux を Enforcing モードに切り替えます。

   ```
   setenforce Enforcing
   ```

OSnova オペレーティングシステムでの本製品の起動の設定

アプリケーションをインストールした後、次の手順を実行して、アプリケーションとそのグラフィカルインターフェイスの起動を設定します：

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"` を設定してください。

2. `/etc/sysctl.d/30-disable-ptrace.conf` ファイルを開き、`kernel.yama.ptrace_scope=0` を設定してください。`kernel.yama.ptrace_scope` パラメータのその他の値は、Kaspersky Endpoint Security の動作に影響する可能性があります。詳細については、既知の問題点と制限事項セクションを参照してください。

3. プロセスメモリおよびカーネルメモリのスキャンを実行する場合は、カーネルで mprotect（または PaX）メモリ保護メカニズムを無効にする必要があります。これを行うには、カーネルのコマンドラインに `mprotect=off` オプションを追加します。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。

閉鎖ソフトウェア環境モードの ALT SP での本製品の起動の設定

本製品をインストールした後、次の手順を実行して本製品を起動します：

1. Kaspersky Endpoint Security のアップデート可能なコンポーネントに対して、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/<build number_*>/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 {} \;
```

2. 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対して、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/
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 {} \;
```

3. システムの署名を開始して、閉鎖ソフトウェア環境モードを有効にします：

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

4. 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、`lsm=integrity ima_hash=sha512 ima_appraise=enforce` の行が含まれている必要があります。

5. 定義データベースのアップデートタスクを実行します：

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

定義データベースのアップデートタスクの出力に *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。

6. 本製品を再起動します：

```
systemctl restart kesl
```

高速インストールスクリプトを使用した Kaspersky Security Center Linux への移行シナリオ

このシナリオでは、データを含むソリューションを新しい管理サーバーデバイスに移行する次のユースケースの例を示します：

- Kaspersky Security Center Windows（MS SQLおよびPostgreSQL）からKaspersky Security Center Linux（PostgreSQL）への移行。
- ハードウェア交換のためのKaspersky Security Center Linux（PostgreSQL）の移行。

新しい管理サーバーは、高速インストールスクリプトを使用して導入されます。

その他のデータ転送方法については、「Kaspersky Security Center Linux への移行」セクションで説明しています。

1 バックアップコピーを作成するための前提条件

この手順では、以前に設定した管理サーバーを、新しいKaspersky Security Center Linux管理サーバーへの移行に向けて準備する方法について説明します。準備プロセスには、次の手順が含まれます：

1. Kaspersky Security Center Linuxと互換性のあるバックアップコピーを作成するために、管理サーバーのバージョンを確認します。

   現在のすべてのバージョンの**Kaspersky Security Center Linux**では、アプリケーションを新しいバージョンにアップグレードする際のデータ移行がサポートされています。バックアップコピーは、同じ種類のDBMS内でのみ作成および復元できます。

   Kaspersky Security Center Windowsでは、**プロパティ → 全般 → バージョン**で管理サーバーのバージョンを確認する必要があります。バージョンが 15.1.0.22239 より古い場合は、Kaspersky Security Center Windows を最新バージョンにアップグレードしてください。

   Kaspersky Security Center for Windows を最新バージョンにアップグレードします。

   1. カスペルスキーのWebサイトで、インストール済みの管理サーバーのローカライズ言語に一致する配布パッケージをダウンロードします：`Version 15.1.0.22239 | Windows | Full distributive`

      実行ファイルは、次の名前で**ダウンロード**フォルダーに保存されます：`ksc_15.1_<build number>_full_<language>.exe`

2. 配布パッケージを管理サーバーにコピーします。

3. `ksc_15.1_<build number>_full_<language>.exe`実行ファイルを管理者として実行します。

4. 表示されたウィンドウで、**Kaspersky Security Center のインストール**リンクをクリックします。

   管理サーバーのセットアップウィザードが開始されます。

5. 使用許諾契約書とプライバシーポリシーの条項を確認します。使用許諾契約書およびプライバシーポリシーのすべての条項に同意する場合は、**次の文書をすべて確認し、理解した上で条項に同意します**セクションで、次のチェックボックスをオンにします：

   - **EULA の条項**
   - **データの取り扱い方法を記載しているプライバシーポリシー**

6. **管理サーバーと Web ベースのコンソールをアップグレード（推奨）** を選択して、次のステップに進みます。

7. 新しいバックアップコピーを作成するには、**データのバックアップコピーを作成する**オプションを選択し、バックアップウィザードの手順に従います。

8. ［**アップグレード**］をクリックします。

9. アップグレード中に、Web コンソールのインストールウィザードで、バージョンをアップグレードするためのすべての手順を確認します。

   管理サーバーのアップグレードのインストールには時間がかかります。インストールウィザードが完了した後、データベースの初期化が完了するまで、管理コンソールは接続を受け付けない場合があります。

10. アップグレードが完了するまでお待ちください。

2. 管理サーバーの証明書の要件への準拠を確認します。

   バックアップコピーを作成する前に、証明書にSubject Alternative Name（SAN）が含まれていることを確認する必要があります。含まれていない場合は、必ず証明書を置き換えてください。そうしないと、バックアップから復元した後に Web コンソールにログインできなくなります。

   証明書にサブジェクト代替名が含まれていることを確認するには：

   - Windows を実行しているデバイスの場合：

     a. 管理コンソールで、確認する管理サーバーを選択します。

     b. コンテキストメニューで、**プロパティ → 全般 → 管理サーバー証明書を表示**を選択します。

     c. ウィンドウが開きます。そのウィンドウで、**サブジェクト代替名**項目の値を確認します。

   - Linux デバイスの場合は、次のコマンドを実行します：

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   サブジェクト代替名に管理サーバーデバイスのドメイン名（DNS）が含まれていることを確認します。

   値にドメイン名（DNS）のない外部 IP アドレスのみが含まれている場合、または値がまったくない場合は、証明書をKaspersky Security Center Linux の要件を満たすものに手動で置き換えてください。klsetsrvcert ユーティリティを使用して、管理サーバーの共通証明書を置き換えます。

klsetsrvcert ユーティリティを使用した管理サーバーの共通証明書の置換

1. 次のコマンドを実行して、デバイスで開始日を後日に設定した新しい証明書を作成します：

   - Kaspersky Security Center Windows の場合：

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
     <oldksc.example.internal>" -o "RsaKeyLen:2048"
     ```

   - Kaspersky Security Center Linux の場合：

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
     ```

   ここで、`"<oldksc.example.internal>"` は管理サーバーへの接続に使用する FQDN です。

   > この値には IP アドレスを使用しないでください。

2. 次のコマンドを実行して、すべてのデバイスで新しい証明書の開始日を設定します：

   - Kaspersky Security Center Windows の場合：

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
     ```

   - Kaspersky Security Center Linux の場合：

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
     ```

   ここで、`"DD-MM-YYYY hh:mm"` は現在の日付から少なくとも 30 日後の日付です。既定では、新しい証明書（`CR`）の配布期間は 90 日です。

   > 設定した時刻になると、Web コンソールへのアクセスを復元して証明書をアップデートするには、Web コンソールを再インストールする必要があります。

3. 必要に応じて、新しい管理サーバーに移行した後、klmover ユーティリティを実行して、デバイスと管理サーバーの接続を復元します。デバイスが証明書の配布期間全体にわたって電源オフの状態だった場合、または管理サーバーに一度も接続したことがない場合は、このユーティリティの起動が必要になることがあります。

2 以前の管理サーバーのインストールのバックアップコピーの作成

Kaspersky Security Center Windows のバックアップコピーの作成

1. ［**スタートメニュー** → **Kaspersky Security Center** → **Kaspersky Backup Utility**］から、Kaspersky Security Center Linux のインストールフォルダーにある `klbackup.exe` ユーティリティを実行します。

   インストールウィザードが起動します。Server Core モードの Microsoft Windows では、klbackup ユーティリティのコンソール版を使用してください。

2. 最初のステップで、**管理サーバーのデータのバックアップを実行**を選択します。

3. **バックアップ設定**ステップで：

   a. **参照**ボタンをクリックし、バックアップコピーを既定のディレクトリとは別の場所に保存するための新しいフォルダー（例：`C:\kscbackups`）を作成します。

   b. Microsoft SQL Server を使用している場合、高速インストールスクリプトで使用するには、**データベースを移行する → Postgres に移行する**オプションを選択します。標準の方法で Kaspersky Security Center Linux を導入する場合は、データを MySQL/MariaDB データベースに移行することもできます。

   c. バックアップコピーにパスワードを設定して、データへの不正なアクセスから保護します。

4. バックアップコピーが作成されるまで待ってから、ユーティリティを終了します。

   指定したディレクトリに、バックアップのタイムスタンプが付いた新しいサブディレクトリが作成されます。

Kaspersky Security Center Linux のバックアップコピーの作成

1. 管理サーバーのデバイスで、コマンドラインから次のコマンドを実行します：

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path /root/kscbackups -use_ts
```

2. バックアッププロセスが完了するまで待ちます。

   `-path` オプションで指定したディレクトリに、バックアップのタイムスタンプが付いた新しいサブディレクトリが作成されます。

古い管理サーバーのバックアップコピーを作成した後、管理サーバーのデバイスを運用から外します。

管理サーバーのデバイスの運用停止

1. 取得したバックアップコピーを、データ移行のために管理者のデバイスにコピーします。

2. 管理サーバーのオペレーティングシステムをシャットダウンします。

3. ネットワークアダプターを企業ネットワークから取り外します。

4. Kaspersky Security Center Linux の新規インストールでデバイスの IP アドレスを再利用する予定がある場合は、その IP アドレスを解放します。

5. デバイスの電源が完全に切れていることを確認します。

古い管理サーバーがネットワーク上に残っていると、デバイス管理で障害が発生したり、新しい管理サーバーの Web コンソールのログインプロセスが中断されたりする可能性があります。また、ネットワークエージェントのインストールタスクが古いサーバーへの接続で開始される原因にもなります。

❸ 高速インストールスクリプトを使用した Kaspersky Security Center Linux の初期導入

このガイドでは、高速インストールスクリプトを使用して Kaspersky Security Center Linux インスタンスを初期導入する方法について説明します。

特記事項：

- Kaspersky Security Center のすべてのコンポーネントは、管理サーバーと同じデバイスにインストールされます。
- 管理サーバーのオペレーティングシステムは、次のいずれかである必要があります：
  - Astra Linux Special Edition RUSB.10015-01（運用アップデート 1.8.5）、PostgreSQL 15
  - Ubuntu Server 26.04 LTS、PostgreSQL 18
  - CentOS Stream 10 と PostgreSQL 18
  - RED OS 8.0 と PostgreSQL 16
- 高速インストールスクリプトで自動化されるのは、Kaspersky Security Center アプリケーションの設定とインストールのみです。管理者は、オペレーティングシステムでの管理サーバーデバイス名、オペレーティングシステムレベルでのネットワークアダプターとセキュリティファイアウォール、およびハードウェアを設定するための手順を実行する必要があります。

高速インストールスクリプトを使用して Kaspersky Security Center Linux のインスタンスを初期導入するには、次の手順を実行します：

1.導入の準備

インストール手順に進む前に、次のものを準備する必要があります：

- オペレーティングシステムのインストールディスクイメージ、アプリケーションパッケージのリポジトリ。
- Web コンソールへのログイン時に 二要素認証（2FA） を行うための認証アプリケーション。
- 新しい FQDN（例：*ksclinux.example.com*）。ソリューションの設定に関する十分な経験がある場合は、独自のスクリプトを使用して、インストール中に以前の FQDN を新しいサーバーに割り当てることができます。この場合、手順 5「バックアップコピーからの復元後のアプリケーションの設定」では、手順 4 を省略してください。管理対象デバイスの以前の管理サーバーの FQDN への接続の復元
- インターネット経由で配布パッケージをダウンロードし、Web コンソールを管理するための、ブラウザーを搭載した管理者のデバイス。
- アプリケーションコンポーネントが DNS とタイムサーバー（NTP）を利用できることを確認します。
- シナリオに応じて、管理対象デバイスの接続に以前の IP アドレスを使用していた場合は、その IP アドレスを解放してください。

- 要件に従って、ネットワーク機器とプロキシサーバーを設定します：
  - アプリケーションコンポーネント間の通信用ポート。
  - カスペルスキーサーバーへのアクセス。
  - ハードニングガイドの推奨事項。

2.オペレーティングシステムのサイジングと設定

1. 管理サーバーで管理するデバイスの数に応じて、機器を設定します。

   各サイジング計算では、カスペルスキーアプリケーションで使用可能なリソースが考慮されます。この計算では、管理サーバー、ネットワークエージェント、DBMS、Web コンソールサーバー、および Kaspersky Endpoint Security for Linux がすべて同じデバイスで動作することを考慮しています。ただし、この計算では、管理サーバーのバックアップコピーの保存は考慮されていません。

   > 別のデバイスにバックアップコピーを保存するためのマウントポイントとして外部ファイル共有を使用するか、バックアップの保存を考慮してハードディスクの空き容量の要件を増やしてください。

   オペレーティングシステム用に、4～6 GB の RAM と 20 GB のハードディスク空き容量を追加することを推奨します。

   管理対象デバイスの数に応じたデバイスのサイジング：

   - **S**（最大 1,000 台のデバイス）：CPU コア 8 個、RAM 16 GB、`/var` ディレクトリ用のハードディスク空き容量 70 GB、300 IOPS 以上。
   - **M**（最大 10,000 台のデバイス）：CPU コア 12 個、RAM 24 GB、`/var` ディレクトリ用のハードディスク空き容量 340 GB、300 IOPS 以上。
   - **L**（最大 30,000 台のデバイス）：CPU コア 20 個、RAM 40 GB、`/var` ディレクトリ用のハードディスク空き容量 490 GB、300 IOPS 以上。
   - **XL**（最大 50,000 台のデバイス）：CPU コア 28 個、RAM 54 GB、`/var` ディレクトリ用のハードディスク空き容量 640 GB、300 IOPS 以上。

2. 選択した仕様に従って、Kaspersky Security Center サーバーのハードウェアを準備します。

3. Kaspersky Security Center サーバーにオペレーティングシステムをインストールします。

   インストール時に、コマンドラインで管理サーバーがインストールされているデバイスをリモート管理する場合は、**SSH リモート接続ツール**オプションを有効にします。

   > Astra Linux は、**強制アクセス制御**オプションを無効にしてインストールする必要があります。また、Kaspersky Endpoint Security for Linux が正しく動作するように、**ptrace トレースをブロックする**オプションを無効にします。

4. 個別にマウントされている場合は `/var` ディレクトリの、そうでない場合はルートディレクトリ `/` のディスク空き容量を確認します。

   M 構成の例：

   Astra Linux

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                  Size  Used Avail Use% Mounted on
   ```

```
/dev/mapper/astra48242-01  406G  8,0G 377G    3% /
<...>
```

Ubuntu

```
administrator@ksclinux:~$ df -h
Filesystem                        Size  Used Avail Use% Mounted on
/dev/mapper/ubuntu--vg-ubuntu--lv  406G   11G  374G   3% /
<...>
```

5. 管理対象デバイスへの接続に IP アドレスを使用していた場合は、以前の管理サーバーの IP アドレスを新しいサーバーに設定します。

動画：オペレーティングシステムの設定

3.配布ファイルのダウンロード

1. 目的のロケール用の配布パッケージをカスペルスキーの Web サイトからダウンロードし、別のディレクトリ（例：*kscdistr*）に保存します。

   Ubuntu および Astra Linux の場合

   - 管理サーバーの deb 形式の配布パッケージ：

     `Version 16.3.0.1207 | Debian x64 | Administration server`

   - Web コンソールの deb 形式の配布パッケージ：

     `Version 16.3.0.1207 | Debian x64 | Web console`

   - 高速インストールスクリプト：

     `Version 16.3.0.1207 | Linux | KSC installation script`

   CentOS および RED OS の場合

   - 管理サーバーの rpm 形式の配布パッケージ：

     `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Administration server`

   - Web コンソールの rpm 形式の配布パッケージ：

     `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Web console`

- 高速インストールスクリプト：

  `Version 16.3.0.1207 | Linux | KSC installation script`

2. Astra Linux のクローズドソフトウェア環境モードでカスペルスキー製品が動作できるようにするには、公開鍵ファイル kaspersky_astra_pub_key.gpg をダウンロードします。

3. ダウンロードしたファイルを、リムーバブルメディアまたはネットワーク経由で、新しい Kaspersky Security Center 管理サーバー用デバイスにコピーします。

   以下は、コマンドラインを使用してネットワーク経由でコピーする手順です。

   > scp ユーティリティを使用してファイルをコピーできるかどうかは、管理サーバーデバイスのオペレーティングシステムで SSH サービスが実行されているかどうか、および組織のセキュリティポリシーによって異なります。

   a. コマンドラインで cd コマンドを使用して、*kscdistr* ディレクトリの 1 つ上の階層のディレクトリに移動します。例：

   Linux 向け

   ```
   cd /home/administrator/Desktop
   ```

   Windows 向け

   ```
   cd C:\Users\Administrator\Downloads
   ```

   b. scp ユーティリティを使用して、配布ファイルをネットワーク経由でコピーします：

   ```
   scp -r <kscdistr> <administrator>@<ksclinux.example.com>:
   ```

   説明：

   `<kscdistr>` は、Kaspersky Security Center のダウンロード済み配布パッケージを含むローカルディレクトリです。

   `<administrator>` は、新しい管理サーバー上で SSH 接続の使用を許可されているスーパーユーザーです。

   `<ksclinux.example.com>` は、新しい管理サーバーの FQDN アドレスです。

   ファイルは、指定したユーザーのホームディレクトリのルートにコピーされます。

4.インストール設定の構成

1. 新しい管理サーバー用デバイスで、スーパーユーザーとしてログインし、ターミナルを開きます。

2. コピーした配布パッケージがあるディレクトリに移動します。

   例

   ```
   cd ~/kscdistr
   ```

3. 高速インストールスクリプトのアーカイブを、配布ファイルがある現在のディレクトリに展開します。

例

```
tar -xf ./ksc_fast_install.tar.gz
```

4. 以下のコマンドを実行して、すべてのファイルが存在することを確認します：

```
ls -la
```

ls -la コマンドの出力例

```
administrator@ksclinux:~$ ls -la
drwxr-xr-x  3 administrator administrator      4096 jul 17 20:32 .
drwx------ 17 administrator administrator      4096 jul 17 17:54 ..
-rw-r--r--  1 administrator administrator       493 apr 20  2023 kaspersky_astra_pub_key.gpg
-rw-r--r--  1 administrator administrator 199128488 jul 10 21:38 ksc64_16.3.0-1207_amd64.deb
-rwxr-xr--  1 administrator administrator    143288 jul 22 17:22 ksc_fast_install.py
-rw-r--r--  1 administrator administrator 158144492 jul 10 21:37 ksc-web-console-16.3.12907.x86_64.deb
-rw-r--r--  1 administrator administrator     15561 jul 22 23:17 nwc_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 nwc_license.txt.sha256
-rw-r--r--  1 administrator administrator       493 jul 22 17:22 params.txt
-rw-r--r--  1 administrator administrator     70869 jul 22 23:17 server_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 server_license.txt.sha256
```

5. 配布ファイルがあるディレクトリで、インストールスクリプトの設定を含むテキストファイルを編集用に開きます。例：

```
nano ./params.txt
```

6. 事前に準備した値を設定し、該当する行の先頭のコメント文字（#）を削除するか、次の値を含む新しい行を追加します：

- 機器のサイジング（S/M/L/XL 構成の値）。

  例

  ```
  klfi_netsize=S
  ```

- ファイル内の 2 つの設定における管理サーバーの FQDN アドレス。

  ```
  klfi_klserver_address=ksclinux.example.com
  ```

  ```
  klfi_kliam_address=ksclinux.example.com
  ```

インストールされる管理サーバーの言語は、ダウンロードした配布パッケージのロケールによって異なります。

7. 新しい管理サーバーのオペレーティングシステムで、管理サーバーの FQDN がループバック IP アドレスに正しく名前解決されているかどうかを確認します。次の手順に従います：

   a. 新しい管理サーバーのアドレスを指定して `ping` コマンドを実行します。

   ループバック IP アドレスの取得に成功した例

   ```
   administrator@ksclinux:~$ ping ksclinux.example.com
   ping ksclinux.example.com
   PING ksclinux.example.com (127.0.1.1) 56(84) bytes of data.
   64 bytes from ksclinux.example.com (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
   ```

   b. アドレスが取得されなかった場合、または外部 IP アドレスが取得された場合は、新しい管理サーバー上のオペレーティングシステムの `/etc/hosts` ファイルに管理サーバーのアドレスを追加します。

   次の手順に従います：

   - 次のコマンドを実行して、`/etc/hosts` ファイルを編集用に開きます：

     ```
     sudo nano /etc/hosts
     ```

   - サーバーのアドレスとして、管理サーバー用デバイスの FQDN を入力します。例：

     ```
     127.0.0.1       localhost
     127.0.1.1       ksclinux.example.com ksclinux
     <...>
     ```

管理対象デバイスでは、管理サーバーの FQDN がサーバーの外部 IP アドレスに名前解決される必要があります。DNS サーバー上のレコードが正しく設定されていることを確認します。

5.高速インストールスクリプトの開始

高速インストールスクリプトを実行するには：

1. デバイスを再起動した後、配布パッケージがあるディレクトリに戻ります：

   ```
   cd ~/kscdistr
   ```

2. 次のコマンドを実行して、ファイルを実行可能にします：

   ```
   chmod +x ./ksc_fast_install.py
   ```

3. 高速インストールスクリプト自体は英語でのみ提供されているため、スクリプトを実行する前に、ご利用のローカライズ言語の使用許諾契約書をお読みください。

4. インストール中にパッケージをダウンロードできるように、ネットワークパッケージリポジトリをオペレーティングシステムまたはオペレーティングシステムのインストールディスクイメージに接続してください。

5. 高速インストールスクリプトを実行します：

   ```
   sudo ./ksc_fast_install.py
   ```

6. インストールウィザードの手順に従います。

> リソースチェックの手順で、スクリプトが RAM が不足していると誤って示した場合は、インストール中に動的 RAM 割り当てを無効にします。

7. インストールが完了するまで待ちます。スクリプトのテキスト出力から、Web コンソールのユーザー名（`User`）とパスワード（`Pass`）を保存します。

例

```
[+] Creating KSC user 'kscadmin' ...
[+] An internal user has been created:
[+]     User: kscadmin
[+]     Pass: ############
[!] If the password is lost, you must create a user by running the command:
        /opt/kaspersky/ksc64/sbin/kladduser -n <user>
[+] OK
[+] Success
```

動画：Ubuntu での高速インストールスクリプトの実行

6.Web コンソールへの初回ログイン

1. ブラウザーで Web コンソールのアドレスを開きます：`https://<FQDN>:8080`

   ここで、`<FQDN>` はインストールスクリプトの設定に含まれる管理サーバーのアドレスです。例：*https://ksclinux.example.com:8080*。

2. スクリプトの出力に表示されているユーザー名とパスワードを使用して、Web コンソールにログインします。

3. Authenticator アプリケーションを設定します：

   a. ワンタイム確認コードを取得するための秘密鍵をアプリケーションにコピーするか、Web コンソールの認証ウィザードから QR コードをスキャンします。

   b. 生成された確認コードを入力して認証を行い、Web コンソールにログインします。

4. ハードニングガイドを確認して承認します。

5. 管理サーバーのデータをバックアップコピーから復元する予定がない場合は、初期セットアップウィザードで管理サーバーを設定します。

4 管理サーバーのバックアップコピーの復元

Kaspersky Security Center Windows からの移行、または Kaspersky Security Center Linux のデータを新しいハードウェアに移行するシナリオでは、管理サーバーの古いインストール環境で作成されたバックアップコピーからデータを復元する必要がある場合があります。

> 新しいサーバー上の PostgreSQL のバージョンは、バックアップコピー内のバージョン以上である必要があります。

データを復元する必要がない場合は、この手順をスキップします。

バックアップコピーがまだ作成されていない場合：

- PostgreSQL データ形式の種別を使用して、古い管理サーバーのインストール環境のバックアップコピーを作成します。
- 新しい Kaspersky Security Center Linux サーバーをインストールし、Web コンソールに初めてログインします。

バックアップコピーから管理サーバーを復元するには、次の手順を実行します：

1.バックアップコピーの管理サーバーへの配置

リムーバブルメディアまたはネットワークを使用して、古い管理サーバーのバックアップコピーを新しい管理サーバーデバイスに配置します。

バックアップコピーをネットワーク経由で管理サーバーにコピーするには：

> scp ユーティリティを使用してファイルをコピーできるかどうかは、管理サーバーデバイスのオペレーティングシステムで SSH サービスが実行されているかどうか、および組織のセキュリティポリシーによって異なります。

1. コマンドラインで *cd* コマンドを使用して、以前の管理サーバーのバックアップファイルが格納されているディレクトリに移動します。例：

   Windows
   ```
   cd C:\kscbackups
   ```

   Linux
   ```
   cd /root/kscbackups
   ```

2. scp ユーティリティを使用して、バックアップファイルが含まれるディレクトリをコピーします：

   ```
   scp -r <klbackup202x-xx-xx> <administrator>@<ksclinux.example.com>:
   ```

   説明：

   `<klbackup202x-xx-xx>` は、バックアップファイルが保存されているディレクトリです。

   `<administrator>` は、新しい管理サーバー上で SSH 接続の使用を許可されているスーパーユーザーです。

`<ksclinux.example.com>` は、新しい管理サーバーの FQDN アドレスです。

バックアップコピーが含まれるディレクトリが、指定したユーザーのホームディレクトリにコピーされます。

2.バックアップからの復元手順

1. 新しい管理サーバーデバイスで、ターミナルを開きます。
2. バックアップコピーからデータを復元する際に、管理サーバーがデータベースへの接続に使用する標準の klserver アカウントと kliam アカウントに PostgreSQL のスーパーユーザー権限を付与します：

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
```

3. klbackup ユーティリティを使用して、古い管理サーバーのバックアップコピーからデータの復元を開始します：

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path </home/administrator/klbackup202x-xx-xx> -restore
```

ここで、`</home/administrator/klbackup202x-xx-xx>` はバックアップファイルが含まれるディレクトリへの完全パスです。

4. バックアップにパスワードが設定されていない場合は、バックアップのパスワードを求められたら、パスワードを入力せずに **Enter** キーを押します。
5. ユーティリティが終了するまで待ちます。

   大規模なインストール環境では時間がかかる場合があります。
6. 管理サーバーがデータベースへの接続に使用する PostgreSQL アカウントの元の権限を復元します。

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
```

5 バックアップコピーからの復元後のアプリケーションの設定

バックアップコピーからデータを復元していない場合は、この手順をスキップしてください。

バックアップコピーからの復元後のアプリケーションの設定には、次の手順が含まれます：

1.Web コンソールの復元

1. IAM サーバーの設定情報ファイルから古いサーバーのアドレスを取得します：

```
sudo grep "ksc_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

例

```
ksc_address: "oldksc.example.internal"
```

2. 古い管理サーバーの FQDN が、新しい管理サーバーのループバック IP アドレスに正しく解決されているかどうかを確認します。次の手順に従います：

   a. 古い管理サーバーのアドレスを指定して `ping` コマンドを実行します。

   ループバック IP アドレスの取得に成功した例

```
administrator@ksclinux:~$ ping oldksc.example.internal
ping oldksc.example.internal
PING ksclinux (127.0.1.1) 56(84) bytes of data.
64 bytes from ksclinux (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
```

   b. アドレスが取得されなかった場合、または外部 IP アドレスが取得された場合は、新しい管理サーバー上のオペレーティングシステムの `/etc/hosts` ファイルに管理サーバーのアドレスを追加します。次の手順に従います：

   - 編集するために /etc/hosts ファイルを開きます：

```
sudo nano /etc/hosts
```

   - 管理サーバーデバイスのアドレスの追加のエイリアスとして、古いサーバーの名前を入力します。

   例

```
127.0.0.1       localhost
127.0.1.1       ksclinux.example.com ksclinux oldksc.example.internal
<...>
```

3. Web コンソールを再インストールします：

   a. ローカルの Web コンソールサーバーをアンインストールします：

   Kaspersky Security Center Linux の配布パッケージに応じて、次のいずれかのコマンドを実行します：

   - Debian ベースの OS の場合：

```
sudo apt remove ksc-web-console -y
```

   - Red Hat Enterprise Linux ベースのオペレーティングシステムを実行しているデバイスの場合：

```
sudo dnf remove ksc-web-console -y
```

b. 配布パッケージが含まれるディレクトリから Web コンソールパッケージをインストールします：

- Debian ベースの OS の場合：

```
sudo apt install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.deb -y
```

- Red Hat Enterprise Linux ベースのオペレーティングシステムを実行しているデバイスの場合：

```
sudo dnf install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.rpm -y
```

2.Kaspersky Security Center Windows から移行する際の kscadmin ユーザーのアクセス権の復元

ユーザーデータベースが上書きされました。kscadmin ユーザーを再作成し、二要素認証を設定します。

1. 管理サーバーデバイスのオペレーティングシステムでターミナルを開き、ユーザーを作成するために次のコマンドを実行します：

```
sudo /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin
```

Enter キーを押した後、パスワードを入力し、もう一度入力します。

2. ブラウザーで Web コンソールのアドレスを開きます：

```
https://<FQDN>:8080
```

ここで、`<FQDN>` はインストールスクリプトの設定に含まれる管理サーバーのアドレスです。例：*https://ksclinux.example.com:8080*。

3. 作成したユーザー名とパスワードを使用して Web コンソールにログインします。

4. 認証アプリケーションを設定します。次の手順に従います：

   a. 管理サーバーのバックアップコピーを復元する前に、認証アプリケーションから古い kscadmin ユーザープロファイルを削除します。

   b. ワンタイム確認コードを取得するための秘密鍵をアプリケーションにコピーするか、Web コンソールの認証ウィザードから QR コードをスキャンします。

   c. 生成された確認コードを入力して認証を行い、Web コンソールにログインします。

3.管理サーバーのテスト

1. kscadmin およびその他のユーザーとしてログインした際に、Web コンソールのインターフェイスが正常に動作することを確認します。

2. 次のタスクを順に実行します：

- 管理サーバーのリポジトリへのアップデートのダウンロード
- 管理サーバーのメンテナンス
- 管理サーバーのデータバックアップ

タスクの設定内の Windows パスを、新しい管理サーバー上の Linux ディレクトリに置き換えるか、タスクを削除して最初から設定し直します。

3. タスクの結果を確認し、必要に応じて、タスクの設定、管理ポリシー、および管理サーバーの設定を変更します。

4.管理対象デバイスの以前の管理サーバーの FQDN への接続の復元

新しい管理サーバーに新しい FQDN（例：ksclinux.example.com）を割り当てた場合は、次のいずれかの種類の DNS レコードを追加してください：

- 古い管理サーバー名を新しい管理サーバー名に対応付ける CNAME レコード。

  必要なレコードの設定方法の詳細については、DNS サーバーのドキュメントを参照してください。

- 以前の管理サーバーのアドレスを新しい管理サーバーの IP アドレスに対応付ける A レコードおよび AAAA レコード。

  Windows Server ベースの DNS サービスの場合は、ご使用のインフラストラクチャに適用される値を使用してコマンドを実行します。

Windows Server ベースの DNS サービスに DNS A レコードを追加するには、ご使用のインフラストラクチャに適用される値を使用してコマンドを実行します：

1. DNS サーバーに接続します。

2. PowerShell を開き、次のコマンドを実行して既存の A レコードから IP アドレスを取得します：

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

3. 次のコマンドを実行して、A レコードの IP アドレスを変更します：

```
$OldKSC = Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration
server>"
```

```
$NewKSC = $OldKSC.Clone()
```

```
$NewKSC.RecordData.IPv4Address = [System.Net.IPAddress]::parse('<IP-address of the administration server>')
```

```
Set-DnsServerResourceRecord -OldInputObject $OldKSC -NewInputObject $NewKSC -ZoneName "<zone name>"
```

4. 次のコマンドを実行して、A レコード内の IP アドレスが更新されていることを確認します：

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

コマンドの出力には、Kaspersky Security Center Linux 管理サーバーの IP アドレスが含まれます。ローカル DNS キャッシュが更新されると、管理対象デバイスは再接続します。

6 管理サーバーのアンチウイルスによる保護の設定

管理サーバーにアンチウイルスによる保護を提供することに関するHardening Guide の推奨事項に準拠するには、管理サーバーにカスペルスキー製品をインストールし、管理ポリシーを設定します。Kaspersky Endpoint Security for Linux を導入するには、導入ガイドを参照してください。

インストールと設定は次の手順で構成されます：

1.別の管理グループの作成

1. Web コンソールのメインウィンドウで、［**資産管理**］→［**グループ階層構造**］の順に選択します。
2. **管理対象デバイス**グループの横にあるチェックボックスをオンにします。
3. ［**追加**］をクリックします。
4. 表示されたウィンドウで、新しいグループの名前を指定し（例：*kscserver*）、［**追加**］ボタンをクリックして作成を確定します。

2.設定を継承しないネットワークエージェントのポリシーの作成

1. Web コンソールのメインウィンドウで、［**アセット管理**］→［**ポリシー**］セクションに移動します。
2. ［**追加**］をクリックします。
3. 新規ポリシーウィザードで、**Kaspersky Security Center ネットワークエージェント**アプリケーションを選択し、［**次へ**］をクリックします。
4. ［**親ポリシーから設定を継承する**］オプションを無効にし、［**保存**］をクリックします。

3.Kaspersky Security Center から、または手動での Kaspersky Endpoint Security for Linux 管理プラグインのインストール

Kaspersky Endpoint Security for Linux 管理プラグインは、次の方法でインストールできます：

- Web コンソールで使用可能な配布パッケージのリストからインストールします。
- ファイルから手動でインストールします。

Web コンソールで使用可能な配布パッケージのリストから Kaspersky Endpoint Security 管理プラグインをインストールするには：

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

   インストールされている Web プラグインのリストが開きます。

2. ［**追加**］をクリックします。

   使用可能な管理プラグインのリストが開きます。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。

3. 使用可能なプラグインのリストで、Kaspersky Endpoint Security for Linux Web プラグインの使用可能な最新バージョンを選択してください。

4. 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。

5. 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。

新しいプラグインが、インストール済み Web プラグインのリストに表示されます。

動画：ウィザードを使用した管理 Web プラグインのインストール

ファイルから Kaspersky Endpoint Security 管理プラグインを手動でインストールするには：

1. Kaspersky Endpoint Security for Linux セクションのアプリケーションのダウンロードページから、Web プラグインを含むアーカイブをダウンロードします：**アプリケーションコントロールプラグイン → Web コンソールプラグイン**。

2. ダウンロードしたアーカイブをローカルで展開します。

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

   インストールされている Web プラグインのリストが開きます。

4. ［**リストから追加**］ボタンをクリックします。

5. ウィンドウが開きます。このウィンドウで、plugin.zip ファイルへのパスと signature.txt ファイルへのパスを指定します。

   これらのファイルは、Web プラグインのアーカイブを展開したフォルダーにあります。

6. ［**追加**］をクリックします。

7. 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。

新しいプラグインが、インストール済み Web プラグインのリスト（［**設定 → Web プラグイン**］）に表示されます。

動画：隔離されたネットワークでの管理 Web プラグインのインストール

4.設定を継承しない Kaspersky Endpoint Security for Linux のポリシーの作成

Kaspersky Endpoint Security for Linux を Kaspersky Security Center Linux と併用する場合は、カスペルスキーのエキスパートによる推奨事項に従ってポリシー設定を管理する必要があります。

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. 管理サーバーの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 for Linux を選択します。
5. Kaspersky Endpoint Security for Linux アプリケーションの **標準モードまたは Endpoint Detection and Response Agent モード** を指定します。
6. Kaspersky Security Network に参加するかどうかを決定します。
7. 管理対象デバイスの最適化に関する推奨事項を確認します。
8. ポリシー名で、そのポリシーが管理サーバーに属していることを示します。
9. **親ポリシーから設定を継承する** オプションを無効にします。
10. 変更内容を保存します。

動画：ポリシーの作成

5.Kaspersky Endpoint Security for Linux の Update グループタスクの作成

1. Web コンソールのメインウィンドウで、［**タスク**］セクションを選択します。
2. 管理サーバーの管理グループを選択します。
3. ［**追加**］をクリックします。
   タスク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 for Linux を選択します。
5. *Update* タスク種別を指定し、設定を変更せずに次の手順に進みます。
   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 → アップデート元**］セクションで、Kaspersky Security Center のソースを有効にし、優先度を上げます。

隔離されたネットワークでは、Kaspersky Update Utility を使用して、アップデートタスク用のリポジトリを作成します。

動画：定義データベースの集中アップデートの設定

6.管理サーバーのストアへのライセンスの追加（ライセンスの自動配布機能を使用）

1. Kaspersky Security Center Web コンソールのメインウィンドウで、［**ライセンス**］セクションに移動します。

2. ［**追加**］をクリックします。

3. ［**アクティベーションコード**］オプションを指定し、［**送信**］をクリックします。

   隔離されたネットワークでは、https://keyfile.kaspersky.com/en-US サービスを使用してリクエストできるライセンス情報ファイルを使用します。

4. ライセンスのリストで、ライセンスの名前をクリックします。

5. ［**管理対象デバイスにライセンスを自動配信する**］チェックボックスをオンにします。

6. 変更内容を保存します。

動画：アクティベーションコードで本製品をアクティベートする

動画：ライセンス情報ファイルで本製品をアクティベートする

7.ネットワークエージェントおよびKaspersky Endpoint Security for Linuxのインストールパッケージの作成

1. Web コンソールのメインウィンドウで、［**ソフトウェア管理**］→［**インストールパッケージ**］の順に選択します。

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. ［**カスペルスキー製品のインストールパッケージを作成する**］を選択します。

4. アプリケーションのリストで、Kaspersky Endpoint Security for Linux の最新バージョンを見つけて、その名前をクリックします。

5. サイドバーで、［**ダウンロードしてインストールパッケージを作成**］をクリックしてダウンロードを開始します。

   アプリケーションの使用を開始するには、使用許諾契約書を確認して同意します。

6. アプリケーションのリストに戻り、Linux 用ネットワークエージェントの最新バージョンをダウンロードします。

   アプリケーションの使用を開始するには、使用許諾契約書を確認して同意します。

7. Web コンソールのメインウィンドウにあるダウンロード済みアプリケーションのリストで、アプリケーションの名前をクリックします。

隔離されたネットワークでは、カスペルスキーの Web サイトから配布パッケージをダウンロードし、新規パッケージウィザードで［**インストールパッケージをファイルから作成する**］オプションを選択します。

動画：Kaspersky Security Center でのインストールパッケージの自動作成

動画：Kaspersky Security Center でのインストールパッケージの手動作成

8.Linux 用ネットワークエージェントのインストール

1. Web コンソールのメインウィンドウで、［**ソフトウェア管理**］→［**インストールパッケージ**］の順に選択します。

2. ［**カスペルスキー ネットワークエージェント for Linux**］パッケージの横にあるチェックボックスをオンにします。

3. ［**展開**］をクリックします。

   保護機能の導入ウィザードが開始されます。

4. ［**スタンドアロンパッケージを使用する**］オプションを選択します。

5. ［**デバイスを管理対象デバイスフォルダーに移動**］ステップで、デバイスを管理グループに移動するルールの設定をスキップします。このオプションは、管理サーバーのデバイスには適用されません。

6. ［**スタンドアロンインストールパッケージ作成の結果**］ステップで、アプリケーションのインストールスクリプトへの完全パスを選択してコピーします。

7. 管理サーバーのオペレーティングシステムで、コマンドラインを開きます。

8. スタンドアロンパッケージのインストールを開始します：

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   ここで、`</var/opt/.../stand-alone_package_sh>`は、事前にコピーした、アプリケーションのスタンドアロンインストールパッケージのスクリプトファイルへの完全パスです。

   インストールが成功すると、対応する通知が表示されます。

9. 管理サーバーのデバイス（例：*ksclinux*）を、［**管理対象デバイス**］グループから、事前に準備した管理グループ（例：*kscserver*）に移動します。

9.Kaspersky Endpoint Security for Linux のインストール

1. Web コンソールのメインウィンドウで、［**ソフトウェア管理**］→［**インストールパッケージ**］の順に選択します。

2. Kaspersky Endpoint Security for Linux パッケージの横にあるチェックボックスをオンにします。

3. ［**展開**］をクリックします。

   保護機能の導入ウィザードが開始されます。

4. ［**スタンドアロンパッケージを使用する**］オプションを選択します。

5. ［**スタンドアロンインストールパッケージ作成の結果**］ステップで、アプリケーションのインストールスクリプトへの完全パスを選択してコピーします。

6. 管理サーバーのオペレーティングシステムで、コマンドラインを開きます。

7. スタンドアロンパッケージのインストールを開始します：

```
sudo bash "</var/opt/.../stand-alone_package_sh>"
```

   ここで、`</var/opt/.../stand-alone_package_sh>`は、事前にコピーした、アプリケーションのスタンドアロンインストールパッケージのスクリプトファイルへの完全パスです。

   インストールが成功すると、対応する通知が表示されます。

8. Web コンソールのメインウィンドウの［**タスク**］セクションで、管理グループのリストにある、管理サーバーの名前が付いたルートノードを選択します。

9. 管理サーバーのタスクのリストから、以下のタスクを順に開始します：

   - 管理サーバーのリポジトリへのアップデートのダウンロード
   - Update（Kaspersky Endpoint Security for Linux）

10. Web コンソールのメインウィンドウで、［**アセット管理**］ → ［**アセット（デバイス）**］の順に選択します。

11. 管理サーバーのデバイスオブジェクトの名前をクリックします。

12. デバイスの状態を示す主な指標を確認します：

    - 定義データベースの前回のアップデート（現在）。
    - 管理サーバーに接続済み（現在）。
    - 保護ステータス（実行中）。
    - *ライセンスが追加されました*イベント（あり）。

ネットワーク内のデバイスにセキュリティソリューションを導入するには、Kaspersky Endpoint Security for Linux 導入ガイドを使用します。

旧バージョンからの本製品のアップデート

Kaspersky Endpoint Security は、保護対象デバイスに本製品の新しいバージョンをリモートまたはローカルでインストールすることにより、アップグレードできます。

Kaspersky Endpoint Security 12.4 for Linux からのみ、Kaspersky Endpoint Security 12.5 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 12.5 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 12.5 for Linux をインストールする必要があります。

アプリケーションをアップグレードするには、以下の手順に従ってください。

1 環境の準備

Kaspersky Endpoint Security のアップグレードを開始する前に、インフラストラクチャに応じて必要な準備手順を完了してください。

2 配布パッケージの準備

オペレーティングシステム、そのアーキテクチャ、CPU の種類に応じて配布パッケージを選択します。

3 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します。

4 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本製品の新しいバージョンをインストールします。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 EDR 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します。

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グレードする
- 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

コマンドラインを使用して RPM パッケージからアプリケーションをアップグレードする方法

コマンドラインでアプリケーションをアップグレードすることは、デバイスに新しいバージョンのアプリケーションをインストールすることと同じです。

アプリケーションをアップデートするには、root 権限が必要です。

アプリケーションをアップグレードするには、次のコマンドを実行します：

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] rpm -U --replacefiles --replacepkgs kesl-12.5.0-<build number>.<arch>.rpm [kesl-gui-12.5.0-<build number>.<arch>.rpm]
```

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

記号

コマンドオプション

設定	説明
KESL_EULA_AGREED=yes	使用許諾契約書の利用条件に同意します。
KESL_PRIVACY_POLICY_AGREED=yes	プライバシーポリシーの条件に同意します。
KESL_USE_KSN=yes/no	Kaspersky Security Network の使用： yes – Kaspersky Security Network に関する声明の条項に同意し、Kaspersky Security Network の使用を有効にします。 no – Kaspersky Security Network に関する声明の条項に同意せず、Kaspersky Security Network の使用を無効にします。
<arch>	アーキテクチャの種類： 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

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-12.5.0-<build number>.x86_64.rpm kesl-gui-12.5.0-<build number>.x86_64.rpm
```

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。

コマンドラインを使用して DEB パッケージからアプリケーションをアップグレードする方法

コマンドラインでアプリケーションをアップグレードすることは、デバイスに新しいバージョンのアプリケーションをインストールすることと同じです。

アプリケーションをアップデートするには、root 権限が必要です。

アプリケーションをアップグレードするには、次のコマンドを実行します：

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] apt-get install ./kesl_12.5.0-
```

```
<build number>_<arch>.deb [./kesl-gui_12.5.0-<build number>_<arch>.deb]
```

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

記号

コマンドオプション

設定	説明
KESL_EULA_AGREED=yes	使用許諾契約書の利用条件に同意します。
KESL_PRIVACY_POLICY_AGREED=yes	プライバシーポリシーの条件に同意します。
KESL_USE_KSN=yes/no	Kaspersky Security Network の使用： yes – Kaspersky Security Network に関する声明の条項に同意し、Kaspersky Security Network の使用を有効にします。 no – Kaspersky Security Network に関する声明の条項に同意せず、Kaspersky Security Network の使用を無効にします。
<arch>	アーキテクチャの種類： 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

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 DEB 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 apt-get install ./kesl_12.5.0-<build number>_amd64.deb [./kesl-gui_12.5.0-<build number>_amd64.deb]
```

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。

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

任意の手順です。Kaspersky Security Center を使用して Kaspersky Endpoint Security を一元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します。アップグレードは、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。詳細については、Kaspersky Security Center のヘルプを参照してください。

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。

旧バージョンのアプリケーションをアップグレードする際の特徴

- 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。

- `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。

  `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。

- 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。ユーザー契約書の本文は、カスペルスキーの Web サイト（**EULA**セクション）および `~/.kesl/12.5/license.<language ID>` ディレクトリで確認できます。

  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。Kaspersky Security Network に関する声明の本文は、~/.kesl/12.5/ksn_license.<言語 ID> で確認できます。Kaspersky Security Network の使用を拒否しても、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。

- 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ログファイルが、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 EDR 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 MMC 管理プラグイン

管理 Web プラグインのインストール方法

Web プラグインは、次の方法でインストールできます：

- 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 コンソールのクイックスタートウィザードについて詳しくは、Kaspersky Security Center ヘルプ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ファイルから配布キットを使用して手動でインストールできます。

Kaspersky Security Center から Kaspersky Endpoint Security の Web プラグインを手動でインストールするには：

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. [**追加**] をクリックします。

   使用可能な管理プラグインのリストが開きます。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。

3. 使用可能なプラグインのリストで、**Kaspersky Endpoint Security <version number> for Linux** Web プラグインを選択します。

4. 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。

5. 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。

新しいプラグインが、インストール済み Web プラグインのリスト（[**設定**] → [**Web プラグイン**]）に表示されます。

ファイルから Kaspersky Endpoint Security の Web プラグインを手動でインストールするには：

1. **Kaspersky Endpoint Security for Linux** セクションのアプリケーションのダウンロードページ（**追加の配布パッケージ → Web コンソールプラグイン**）から、Web プラグインを含むアーカイブをダウンロードします。

2. ダウンロードしたアーカイブをローカルで展開します。

3. 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。

4. ［**リストから追加**］ボタンをクリックします。

5. ウィンドウが開きます。このウィンドウで、plugin.zip ファイルへのパスと signature.txt ファイルへのパスを指定します。これらのファイルは、Web プラグインのアーカイブを展開したフォルダーにあります。

6. ［**追加**］をクリックします。

7. 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。

MMC 管理プラグインのインストール方法

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：

1. **Kaspersky Endpoint Security for Linux** セクションのアプリケーションのダウンロードページ（**ビルド → 管理プラグイン**）から klcfginst.msi ファイルをダウンロードします。

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、klcfginst.msi ファイルを実行します。

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を開き、**プロパティ**を選択します。

   - ［**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**］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**

ポリシーおよびタスクの変換

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には、「*<元のポリシーまたはタスクの名前>（変換済み）*」という名前が付けられます。

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。

Kaspersky Security Center Web コンソールでは、ポリシーとタスクを変換できません。

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。

管理プラグインに関する特記事項

- 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。

アップグレード後の本製品の設定

Kaspersky Security Center 管理コンソールを使用して本製品を管理している場合、新しいバージョンで以前のバージョンの本製品に指定されていたポリシー設定の値を使用するように、*ポリシーを変換*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）。

Kaspersky Security Center Web コンソールではポリシーを変換できません。

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。

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。

コマンドラインで本製品をアップデートすると、`UseKSN` 設定は次のように変更されます：

- アップグレード中に `KESL_USE_KSN=No` を設定した場合、`UseKSN=No` になります。
- アップグレード中に `KESL_USE_KSN=Yes` を設定した場合、`UseKSN=Extended` になります。
- 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。

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：

- 管理コンソールまたは Web コンソールで、［**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。
- コマンドラインで次の設定を行います：

```
UseKSN=<Basic|Extended>
CloudMode=Yes
```

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。

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。

Endpoint Detection and Response Expert 連携設定

新しいバージョンの本製品では、Kaspersky Endpoint Detection and Response Expert（クラウド）との連携モードが提供されます。

Kaspersky Endpoint Security for Linux と Kaspersky Endpoint Detection and Response Expert（クラウド）の連携機能は、現在一時的にご利用いただけません。この機能は 2026 年末までにサポートされる予定です。アプリケーションのアップグレードと新機能について知るには、リリースノートを確認してください。

MMC プラグインでポリシーを変換すると、Endpoint Detection and Response Expert（クラウド）との連携が無効になります（**Endpoint Detection and Response Expert（クラウド）を有効にしてください** チェックボックスはオフになります）。本製品は Endpoint Detection and Response Expert（オンプレミス）との連携を使用します。

コマンドラインで本製品をアップデートすると、`EDR_EXPERT_CLOUD_MODE` は次のように設定されます：`EDR_EXPERT_CLOUD_MODE=No`（既定値）。

ユーザー権限の設定

新しいバージョンの本製品は、パスワードによる保護に対応しています。

MMC プラグインでポリシーを変換すると、パスワードによる保護が無効になります。

コマンドラインを使用して本製品をアップグレードすると、ユーザー権限は、以前のバージョンの本製品で設定されていたユーザーロール（*kesladmin*、*kesluser*、*keslaudit*、*nokesl*）に従って保持されます。

本製品のアンインストール

Kaspersky Endpoint Security をアンインストールするには、以下の手順に従ってください。

Kaspersky Endpoint Security for Linuxの削除に関する特別な考慮事項

- 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。
- アプリケーションをアンインストールすると、インストールされていたアプリケーション証明書を含め、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。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。一意のコンピューター 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。

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を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

> アンインストールには root 権限が必要です。

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。

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したアプリケーションとグラフィカルインターフェイスをアンインストールします

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

DEB パッケージからインストールしたアプリケーションとグラフィカルユーザーインターフェイスをアンインストールします

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

グラフィカルインターフェイスを使用せずに使用していたアプリケーションパッケージの削除

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削除してください。

```
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削除してください。

```
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したアプリケーションのグラフィカルインターフェイスをアンインストールします

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

DEB パッケージからインストールしたアプリケーションのグラフィカルインターフェイスをアンインストールします

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

アンインストールはバックグラウンドで実行されます。

❷ 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

アンインストールには root 権限が必要です。

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。

32 ビットオペレーティングシステムに RPM パッケージからインストールしたネットワークエージェントをアンインストールします

```
rpm -e klnagent
```

64 ビットオペレーティングシステムに RPM パッケージからインストールしたネットワークエージェントをアンインストールします

```
rpm -e klnagent64
```

32 ビットオペレーティングシステムに DEB パッケージからインストールしたネットワークエージェントをアンインストールします

```
apt-get purge klnagent
```

64 ビットオペレーティングシステムに DEB パッケージからインストールしたネットワークエージェントをアンインストールします

```
apt-get purge klnagent64
```

❸ 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。

Kaspersky Endpoint Security MMC 管理プラグインを削除する方法

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。

Kaspersky Endpoint Security Web プラグインを削除する方法

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. ［**Kaspersky Endpoint Security <version number> for Linux**］チェックボックスをオンにします。

3. ［**削除**］をクリックします。

   Web プラグインのアンインストールを確認します。

本製品の使用

既定では、Kaspersky Endpoint Security 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。

本製品を既定の設定で起動すると、次のコンポーネントが起動します：

- 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、追加機能（本製品のアクティベーション機能とバックアップ機能）を動作させるために、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。PS 実行モードで中断されたユーザータスクは、中断した時点から再開されません。次回の本製品の起動時に、このようなタスクは中断した時点から再開されず、最初から実行されます。タスクの種別について詳しくは、「Kaspersky Endpoint Security のローカルタスク」セクションを参照してください。

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。

Web コンソールを使用して本製品を起動または停止する方法

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）**］→［**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て本製品を起動または停止する方法

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：

   – 本製品を起動します。

   – 本製品を停止します。

   コンテキストメニューから本製品を管理することもできます。

コマンドラインを使用して本製品を起動または停止する方法

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

systemd を使用するオペレーティングシステム

本製品を起動します

```
systemctl start kesl
```

本製品を停止します

```
systemctl stop kesl
```

本製品を再起動します

```
systemctl restart kesl
```

本製品の現在のステータスを表示します

```
systemctl status kesl
```

init を使用するオペレーティングシステム

本製品を起動します

```
service kesl start
```

本製品を停止します

```
service kesl stop
```

本製品を再起動します

```
service kesl restart
```

本製品の現在のステータスを表示します

```
service kesl status
```

ライセンス管理

*ライセンス*とは、Kaspersky Endpoint Security の期間限定の使用権であり、使用許諾契約書に基づいて付与されます。使用可能な機能のリストと製品の有効期間は、製品が使用されるライセンスによって異なります。

ライセンス種別

無料

- *試用版* – 製品をお試しいただくための無償ライセンス。

  試用版ライセンスの有効期間は短く設定されています。試用版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。

  試用版ライセンスでアプリケーションをアクティベートできるのは一度だけです。本製品を製品版ライセンスでアクティベートすると、以降は試用版ライセンスでアクティベートできません。

- *Kaspersky Security Center Cloud コンソールの試用版ライセンス*は、Cloud コンソールの評価を目的としたライセンスです。このライセンスでは、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。

> 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。

有料

- *製品版* - 本製品の購入時に提供される有償ライセンス。

  製品版ライセンスの有効期限が切れると、本製品の主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。

- *定額制サービス* とは、アプリケーションを 購入するための 注文であり、特定の パラメータ（定額制サービスの有効期限、保護対象デバイスの数）を 含みます。お住まいの地域のサービスプロバイダーから定額制サービスを購入できます。

  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。期限付き月額制サービスの有効期間が終了した後、契約更新の猶予期間がある場合、製品は機能し続けます。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。

  サービスプロバイダーの Web サイトで、解約を含む定額制サービスの管理を行うことができます。

ライセンスの仕組み

1. **アクティベーションコードを受け取ります**

   カスペルスキーのソリューションをカスペルスキー公式 Web サイトまたは当社のパートナーから購入すると、購入時に指定したメールアドレスにメッセージが届きます。このメッセージには、アクティベーションコードと、ライセンス情報ファイルの入手方法に関する情報が記載されています。組織で、コードを使用したアプリケーションのオンラインアクティベーションがサポートされていない場合、ライセンス情報ファイルが必要になることがあります。

   > Kaspersky Endpoint Security の定額制サービスを購入した場合、サービスプロバイダーから提供されるのはアクティベーションコードのみです。

2. **製品のアクティベーション**

   次に、アプリケーションをアクティベートする、つまりアプリケーションのライセンスを有効な状態にする必要があります。これを行うには、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を使用して、ライセンスをアプリケーションに追加する必要があります。

   次のアクティベーション方法が用意されています：

   - Kaspersky Security Center を使用してリモートで
   - コマンドラインで操作
   - グラフィカルインターフェイスを使用して

標準モード

アプリケーションを標準モードで使用するには、対象となる機能範囲が異なるライセンスを使用できます。一部のコンポーネントがライセンスの対象に含まれていない場合、別のライセンスが必要になることがあります：

- Kaspersky EDR Optimum コンポーネントをアクティベートするための Kaspersky Endpoint Detection and Response Optimum Add-on ライセンス（以下、「*EDR Optimum ライセンス*」とも表記）
- Kaspersky Unified Monitoring and Analysis Platform 機能との連携をアクティベートするための Kaspersky Unified Monitoring and Analysis Platform Add-on ライセンス（以下、「*KUMA ライセンス*」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 Kaspersky Managed Detection and Response Optimum/Expert Add-on ライセンス（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ための Kaspersky Endpoint Detection and Response Expert（オンプレミス）Add-on ライセンス（以下、「*EDR Expert（オンプレミス）ライセンス*」とも表記）
- EDR Expert（クラウド） コンポーネントをアクティベートするための Kaspersky Endpoint Detection and Response Expert（クラウド）Add-on ライセンス（以下、「*EDR Expert（クラウド）ライセンス*」とも表記）
- システム変更監視およびコンテナスキャンコンポーネントをアクティベートするための Kaspersky Workload Security Module Add-on ライセンス（以下、「*KWSM ライセンス*」とも表記）

これらのコンポーネントがライセンスの対象に含まれていない場合、Kaspersky Endpoint Security アプリケーション自体をアクティベートした後でのみ、これらのコンポーネントをアクティベートできます。

EDR Agent モード

Kaspersky Endpoint Security アプリケーションを EDR Agent モードで使用している場合、アクティベートするには EDR Expert（オンプレミス）ライセンスが必要です。

Light Agent モード

Kaspersky Endpoint Security を Light Agent モードで使用している場合、アプリケーションにライセンスを追加する必要はありません。Kaspersky Security for Virtualization Light Agent は Protection Server 側でアクティベートします。

Endpoint Detection and Response Optimum コンポーネントおよびカスペルスキーのソリューションとの連携用コンポーネントも、Protection Server 側でアクティベートされます。

アプリケーションのアクティベーションに関する問題のトラブルシューティング

3 ライセンスまたは定額制サービスの更新

ライセンスまたは定額制サービスを期限内に更新できるよう、有効期限に注意することをお勧めします。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更新することを推奨します。

ライセンスを期限内に更新するには、予備のライセンスを使用できます。サービスプロバイダーの Web サイトで、定額制サービスを手動または自動で更新できます。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。

ライセンスの追加時の注意事項

- 試用版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。
- 予備のライセンスの有効期限は、現在のライセンスの有効期限より後である必要があります。

- アプリケーションに現在のライセンスと予備のライセンスの両方が追加されている場合に新しい現在のライセンスを追加すると、以前に追加された現在のライセンスは新しいライセンスに置き換えられます。新しい予備のライセンスを追加すると、以前に追加された予備のライセンスは新しい予備のライセンスに置き換えられます。

- アプリケーションに現在のライセンス、Endpoint Detection and Response Optimum コンポーネントをアクティベートするためのライセンス、およびカスペルスキーのソリューションとの連携用コンポーネントをアクティベートするためのライセンスが追加されており、Endpoint Detection and Response Optimum コンポーネントと連携用コンポーネントも対象に含む予備のライセンスを 1 つ追加した場合、現在のライセンスの有効期限が切れると、予備のライセンスが現在のライセンスとなり、その他の現在のライセンスを解放します。その後、これらのライセンスを使用して、別のデバイスで Endpoint Detection and Response Optimum コンポーネントと連携コンポーネントをアクティベートできます。

4. **追加済みのライセンスに関する情報の表示**

   Kaspersky Security Center を使用してリモートから、または保護対象デバイスでコマンドラインまたはグラフィカルインターフェイスを使用してローカルに、本製品に追加されたライセンスに関する情報を表示できます。

役立つ記事

使用許諾契約書

*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。

  アプリケーションのインストールパッケージを作成する際（Kaspersky Security Center を使用してインストールする場合）、またはアプリケーションの初期設定時（コマンドラインを使用してインストールする場合）に、使用許諾契約書およびプライバシーポリシーの諸条件に同意することを確認すると、使用許諾契約書およびプライバシーポリシーの諸条件に同意したものとみなされます。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、アプリケーションのインストールをキャンセルする必要があり、アプリケーションを使用することはできません。

- 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。

アクティベーションコード

*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

*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を使用してアプリケーションをアクティベートする場合、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いて、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します。

識別 ID

*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。

現在アプリケーションのアクティベーションに使用されているライセンスが、*現在のライセンス*になります。現在のライセンスとして、試用版ライセンス、製品版ライセンス（商用ライセンス）、または定額制サービスのライセンスを追加できます。

予備のライセンス

*予備のライセンス*は、製品を使用するユーザーに権利を与えるもので、現在使用されていないライセンスです。現在のライセンスの有効期間が終了すると、予備のライセンスが自動的に現在のライセンスとなります。予備のライセンスは、現在のライセンスを追加した後でのみ追加できます。

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。

カスペルスキーの別のソリューションに切り替える方法

アプリケーションが Light Agent モードで使用されている場合、ライセンスは Kaspersky Security for Virtualization Light Agent ソリューションで管理されます。

組織にカスペルスキーソリューションが導入されており、Kaspersky Endpoint Security が標準モードまたは EDR Agent モードで使用されていて、別のカスペルスキーソリューションに切り替える必要がある場合は、次の手順に従います。

1. **新しいライセンスを準備する**

   別のカスペルスキーソリューションをカスペルスキーの Web サイトまたは当社のパートナーから購入します。ご購入時に指定したメールアドレスにメールが届きます。このメッセージには、アクティベーションコードと、ライセンス情報ファイルの入手方法に関する情報が記載されています。

   以前にアクティベーションコードを使用して Kaspersky Endpoint Security をアクティベートした場合、今回もアクティベーションコードを使用する必要があります。以前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した場合、ライセンス情報ファイルを使用する必要があります。

2. **ライセンスを置き換える**

   ライセンスは次のいずれかの方法で置き換えることができます：

   - Kaspersky Security Center を使用してリモートでアップデートする。ライセンスを管理サーバーのリポジトリに追加し、保護対象デバイスに配信します。
   - コマンドラインで次のコマンドを使用します：`kesl-control [-L] --add-active-key <path to key file / activation code>`。
   - グラフィカルインターフェイスで、本製品に現在適用されているライセンスを削除し、新しいライセンスを追加します。

3. **ライセンスが正常に置き換えられたことを確認する**

   そのためには、保護対象デバイスで使用されているライセンスの詳細を表示します。

役立つ記事

アクティベーションコード

*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

*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を使用してアプリケーションをアクティベートする場合、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いて、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します。

ライセンスの管理

アプリケーションが Light Agent モードで使用されている場合、ライセンスは Kaspersky Security for Virtualization Light Agent ソリューションで管理されます。ライセンス管理コマンドがエラーを返します。

Kaspersky Security Center を使用したライセンス管理

Kaspersky Security Center では、次の方法で管理対象デバイス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、個別のデバイスまたは管理グループに含まれるすべてのデバイス上のアプリケーション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、事前にライセンス保管領域に追加することも、［ライセンスの追加］タスクの作成時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デバイスに配信する。この方法では、Kaspersky Security Center に既に接続されている管理対象デバイスと新しい管理対象デバイスに、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。

  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。

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方法

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 コンソール経由でアプリケーションにライセンスを追加する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
   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。
   これにより、［**ライセンスの選択**］ウィンドウが開きます。

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. 必要なライセンスがライセンス保管領域にない場合は、［**新しいライセンスを追加**］リンクをクリックします。

   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. ［**製品設定**］タブで、［**予備のライセンスとして使用する**］チェックボックスをオンにできます。予備のライセンスとして追加されたライセンスは、現在のライセンスの有効期限が切れた後にアクティブになります。

9. 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。

10. 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。

Web コンソールを使用して、デバイスにライセンスを配信することでアプリケーションにライセンスを追加する方法

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。

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。

アプリケーションにライセンスを追加する方法

これらのコマンドを使用すると、ライセンスに含まれていないコンポーネントをアクティベートするため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。

アプリケーションに現在のライセンスを追加する

```
kesl-control [-L] --add-active-key <path to key file / activation code>
```

説明：

- `path to key file`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。
- `activation code`は、アクティベーションコードです。

アプリケーションに予備のライセンスを追加する

```
kesl-control [-L] --add-reserve-key <path to key file / activation code>
```

デバイス上の製品に現在のライセンスがまだ追加されていない場合、コマンドは失敗します。

ライセンスを削除する方法

ライセンスを削除するためのさまざまなコマンドを使用できます。

現在のライセンスを削除する

```
kesl-control [-L] --remove-active-key
```

予備のライセンスを削除する

```
kesl-control [-L] --remove-reserve-key
```

EDR Optimum の現在のライセンスを削除する

```
kesl-control [-L] --remove-active-key --edr-optimum
```

EDR Optimum の予備のライセンスを削除する

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

KUMA の現在のライセンスを削除する

```
kesl-control [-L] --remove-active-key --kuma
```

KUMA の予備のライセンスを削除する

```
kesl-control [-L] --remove-reserve-key --kuma
```

MDR の現在のライセンスを削除する

```
kesl-control [-L] --remove-active-key --mdr
```

MDR の予備のライセンスを削除する

```
kesl-control [-L] --remove-reserve-key --mdr
```

EDR Expert（オンプレミス）の現在のライセンスを削除する

```
kesl-control [-L] --remove-active-key --edr-kata
```

EDR Expert（オンプレミス）の予備のライセンスを削除する

```
kesl-control [-L] --remove-reserve-key --edr-kata
```

EDR Expert（クラウド）の現在のライセンスを削除する

```
kesl-control [-L] --remove-active-key --cxdr
```

EDR Expert（クラウド）の予備のライセンスを削除する

```
kesl-control [-L] --remove-reserve-key --cxdr
```

KWSM の現在のライセンスを削除する

```
kesl-control [-L] --remove-active-key --khcs
```

KWSM の予備のライセンスを削除する

```
kesl-control [-L] --remove-reserve-key --khcs
```

グラフィカルインターフェイスでのライセンス管理

現在のライセンスを追加する方法

1. アプリケーションの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。

      このウィンドウには、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。このウィンドウには、試用版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。

予備のライセンスを追加する方法

1. アプリケーションの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。

   このウィンドウには、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。

ライセンスを削除する方法

1. アプリケーションの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. 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。

役立つ記事

アプリケーションのアクティベーションに関する問題のトラブルシューティング

ライセンスに関する情報の表示

Kaspersky Security Center のライセンスに関する情報

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：

- アプリケーションのアクティベーションに使用する*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。

- クライアントデバイスにインストールされているカスペルスキー製品のプロパティでは、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。

  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方法

  1. Web コンソールのメインウィンドウで、［**アセット管理**］ → ［**アセット（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。下位グループを選択するには、ウィンドウ上部の **階層を表示** ボタンをクリックします。

     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. デバイス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. 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。このウィンドウで、［**全般**］タブの［**ライセンス**］セクションに移動します。

このセクションには、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、ライセンスの種別（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方法

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**］：一意の英数字列。
   - ［**ステータス**］：ライセンスのステータス（有効または予備など）。
   - **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。

- ライセンスの使用状況レポートには、Kaspersky Security Center を使用して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。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 のライセンスストアには、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。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。

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。

保護対象デバイスのライセンスに関する情報

コマンドラインでライセンスに関する情報を表示する方法

デバイスのライセンスに関する情報の表示

```
kesl-control -L --query [--json]
```

ここで、 `--json` は、データを JSON 形式で出力することを意味します。 `--json` 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。

コマンドは次の情報をコンソールに出力します：

- 現在のライセンスに関する情報：
  - ライセンスの有効期限の日時。
  - 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（この行は、Kaspersky Endpoint Security アプリケーションがアクティベートされているライセンスに対してのみ表示されます）。
  - アプリケーションの定義データベースのアップデートに関する制限事項の情報。
  - 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。

- 予備のライセンスに関する情報。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おり、予備のライセンスが追加されている場合に表示されます。アプリケーションが Light Agent モードで使用されている場合、予備のライセンスに関する情報は表示されません。
  - ライセンスの有効期限の日時。
  - 保護機能の制限に関する情報（この行は、Kaspersky Endpoint Security アプリケーションのアクティベーションに使用できるライセンスに対してのみ表示されます）。
  - アプリケーションの定義データベースのアップデートに関する制限事項の情報。
  - 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)。

アプリケーションの詳細を表示すると、アプリケーションの使用に適用されているライセンスに関する情報も確認できます：

```
kesl-control --app-info
```

アプリケーションのグラフィカルインターフェイスでライセンスに関する情報を表示する方法

1. アプリケーションの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、追加済みの現在のライセンスと、それに関連付けられているライセンスに関する情報が表示されます：

- 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、追加済みの予備のライセンスと、それに関連付けられているライセンスに関する情報が表示されます：

- 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。

Kaspersky Endpoint Security アプリケーションを標準モードまたは EDR 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間の終了に関する情報が OS ログに記録されます。

本製品の管理インターフェイス

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 のグラフィカルインターフェースを使用して実行できる操作は、一部に限られています。

Kaspersky Endpoint Security を仮想環境保護用 Light Agent モードで使用している場合、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本製品を管理することはできません。

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 エージェント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。

組織の IT インフラストラクチャ、および管理者の役割とワークフローに応じて、管理ツールを選択してください。クライアントデバイス上の本製品は、Kaspersky Security Center を使用してリモートで一元管理することを推奨します。

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。

Kaspersky Security Center の管理グループ

デバイスにインストールされている 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*に追加する必要があります。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。本製品のインストール後に、デバイスを管理グループに手動で移動することもできます（詳細は、Kaspersky Security Center ヘルプを参照してください）。

管理コンソールと管理プラグイン

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、Kaspersky Endpoint Security MMC 管理プラグイン（以後「MMC プラグイン」とも表記）によって提供されます。

  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る必要があります。

- 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。任意のデバイスのブラウザーを使用して、Kaspersky Security Center Web コンソールで作業できます。

  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、Kaspersky Endpoint Security 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。

  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ている必要があります。

- 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 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本製品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。

Kaspersky Security Center のポリシーとタスク

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。

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。ポリシーには、以下のいずれかのステータスがあります：

ポリシーのステータス

ステータス	説明
処理を実行	デバイスに適用されている現在のポリシーです。
非アクティブ	現在デバイスに適用されていないポリシーです。
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。

ポリシーは以下のルールに従います：

- 1つのアプリケーションに対して、異なる設定を持つ複数のポリシーを設定できます。
- 1つのアプリケーションにつき、有効にできるポリシーは1つのみです。
- ポリシーには子ポリシーを含めることができます。

設定のロック

各ポリシー設定には「南京錠」属性があります。この属性の状態によって、設定が管理グループ内の管理対象デバイスに渡されるかどうかが決まります。

- 「南京錠」が閉じている場合（🔒）、その設定はポリシーが適用されているデバイスに適用されます。ユーザーは、管理対象アプリケーションのユーザーインターフェイスでこれらの設定を変更することはできません。このような設定は、*ロック済み*と呼ばれます。
- 「南京錠」が開いている場合（🔓）、その設定はポリシーで指定されていません。ユーザーは、管理対象アプリケーションのユーザーインターフェイスでこれらの設定を変更できます。このような設定は、*ロック解除済み*と呼ばれます。

管理対象デバイスに適用するポリシー設定はロックすることを推奨します。ロックされていないポリシー設定は、管理対象デバイスで上書きできます。

Web コンソールと管理コンソールでは、「南京錠」が付いている設定の数が異なる場合があります。

ポリシープロファイル

多数のポリシーをサポートする必要がないようにするため、たとえば変更可能にする設定がごく少数の場合は、ポリシープロファイルを使用できます。

*ポリシープロファイル*とは、「基本」ポリシーの設定とは異なり、設定された条件（アクティベーションルール）が満たされたときにクライアントデバイスに適用される個別のポリシー設定のセットです。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。

「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。

ポリシープロファイルは以下のルールに従います：

- ポリシープロファイルは、特定のアクティベーション条件が満たされたときに有効になります。
- ポリシープロファイルには、ポリシーで設定された値とは異なる設定値が含まれます。

- ポリシープロファイルをアクティベートすると、管理対象デバイスの有効な設定（現在デバイスに適用されている設定）が変更されます。

- 1つのポリシーには、最大100個のプロファイルを含めることができます。

設定の継承

ポリシーには、管理グループと同様に階層があります。*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。

既定では、子ポリシーは親ポリシーの設定を継承します。親ポリシーの設定がロックされている場合（🔒）、子ポリシーとアプリケーションのローカル設定には同じ値が適用され、その設定はロックされます。必要に応じて、親ポリシーからの設定の継承を無効にすることができます。モバイルユーザーポリシーは、管理グループの階層でその他のポリシーに影響を及ぼしません。

子ポリシーの設定がロックされている場合（*アクセスが拒否されました*エラー）、ユーザーのアクセス権限を確認してください。ユーザーにポリシー設定を編集する権限がある場合は、Kaspersky Security Center の *管理サーバーのリポジトリへのアップデートのダウンロード*タスクを開始して、認証を再試行してください。Kaspersky Security Center で管理プラグインをアップグレードした後に、このエラーが発生することがあります。アップデートのダウンロード後、アプリケーションは新しいバージョンの管理プラグインに必要なファイルを取得します。

リストを値として持つ一部の設定（たとえば、ルールのリスト、除外リスト）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。

親ポリシーで継承によってマージされたリストから項目を削除しても、その項目は子ポリシーから削除されません。子ポリシーからこの項目を削除するには、それらのポリシーのプロパティを開き、項目を手動で削除する必要があります。

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。

ポリシーの管理

Web コンソールでポリシーを作成する方法

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。

   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管理グループを選択します。下位グループを選択するには、ウィンドウ上部の **階層を表示** ボタンをクリックします。

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。

     このモードを選択するには、ウィザードの次のステップに進みます。

   - **仮想環境を保護する Light Agent** – Kaspersky Security for Virtualization Light Agent ソリューションの一部として、このアプリケーションは 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の保護に使用されます。

6. アプリケーションを Light Agent モードで使用している場合は、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、Light Agent が拡張 SVM 選択アルゴリズムを使用しており、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っている場合、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。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. 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. ［**設定する**］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. ［**チェック**］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 の接続設定**］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. 手動で定義した SVM アドレスのリストを選択した場合は、このポリシーで管理される Light Agent が接続できる SVM のリストを作成します。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：

- 本声明のすべての条項に同意し、アプリケーションで Kaspersky Security Network を使用する場合は、**Kaspersky Security Network の使用に同意する** を選択します。
- Kaspersky Security Network を使用しない場合は、**Kaspersky Security Network の使用に同意しない** を選択し、表示されたウィンドウで決定を確認します。

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 の設定に関する推奨事項を確認するよう求められます。アプリケーションによるシステムリソース使用の最適化を可能にする設定を確認します。

ウィザードの次のステップに進みます。

9. 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。

  ポリシー設定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。

10. 他のポリシー設定を管理する場合は、**アプリケーション設定**タブに移動し、必要に応じて変更します。

    ポリシー設定は後で変更することもできます。

11. ［**保存**］をクリックします。

管理コンソールでポリシーを作成する方法

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。

   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、Light Agent が拡張 SVM 選択アルゴリズムを使用しており、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っている場合、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。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. 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）。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. 手動で定義した SVM アドレスのリストを選択した場合は、このポリシーで管理される Light Agent が接続できる SVM のリストを作成します。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。

役立つ記事

タスクが実行されない場合、またはポリシーが適用されない場合の対処方法

デバイスのステータスが次の場合の対処方法：「ポリシー設定が無効です。ポリシーが適用されていません。」

エラー：「アプリケーションは現在のバージョンの Kaspersky Security Center Web コンソールでサポートされていないか、アプリケーションの Web プラグインがインストールされていません」

ポリシー設定のエクスポートとインポート

Kaspersky Endpoint Security では、ポリシーとその設定およびプロファイルを KLP ファイルにエクスポートできます。その後、ポリシーのエクスポート / インポート機能を使用して、ポリシーのバックアップ作成、ポリシーの別のサーバーへの移行、または、Kaspersky Security Center Windows から Kaspersky Security Center Linux へのポリシーの移行などを行うことができます。ポリシーの管理について詳しくは、Kaspersky Security Center ヘルプを参照してください。

管理コンソール（MMC）でポリシーをエクスポートおよびインポートする方法

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーの［**管理対象デバイス**］フォルダーで、設定を適用するクライアントコンピューターが属している管理グループのフォルダーを開きます。
3. 作業領域で、［**ポリシー**］タブを選択します。
4. ポリシーをエクスポートするには：
   a. エクスポートするポリシーをクリックします。
   b. ウィンドウの右にある［**ポリシーをファイルにエクスポート**］リンクをクリックします。
   c. 表示されたウィンドウで、ポリシーをエクスポートする KLP ファイルの名前とそのファイルを保存するフォルダーを指定します。
   d. ファイルを保存します。
5. ポリシーをインポートするには：
   a. ［**ポリシーをファイルからインポート**］をクリックします。
   b. 表示されたウィンドウで、インポートするポリシーの KLP ファイルを選択します。
   c. ファイルを開きます。

   これにより、*非アクティブポリシー*のステータスの新しいポリシーが追加されます。

Web コンソールでポリシーをエクスポートおよびインポートする方法

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. ポリシーをエクスポートするには：
   a. エクスポートするポリシーの横にあるチェックボックスをオンにします。
   b. ［**エクスポート**］を選択します。
   c. 表示されたウィンドウで、ポリシーをエクスポートする KLP ファイルの名前とそのファイルを保存するフォルダーを指定します。
   d. ファイルを保存します。

3. ポリシーをインポートするには：

   a. ［**インポート**］をクリックします。

   b. インポートするポリシーの KLP ファイルを選択します。

   c. ポリシーの処理が正常に完了したら、ポリシーを適用する管理グループを選択します。

   d. ［**完了**］をクリックしてポリシーのインポートを終了します。

   これにより、*非アクティブ*のステータスの新しいポリシーが追加されます。

Web コンソールでの一部のポリシー設定のエクスポートとインポート

Web コンソールでは、個々のポリシー設定を JSON ファイルにエクスポートしたり、これらの設定をファイルからインポートしたりできます。たとえば、ウェブコントロールルールまたはファイル脅威対策の保護範囲のリストをエクスポートできます。

次の設定をエクスポートおよびインポートできます：

- ファイル脅威対策の保護範囲
- メール脅威対策の添付ファイルフィルター
- ネットワークパケットルール
- ウェブコントロールルール
- アプリケーションコントロールルール
- 監視範囲とシステム変更監視の除外範囲
- テレメトリの設定
- 特定の信頼ゾーンの除外リスト

Web コンソールで設定をエクスポートまたはインポートするには：

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. 設定をエクスポートまたはインポートするセクションに移動します。
5. を選択します。
6. 操作を選択します：**インポート** または **エクスポート**。
7. 設定をインポートする場合は、設定のインポート元のファイルを選択します。

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の抽出のタスク。

タスクはいくつでも作成できます。

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。

タスクの種別

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、本製品は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信し、ゴールデンイメージを管理します。
- *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。

Web コンソールでデバイスグループまたはデバイスの抽出のタスクを作成する方法

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）**］→［**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 のヘルプを参照してください。

   ウィザードの次のステップに進みます。

4. タスク範囲を定義するために選択した方法に応じて、次のいずれかの処理を実行します：

   - 管理グループツリーで、必要な管理グループの横にあるチェックボックスをオンにします。

   - デバイスのリストで、必要なデバイスの横にあるチェックボックスをオンにします。必要なデバイスがリストにない場合は、次の方法でデバイスを追加できます：

      - ［**デバイスの追加**］ボタンを使用します。名前または IP アドレスでデバイスを追加したり、指定した IP 範囲からデバイスを追加したり、企業 LAN のポーリング時に管理サーバーによって検知されたデバイスのリストからデバイスを選択したりできます。

      - ［**ファイルからデバイスをインポート**］ボタンを使用します。インポートには、デバイスアドレスのリストを含む TXT ファイルが使用されます。各アドレスは別の行に入力する必要があります。

   - リストから、必要なデバイスを含む選択の名前を選択します。

   ウィザードの次のステップに進みます。

5. タスクの作成直後にタスク設定を管理するには、ウィザードの最後のステップで、［**作成が完了したらタスクの詳細を開く**］チェックボックスをオンにします。タスクは既定で作成されます。

6. ウィザードを終了します。

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）**］→［**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、管理対象デバイスのリストの上にある［**階層を表示**］ボタンをクリックし、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. タスクの作成直後にタスク設定を管理するには、ウィザードの最後のステップで、［**作成が完了したらタスクの詳細を開く**］チェックボックスをオンにします。タスクは既定で作成されます。

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 コンソールでタスクを開始、停止、一時停止、再開する方法

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［**階層を表示**］ボタンをクリックし、表示され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台以上のデバイスで実行されるタスク（デバイスセットのタスク）を開始または停止するには、ウィンドウの上部にある［**階層を表示**］ボタンをクリックし、表示されたウィンドウで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。

> 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。

管理コンソールでのタスクの管理

管理コンソールでデバイスグループまたはデバイスの抽出のタスクを作成するには

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、以前に設定したデバイスの抽出を指定します（詳細については、Kaspersky Security Center ヘルプを参照してください）。

   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する方法

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。

管理コンソールでタスクを開始、停止、一時停止、再開する方法

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。

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については、Kaspersky Security Center 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。

タスクの管理と実行に関する特別な考慮事項

- デバイスのセットに対するタスクは、タスク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デバイスのセットに新しいデバイスが追加された場合、そのタスクは追加されたデバイスに対しては実行されません。この場合は、新しいタスクを作成するか、既存のタスクを編集する必要があります。
- 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。
- 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。
- Kaspersky Security Center の Kaspersky Endpoint Security アプリケーションでは、すべての種類のタスクを作成できます。保護対象デバイスでのタスクの適用および実行は、そのデバイスでのアプリケーションのモードによって決まります。たとえば、本製品が Light Agent モードで実行されている場合、*ライセンスの追加*、*アップデート*、*ロールバック*の各タスクはデバイスに適用されません。

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。

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、デバイス上で Kaspersky Endpoint Security をインストール、アンインストール、起動および停止したり、本製品をローカルで管理したりできます。

コンポーネントとタスク

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。デバイス上で本製品の機能コンポーネントを有効または無効にするには、コマンドラインで対応する Kaspersky Endpoint Security タスクを開始または停止する必要があります。

デバイスを 1 回スキャンするには、対応する Kaspersky Endpoint Security タスクを開始する必要もあります。

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管理するには、対応する Kaspersky Endpoint Security タスクの設定を管理する必要があります。

全般設定

Kaspersky Endpoint Security の個々のタスクに固有の設定に加えて、全般的な設定がいくつかあります：

- コンテナスキャンの全般設定。コンテナと名前空間をリアルタイムでスキャンするときに使用されます（コンテナ監視）。
- ネットワークトラフィックのスキャン設定。ウェブ脅威対策、ネットワーク脅威対策、メール脅威対策、ウェブコントロールの各コンポーネントで使用されます。
- 全般的な製品設定。これらの設定により、製品全体の動作と個々の機能の動作が制御されます。

管理コマンド

コマンドラインで *kesl-control ユーティリティ*を使用して、Kaspersky Endpoint Security のタスクと設定を管理できます。

作成または削除できるのは、ユーザータスクのみです。事前定義済みタスクは作成または削除できません。

製品のモードに応じて、次の種類のユーザー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*
- Light Agent モード：*ODS*、*ODFIM*、*ContainerScan*、*InventoryScan*。

*ライセンス*タイプのタスクを除き、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できます。

ODS、*ODFIM*、*InventoryScan*タスクを一時停止および再開できます。

Kaspersky Endpoint Security のローカルタスク

コマンドラインで Kaspersky Endpoint Security を管理するには、以下の表に示すタスクを使用できます：

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。

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	タスクの説明	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	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。ファイル脅威対策が有効になっている場合、このタスクはアプリケーションの起動時に自動的に実行されます	File_Threat_Protection	1	OAS
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。	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	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ため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。	Scan_File	3	ODS
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。	Critical_Areas_Scan	4	ODS
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。	Update	6	Update
アップデート（ユーザータスク）		ユーザーによって定義	100 以上	Update
ロールバック	このタスクを使用すると、アプリケーションの定義データベースとモジュールの最後のアップデートをロールバックできます。	Rollback	7	Rollback
ロールバック（ユーザータスク）		ユーザーによって定義	100 以上	Rollback
ライセンス管理	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。	License	9	License
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。	System_Integrity_Monitoring	11	OAFIM
システム変更チェック（ユーザータスク）		ユーザーによって定義	100 以上	ODFIM

タスク	タスクの説明	コマンドラインのタスク名	タスク ID	タスク種別
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。	Firewall_Management	12	Firewall
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。	Anti_Cryptor	13	AntiCryptor
ウェブ脅威対策	このタスクでは、ウェブ脅威対策を有効または無効にし、ウェブ脅威対策コンポーネントの設定を定義できます。ウェブ脅威対策が有効になっている場合、このタスクはアプリケーションの起動時に自動的に実行されます	Web_Threat_Protection	14	WTP
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。デバイスコントロールが有効になっている場合、このタスクはアプリケーションの起動時に自動的に実行されます。	Device_Control	15	DeviceControl
リムーバブルドライブのスキャン	このタスクを使用すると、リムーバブル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。	Removable_Drives_Scan	16	RDS
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。	Network_Threat_Protection	17	NTP
コンテナスキャン	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。	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	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ため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。	Custom_Container_Scan	19	ContainerScan
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。ふるまい検知が有効になっている場合、このタスクはアプリケーションの起動時に自動的に実行されます。	Behavior_Detection	20	BehaviorDetection
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。	Application_Control	21	AppControl
インベントリ	このタスクを使用すると、デバイス上のアプリケーションのすべての実行可能ファイルに関する情報を取得し、アプリケーションのゴールデンイメージカテゴリを管理できます。	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。	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。	KATAEDR	24	KATAEDR

タスク	タスクの説明	コマンドラインのタスク名	タスク ID	タスク種別
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。	Web_Control	26	WebControl
サンドボックス統合	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。	Standalone_Sandbox	29	StandaloneSandbox
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。	KATAEDR_Prevention	30	KATAEDRPrevention
Kaspersky Endpoint 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。	KATANDR	31	KATANDR
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。	EDRO_Prevention	32	Prevention
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。	KUMA	33	KUMA
メール脅威対策	このタスクを使用すると、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できます。メール脅威対策が有効になっている場合、このタスクはアプリケーションの起動時に自動的に実行されます	Mail_Monitoring	35	MailMonitoring
有害 USB 攻撃ブロック	このタスクを使用すると、キーボードを模倣した感染した USB デバイスがクライアントデバイスに接続されるのを防止できます。	Bad_USB	37	BadUSB
Kaspersky Endpoint Detection and Response Expert（クラウド）との連携	このタスクでは、Kaspersky Endpoint Detection and Response Expert（クラウド）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。	EDRExpertCloud	39	EDRExpertCloud

タスクの設定の編集

*ロールバック*タイプおよび*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を編集できます（これらのタスクには設定がありません）。アプリケーションが Light Agent モードで使用されている場合、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。

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。

タスク設定は、次の方法で編集できます：

- 設定情報ファイルを使用する。この方法を使用すると、すべてのタスク設定を同時に変更できます。タスク設定を出力するコマンドを使用して、編集する設定情報ファイルを取得できます。
- <setting name>=<setting value> 形式のコマンドラインオプションを使用する。この方法を使用すると、個々のタスク設定を変更できます。タスク設定の現在の値は、タスク設定を出力するコマンドを使用して表示できます。

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。

タスク設定の現在の値を出力する方法

タスク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。その後、このファイルを編集してタスク設定を変更できます。

タスク設定の現在の値をコンソールに出力する

```
kesl-control --get-settings <task ID|name>
```

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。

タスク設定の現在の値を設定情報ファイルに出力する

```
kesl-control --get-settings <task ID/name> --file <path to configuration file> [--json]
```

説明：

- `--file <path to configuration file>` は、タスク設定の出力先となる設定情報ファイルへのパスです。パスなしでファイルの名前を指定した場合、そのファイルは現在のディレクトリに作成されます。ファイルが指定されたパスに既に存在する場合は、上書きされます。指定されたディレクトリが存在しない場合、設定情報ファイルは作成されません。

- `--json` を指定すると、設定は JSON 形式で出力されます。`--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タスク設定を変更する方法：

1. 次のコマンドを使用して、タスク設定を設定情報ファイルに出力します：

   ```
   kesl-control --get-settings --file <path to configuration file> [--json]
   ```

   説明：

   - `--file <path to configuration file>` は、タスク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。

   - 設定を JSON 設定情報ファイルに出力する場合は、`--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、製品は設定を INI ファイルに出力します。

2. 生成された設定情報ファイルを開き、必要に応じて 設定を編集し、 変更を保存します。

   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. 次のコマンドを実行します：

```
kesl-control --set-settings <task ID/name> --file <path to configuration file> [--json]
```

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。

- `--file <path to configuration file>` は、タスク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。

コマンドラインオプションを使用して個々のタスク設定を変更する方法

次のコマンドを実行します：

```
kesl-control --set-settings <task ID|name> <setting name >=<setting value> [<setting name >=<setting value>]
```

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。
- `<setting name >=<setting value>` は、1つ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用して、タスク設定の現在の値を取得できます。

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。

コマンドラインオプションを使用してスキャン範囲を追加または削除する方法

コマンドラインオプションを使用してスキャン範囲を追加する

```
kesl-control --set-settings <task ID|name> --add-path <path>
```

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。
- `<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。

このコマンドは、新しい `[ScanScope.item_#]` セクションをタスク設定に追加します。`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。

ID=100 のタスクのスキャン範囲に /home ディレクトリを追加する例

```
kesl-control --set-settings 100 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.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=*
```

コマンドラインオプションを使用してスキャン範囲を削除する

```
kesl-control --set-settings <task ID|name> --del-path <path>
```

このコマンドは、指定されたパスを含む `[ScanScope.item_#]` セクションをタスク設定から削除します。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。

コマンドラインオプションを使用して除外範囲を追加または削除する方法

コマンドラインオプションを使用して除外範囲を追加する

```
kesl-control --set-settings <task ID|name> --add-exclusion <path>
```

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。
- `<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。

このコマンドは、新しい `[ExcludedFromScanScope.item_#]` セクションをタスク設定に追加します。`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。

コマンドラインオプションを使用して除外範囲を削除する

```
kesl-control --set-settings <task ID|name> --del-exclusion <path>
```

このコマンドは、指定されたパスを含む `[ExcludedFromScanScope.item_#]` セクションをタスク設定から削除します。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。

既定のタスク設定を復元する方法

次のコマンドを実行します：

```
kesl-control --set-settings <task ID|name> --set-to-default
```

ここで、`<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。

設定が既定値に変更されます。

タスクスケジュールの設定

本製品のモードに応じて、次の種類のタスクのスケジュールを設定できます：

- 標準モード：*ODS*、*アップデート*、*ロールバック*、*ODFIM*、*ContainerScan*、および *InventoryScan*
- Light Agent モード：*ODS*、*ODFIM*、*ContainerScan*、*InventoryScan*。

次の方法でタスクスケジュールを編集できます：

- 設定情報ファイルを使用する。この方法では、タスクスケジュールのすべての設定を同時に変更できます。スケジュール設定を出力するコマンドを使用して、編集用の設定情報ファイルを取得できます。
- <setting name>=<setting value> 形式のコマンドラインオプションを使用する。この方法では、タスクスケジュールの個別の設定を変更できます。スケジュール設定を出力するコマンドを使用して、タスク設定の現在の値を表示できます。

現在のスケジュール設定を出力する方法

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。このファイルを編集して、設定を変更できます。

現在のタスクスケジュール設定をコンソールに出力する

```
kesl-control --get-schedule <task ID|name> [--json]
```

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。
- `--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。

現在のタスクスケジュール設定を設定情報ファイルに出力する

```
kesl-control --get-schedule <task ID|name> --file <path to configuration file> [--json]
```

ここで、`--file <path to configuration file>` は、タスクスケジュール設定の出力先となる設定情報ファイルへのパスです。パスなしでファイルの名前を指定した場合、そのファイルは現在のディレクトリに作成されます。ファイルが指定されたパスに既に存在する場合は、上書きされます。指定されたディレクトリが存在しない場合、設定情報ファイルは作成されません。

アップデートタスクのスケジュール設定を update_schedule.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する例

```
kesl-control --get-schedule 6 --file update_schedule.ini
```

アップデートタスクのスケジュールをターミナルに書き込む例

```
kesl-control --get-schedule 6
```

設定情報ファイルを使用してタスクスケジュールを設定する方法

```
kesl-control --set-schedule <task ID|name> --file <path to configuration file> [--json]
```

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。
- `--file <path to configuration file>` 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。

設定情報ファイル /home/test/on_demand_schedule.ini から、ID=2 のタスクにスケジュール設定をインポートする例

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

コマンドラインオプションを使用してタスクスケジュール設定を変更する方法：

```
kesl-control --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

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。
- `<setting name>=<setting value>` は、1つのタスクスケジュール設定の名前と値です。

10時間ごとにタスクを実行するように設定する例

```
RuleType=Hourly
RunMissedStartRules=No
StartTime=2021/May/30 23:05:00;10
RandomInterval=0
```

10分ごとにタスクを実行するように設定する例

```
RuleType=Minutely
RunMissedStartRules=No
StartTime=23:10:00;10
RandomInterval=0
```

毎月15日にタスクを実行するように設定する例

```
RuleType=Monthly
RunMissedStartRules=No
StartTime=23:25:00;15
RandomInterval=0
```

毎週火曜日にタスクを実行するように設定する例

```
RuleType=Weekly
StartTime=18:01:30;Tue
RandomInterval=99
RunMissedStartRules=No
```

11日ごとにタスクを実行するように設定する例

```
RuleType=Daily
RunMissedStartRules=No
StartTime=23:15:00;11
RandomInterval=0
```

本製品の全般設定の管理

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。全般設定を使用すると、次の操作ができます。

- 本製品で、Kaspersky Security Network の使用とマルウェア対策データベースの軽量バージョンを設定します。
- 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します。
- リアルタイムでのコンテナ監視を有効または無効にします。

- 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。

次の方法で、特別な管理コマンドを使用して本製品の全般設定を管理できます：

- 設定情報ファイルを使用する。この方法では、すべての全般設定を同時に変更できます。全般設定出力コマンドを使用して、編集用の設定情報ファイルを取得できます。
- <setting name>=<setting value> 形式のコマンドラインオプションを使用する。この方法では、個々の設定を変更できます。全般設定出力コマンドを使用して、現在の設定値を取得できます。

本製品の全般設定の現在の値を出力する方法

本製品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。その後、このファイルを使用して設定を編集できます。

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

```
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

```
kesl-control --get-app-settings --file <path to configuration file> [--json]
```

`--file <path to configuration file>` は、アプリケーションの全般設定の出力先とな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。

現在のディレクトリにある `kesl_config.ini` ファイルにアプリケーションの全般設定を書き込む例

```
kesl-control --get-app-settings --file kesl_config.ini
```

設定情報ファイルを使用してタスク設定を編集する方法：

1. コマンド `kesl-control --get-app-settings` を使用して、本製品の全般設定を設定情報ファイルに出力します。
2. 生成された設定情報ファイルを開き、必要に応じて 設定を編集し、 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 <path to configuration file> [--json]
```

説明：

- `--file <path to configuration file>` 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。

/home/test/kesl_config.ini 設定情報ファイルからアプリケーションに全般設定をインポートする例

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

コマンドラインオプションを使用して全般設定を変更する方法

コマンドラインオプションを使用して全般設定を変更します

```
kesl-control --set-app-settings <setting name>=<setting value> [<setting name >=<setting value>]
```

ここで、`<setting name>=<setting value>` は、アプリケーションの全般設定の名前と値です。

指定された全般設定の値が変更されます。

トレースファイルの詳細レベルを低く設定する例

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

ファイル操作のインターセプトから除外するマウントポイントを追加する例

```
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：

フィルターは、以下の目的で使用できます：

特定のアプリケーションの現在のイベントに関する情報を表示する

```
kesl-control -W --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

イベントログ内の特定のアプリケーションイベントに関する情報を表示する

```
kesl-control -E --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

バックアップ内の特定のオブジェクトに関する情報を表示する

```
kesl-control -B --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

バックアップから特定のオブジェクトを削除する

```
kesl-control -B --mass-remove --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator>
'<value>']"
```

説明：

- `<field>` は、データベースのフィールド名です。
- `<comparison operator>` は、次の比較演算のいずれかです：
  - `>` は "対象より大きい"
  - `<` は「より小さい」です
  - `like` は、指定した値と一致します。値を指定する時に、`%` 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

- <value> 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。

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の出力例

```
kesl-control -E --query "FileName like '%etc%'"
```

ThreatDetected タイプのイベントに関する情報の出力例

```
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の出力例

```
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の出力例

```
kesl-control -E --query "Date > '1583425000'"
```

YYYY-MM-DD hh:mm:ss 形式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の出力例

```
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の出力例

```
kesl-control -B --query "DangerLevel == 'High'"
```

製品設定のエクスポートとインポート

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。

設定情報ファイルへのアクセス権限は、信頼できるユーザーのみに付与してください。本製品に設定をインポートする前に、ディレクトリ、設定情報ファイル、実行可能ファイル、隔離領域へのパスを確認してください。信頼できないソースから設定情報ファイルをインポートしないでください。設定情報ファイルが侵害されると、組織のインフラストラクチャやユーザーデータのセキュリティ、整合性、機能に影響が及ぶ可能性があります。

設定のエクスポート

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、その後、設定をアプリケーションにインポートできます。

製品設定のエクスポート

```
kesl-control --export-settings --file <configuration file path> [--json]
```

説明：

- `--file <configuration file path>` 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。

インポートの設定

1. 次のコマンドを実行します：

```
kesl-control --import-settings --file <configuration file path> [--json]
```

   説明：

   - `--file <configuration file path>` は、アプリケーション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。

2. 本製品を再起動します。

設定のエクスポートとインポートに関する特別な考慮事項と制限事項

- 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。
- Kaspersky Endpoint Security が Light Agent モードで使用されている場合、`Update` 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。
- ポリシーによって設定の変更が禁止されている場合、設定をインポートすることはできません。
- 旧バージョンのアプリケーションからエクスポートした設定を新しいバージョンにインポートする場合、旧バージョンに存在しなかった設定は既定値に設定されます。
- 新しいバージョンから古いバージョンに設定をインポートすることはできません。
- 一部のポリシーおよびタスク設定は、アプリケーション Web プラグインのバージョン 12.3 および 12.4 からアプリケーションのバージョン 12.5 にインポートできません。この制限は、次のポリシーおよびタスク設定に適用されます：
  - 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）
- *ODS*、*ContainerScan*、*InventoryScan*、*ODFIM* タスクのスキャン範囲。

- 設定をインポートした後、次の機能は無効になります：Kaspersky Security Network（`UseKSN=No`）、クラウドモード（`CloudMode=No`）、MDR 統合（`UseMDR=No`）。この機能を使用する場合は、設定を行ってください。
- 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。
- Kaspersky Endpoint Detection and Response Expert（クラウド）と統合されている場合、Kaspersky Endpoint Detection and Response Expert（クラウド）から受信した設定を含め、すべての設定がエクスポートされます：
  - テレメトリサーバーのアドレスとポート
  - レスポンスサーバーのアドレスとポート
  - レスポンスサーバーの接続タイムアウト
  - レスポンスサーバーの応答タイムアウト
  - テレメトリサーバーの接続タイムアウト
  - テレメトリサーバーの応答タイムアウト
  - テレメトリサーバーのクライアント証明書
  - テレメトリサーバーのサーバー証明書
  - レスポンスサーバーのクライアント証明書
  - レスポンスサーバーのサーバー証明書

  インポート時、上記の設定はデバイスにインポートされません。

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

グラフィカルインターフェイスを使用してアプリケーションを管理するには、管理者（admin）ロールの権限が必要です。

Kaspersky Endpoint Security を Light Agent モードで使用している場合、グラフィカルインターフェイスはサポートされません。

アプリケーションの**標準モード**では、グラフィカルインターフェイスを使用して以下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。
- アプリケーションコンポーネントの設定。

  選択ツリー

  - 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
- ファイルとディレクトリのスキャン（スキャンのためのサンドボックスへのファイル送信を含む）。
- アップデートの開始および定義データベースのアップデートのロールバック。

- アプリケーションでの Kaspersky Security Network の有効化または無効化。
- 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ライセンスの管理、および現在使用されているライセンスに関する情報の表示。
- Backup に配置されたオブジェクトの情報を表示。
- アプリケーションのレポートの表示。
- アプリケーショントレースファイルを作成。

通知領域の製品アイコン

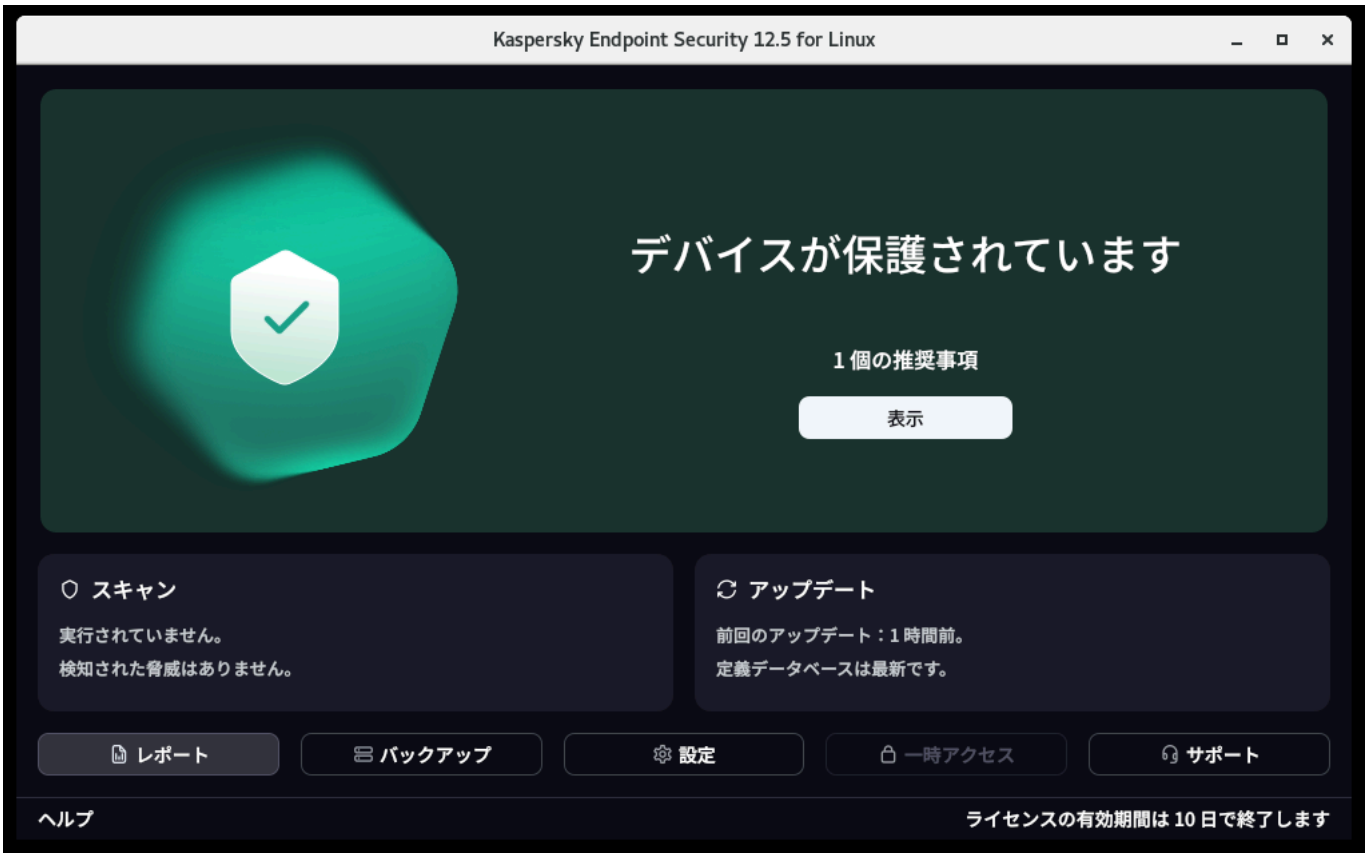
トレイの Kaspersky Endpoint Security アイコンを使用すると、アプリケーションのグラフィカルインターフェイスのコンテキストメニューとメインウィンドウにアクセスできます。

> 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 12.5 for Linux**。アプリケーションの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。
- **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

保護ステータス	デバイスの保護ステータスに関する情報。メインウィンドウの上部に表示されます。 ［**表示**］ボタンをクリックすると、［**プロテクションセンター**］ウィンドウを開くことができます。このウィンドウには、保護に関する問題がある場合に、その問題を修正するために実行する操作についての推奨事項が表示されます。
スキャン	マルウェアのスキャンタスクのステータスと、検知した脅威の数に関する情報。 このセクションをクリックすると、［**スキャン**］ウィンドウを開くことができます。このウィンドウでは、*マルウェアのスキャン*、*簡易スキャン*、*コンテナスキャン*の各タスクを開始および停止し、これらのタスクのレポートを表示できます。
アップデート	定義データベースのアップデートタスクのステータスに関する情報。 このセクションをクリックすると、［**アップデート**］ウィンドウを開くことができます。このウィンドウでは、*アップデートタスク*と*ロールバック*タスクを開始し、これらのタスクのレポートを表示できます。
レポート	コンポーネントとタスクのレポートおよび統計情報の表示。
バックアップ	バックアップ内のオブジェクトの詳細の表示。 ボタンが無効な場合の対処方法
設定	アプリケーションコンポーネントの有効化または無効化、Kaspersky Security Networkの設定。 ボタンが無効な場合の対処方法
一時アクセス	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。
サポート	本製品に関する情報：Kaspersky Endpoint Security の現在のバージョン、定義データベースの公開日、ライセンスおよびその他の情報です。 カスペルスキーのリソースにアクセスして、有用な情報を入手したり、テクニカルサポートに問い合わせたりすることもできます。
ライセンスの有効期間	ライセンスの残り有効期間 この領域をクリックすると、［**ライセンス**］ウィンドウを開くことができます。このウィンドウでは、ライセンスに関する詳細情報を表示したり、カスペルスキーのWebサイトにアクセスして新しいライセンスを購入したりできます。

保護ステータスの監視

Kaspersky Security Center クライアントデバイスの保護ステータス

Kaspersky Security Center では、クライアントデバイスのステータスを使用して、デバイスの保護ステータスに関する情報を取得できます。Kaspersky Security Center において、クライアントデバイスとは 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です。

クライアントデバイスのステータスは、Kaspersky Security Center で設定されたルールに従って、*緊急*または*警告*に変更されることがあります。たとえば、デバイスに保護アプリケーションがインストールされていない場合、長期間ウイルススキャンが実行されていない場合、アプリケーションのデータベースが最新でない場合、ライセンスの有効期間が終了している場合、または Kaspersky Security Center が管理対象アプリケーションからデバイスのステータスを受信した場合に、ステータスが変更されることがあります。

ステータスが変更される理由、およびステータスを割り当てる条件の設定の詳細については、Kaspersky Security Center ヘルプを参照してください。

Web コンソールでデバイスの保護ステータスを確認する方法

1. Web コンソールのメインウィンドウで、［**アセット管理**］ → ［**アセット（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。下位グループを選択するには、ウィンドウ上部の **階層を表示** ボタンをクリックします。

   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. デバイスの名前をクリックします。

4. 管理対象デバイスのプロパティウィンドウが開きます。このウィンドウの［**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**は、Kaspersky Endpoint Security がインストールされてから選択し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）を表します。

- **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。

管理コンソールでデバイスの保護ステータスを確認する方法

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。

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。

デバイス上でのアプリケーションの動作に関する全般情報

Web コンソールでアプリケーションに関する全般情報を表示する方法

1. Web コンソールのメインウィンドウで、［**アセット管理**］ → ［**アセット（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。下位グループを選択するには、ウィンドウ上部の **階層を表示** ボタンをクリックします。

   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. デバイス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. ［**全般**］タブの［**情報**］セクションで、アプリケーションに関する全般情報を表示します：

   - **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**は、デバイス上のアプリケーションの状態です（例：*実行中*、*停止*）。
   - **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。

7. ［**全般**］タブの［**コンポーネント**］セクションで、アプリケーションの機能コンポーネントに関する情報を表示します。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。

8. ［**イベント**］タブで、デバイス上のアプリケーションイベントの一覧を表示します。

管理コンソールでアプリケーションに関する全般情報を表示する方法

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。

6. ［**全般**］セクションで、アプリケーション行に関する全般情報を表示します。

- **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**は、アプリケーション（kesl サービス）のステータスです。アプリケーションには、*実行中*や*一時停止*などのステータスがあります。
- **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。

7. ［**コンポーネント**］セクションで、アプリケーションの機能コンポーネントに関する情報を表示します。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。

コマンドラインでアプリケーションに関する全般情報を表示する方法

次のコマンドを実行します：

```
kesl-control --app-info [--json] [--check-permissions]
```

説明：

`--json` – データを JSON 形式で出力します。

`--check-permissions` は、権限が正しく設定されていないアプリケーションディレクトリへのパスを表示します。

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：

- **名前**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の設定の詳細については、Kaspersky Security Center ヘルプを参照してください。

- アプリケーションが使用されているライセンスに関する情報：
  - **アプリケーションのライセンスの情報**アプリケーションのライセンスの情報、またはアプリケーションの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**。アプリケーションライセンスの有効期限の日時（UTC）。
- Endpoint Detection and Response Optimum コンポーネントおよびカスペルスキー製品との連携用コンポーネントのライセンスの情報。保護対象デバイスで次のコンポーネントがアクティベートされている場合、これら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）コンポーネントのアクティベーションに使用されたライセンス、または 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)。
  - **EDR Expert（クラウド）のライセンスの情報**。Endpoint Detection and Response Expert（オンプレミス）コンポーネントのアクティベーションに使用されたライセンス、または EDR Expert（クラウド）のライセンスのステータスに関する情報。
  - **EDR Expert（クラウド）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。
- **バックアップの用途**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。
- **定義データベースを読み込み済み**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。
- **更新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**。
- **Light Agent モード**。アプリケーションが 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**。EDR Agent モードで使用されているアプリケーションに関する情報。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 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**. Kaspersky Managed Detection and Response との連携ステータス。
- **Kaspersky Endpoint Detection and Response Optimum の連携**。Kaspersky Endpoint Detection and Response Optimum との連携のステータス。
- **ファイル脅威対策**リアルタイムのファイル脅威対策ステータス。
- **コンテナの監視**。リアルタイムのコンテナスキャンステータス。
- **システム変更監視**。システム変更監視コンポーネントのステータス。
- **ファイアウォール管理**。ファイアウォール管理コンポーネントのステータス。
- **アンチクリプター**。アンチクリプターコンポーネントのステータス。
- **ウェブ脅威対策**. ウェブ脅威対策コンポーネントのステータス。
- **デバイスコントロール**。デバイスコントロールコンポーネントのステータス。
- **リムーバブルドライブのスキャン**。リムーバブルドライブのスキャンコンポーネントのステータス。
- **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）との連携**。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。
- **Kaspersky Endpoint Detection and Response Expert（クラウド）との連携**。Kaspersky Endpoint Detection and Response Expert（クラウド）との連携のステータス。
- **Sandbox との連携**. Sandbox との連携のステータス。
- **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。
- **アプリケーションが不安定です**アプリケーションがクラッシュした場合のダンプに関する情報。このフィールドは、ダンプディレクトリ内にファイルが見つかった場合に表示されます。
- **アプリケーションのステータス**ネットワークエージェントの接続ステータスとシステムディレクトリに対する権限に関する情報：
  - *OK*ネットワークエージェントが接続されており、システムディレクトリに対する権限が正しく設定されています。
  - *緊急性が高い問題です。ネットワークエージェントへの接続が確立されていません*
  - *緊急性が高い問題です。システムディレクトリの権限が正しく設定されていません*
  - *緊急性が高い問題です。ネットワークエージェントへの接続が確立されていません。システムディレクトリの権限が正しく設定されていません*

グラフィカルインターフェイスでアプリケーションに関する全般情報を表示する方法

1. アプリケーションの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. デバイスと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を表示します：
   - 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をクリックすると、**ライセンス**ウィンドウが開き、詳細なライセンスの情報が表示されます。
   - **ライセンスのステータス**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。

アプリケーションの統計情報

最も頻繁にスキャンされたファイルおよび起動されたプロセスに関する統計情報を表示できます。

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 コンソールでスキャンの統計情報を表示する方法

1. Web コンソールのメインウィンドウで、［**アセット管理**］→［**アセット（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。下位グループを選択するには、ウィンドウ上部の **階層を表示** ボタンをクリックします。

   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. デバイス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、［**統計**］→［**スキャン統計**］を選択します。

7. **スキャンの統計情報**ウィンドウでアプリケーションの統計情報を表示します：

   - ［**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。

   各領域の上部にある［**エクスポート**］をクリックすると、対応す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。

管理コンソールでスキャンの統計情報を表示する方法

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. 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。

7. アプリケーションの統計情報を表示します：

   - ［**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。

   各領域の下にある［**エクスポート**］をクリックすると、対応す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。

コマンドラインでスキャンの統計情報を表示する方法

次のコマンドを実行します：

```
kesl-control [-S] --get-statistic [--files] [--processes]
```

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。

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。

> CentOS 5.2、5.4、6.4、6.6 では、頻繁にスキャンされるファイルの統計情報は収集されません。

検出されたマウントポイント

デバイスで検出されたマウントポイントのリストを表示できます。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す情報がリストに表示されます。

Web コンソールでマウントポイントのリストを表示する方法

1. Web コンソールのメインウィンドウで、［**アセット管理**］ →［**アセット（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。下位グループを選択するには、ウィンドウ上部の **階層を表示** ボタンをクリックします。

   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. デバイス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、［**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。

7. マウントポイントに関する情報を表で表示します：

   - **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。

管理コンソールでマウントポイントのリストを表示する方法

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. 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、［**統計**］→［**マウントポイント**］セクションを選択します。
7. **マウントポイントのリスト**テーブルでマウントポイントに関する情報を表示します：

   - **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。

コマンドラインでマウントポイントのリストを表示する方法

次のコマンドを実行します：

```
kesl-control [-S] --get-statistic --mountpoints
```

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

機能と技術の一覧

コマンドラインで、状態情報（使用中または未使用）と、これらのアプリケーション機能の実装に使用されている Linux 技術を含むアプリケーション機能の一覧を表示できます。

機能と技術の一覧を表示する

```
kesl-control --supported-tech-info
```

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：

ファイル操作のインターセプト：

ステータス：使用中または未使用

技術：fanotify、ファイル脅威対策カーネルモジュール、更新可能なカーネルモジュール。

プロセス起動のインターセプト：

ステータス：使用中または未使用

技術：eBPF、kprobe、netlink、未定義、更新可能なカーネルモジュール。

ネットワークトラフィックのスキャン：

ステータス：使用中または未使用

技術：eBPF、iptables、未定義。

iptables ユーティリティ：

ステータス：使用中または未使用

技術：ipv6、未定義、タイムアウト、ルール内の複数ラベルのサポート。

ネットワーク分離：

ステータス：使用中または未使用

技術：eBPF、iptables、未定義。

脆弱性攻撃ブロック：

ステータス：使用中または未使用

技術：未定義、更新可能なカーネルモジュール。

リアルタイム保護のステータス

リアルタイムコンピュータ保護のステータスにより、ファイル脅威対策コンポーネントのステータスが決まります。ファイル脅威対策は、コンピュータに最低限のセキュリティレベルを提供します。このコンポーネントは Kaspersky Endpoint Security と同時に起動し、ファイルをリアルタイムでスキャンします。

リアルタイム保護のステータス

Kaspersky Security Center でのステータス	コマンドラインでのステータス	説明
実行中	開始済み	ファイル脅威対策タスクは開始され、実行中です。
開始中	開始中 または 再開中	ファイル脅威対策タスクの実行を試行します。タスクが開始されるまで待ちます。
停止	停止 または 停止中	ファイル脅威対策タスクが手動で停止されました。Kaspersky Security Center で、またはコンピュータ上でローカルにタスクを実行します。 アプリケーションが Light Agent モードでインストールされている場合、SVM との接続がないときにデバイスはこのステータスになります。
一時停止	一時停止中 または 一時停止	ファイル脅威対策タスクが手動で一時停止されました。Kaspersky Security Center で、またはコンピュータ上でローカルにタスクを実行します。
未設定		アプリケーションは EDR Agent モードでインストールされています。ファイル脅威対策コンポーネントは通知モードで動作します。
不明		不明なエラーです。

リアルタイムコンピュータ保護のステータスを確認する方法

リアルタイムコンピュータ保護のステータスは、Kaspersky Security Center コンソールの管理対象デバイスのリストで、またはコンピュータ上でローカルに確認できます。

Web コンソールでリアルタイムコンピュータ保護を確認する方法

Web コンソールのメインウィンドウで、［**資産管理**］→［**アセット（デバイス）**］の順に選択します。

現在の保護ステータスは、デバイスのリストの **リアルタイム保護のステータス** 列に表示されます。**リアルタイム保護のステータス** 列が表示されない場合は、列の設定を管理してください（⚙）。

コマンドラインでリアルタイムコンピュータ保護を確認する方法

次のコマンドを実行します：

```
kesl-control --get-task-state 1
```

その結果、Kaspersky Endpoint Security は、ファイル脅威対策の動作に関する情報を次の形式で表示します：

名前: File_Threat_Protection	
ID	: 1
種別	: OAS
ステータス	: <protection status>

リアルタイムコンピュータ保護のステータスが 実行中 でない場合の対処方法

1. ポリシーのプロパティでファイル脅威対策が有効になっていることを確認します。
2. アプリケーションがアクティベートされていることを確認します。
3. ファイル脅威対策 タスクを実行してみてください：

   Web コンソールでファイル脅威対策タスクを実行する方法

   1. Web コンソールのメインウィンドウで、［**資産管理**］→［**アセット（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. リストからデバイスを見つけて、その名前をクリックします。
   3. 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。

      これにより、デバイス上のすべてのタスクのリストが開きます。
   4. **ファイル脅威対策** タスクを選択し、**実行** ボタンをクリックします。

   コマンドラインでファイル脅威対策タスクを実行する方法

   次のコマンドを実行します：

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

イベントとレポート

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、アプリケーションはイベント情報を /var/opt/kaspersky/kesl/private/storage ディレクトリにあるイベントログデータベースファイルに保存します。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

- 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 – ポリシーのプロパティまたはアプリケーションの全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 のレポートの操作に関する詳細は、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、そのコンポーネント、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、'\\\\' 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（syslog）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。

既定では、オペレーティングシステムのログへのイベントの記録は無効になっています。

Kaspersky Endpoint Security が標準モードまたは EDR Agent モードで実行されており、Kaspersky Security Center のポリシーによって管理されている場合、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切れに関する情報がオペレーティングシステムの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 syslog へのイベントの記録を設定する方法

1. Web コンソールのメインウィンドウで、［**アセット管理**］ → ［**ポリシー**］の順に選択します。

2. Kaspersky Endpoint Security for Linux 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**］タブに移動します。

4. ［**全般設定 → イベントの設定**］の順に選択します。

   イベントの種類は重要度別にグループ化されて表示されます。

5. オペレーティングシステムのログへの記録を設定するイベントに対応する重要度レベルの名前が付いたブロックで、［**設定**］をクリックします。

   選択した重要度レベルのすべて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記録を個別に有効または無効にできます。

6. ［**イベント**］列で、オペレーティングシステムのログへの記録を設定するイベントの名前をクリックします。

7. ［**通知**］タブに移動します。

8. ［**オペレーティングシステムのイベントログに保存する**］チェックボックスをオンまたはオフにします。

イベント通知の設定

管理コンソールで syslog へのイベントの記録を設定する方法

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。

4. ［**全般設定**］→［**インターフェイス**］セクションに移動します。

5. ［**通知**］で、［**設定**］をクリックします。

   ［**通知設定**］ウィンドウが開きます。

6. 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のログに記録するイベントを選択します。

特定の重要度レベルのすべてのイベントを選択することもできます：

- *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。

コマンドラインで syslog へのイベントの記録を設定する方法

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。

イベントの syslog への記録を有効または無効にする

```
kesl-control --set-app-settings UseSyslog=<Yes|No>
```

説明：

- `Yes`：すべてのイベントの syslog へ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

アプリケーションの全般設定の現在の値は、コマンドラインまたは設定情報ファイルで確認できます。

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

```
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。

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

```
kesl-control --get-app-settings --file <path to configuration file> [--json]
```

`--file <path to configuration file>` は、アプリケーションの全般設定の出力先とな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。

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。

コマンドラインオプションを使用してイベント設定を変更する

```
kesl-control --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

ここで、<設定名>=<設定値> は、いずれかの設定の名前と値です。

設定情報ファイルを使用してイベント設定を変更する

```
kesl-control --set-app-settings --file <path to configuration file> [--json]
```

説明：

- `--file <path to configuration file>` 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、アプリケーションは INI ファイルからインポートを試みます。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。

アプリケーションイベントの表示

Kaspersky Security Center で Kaspersky Endpoint Security アプリケーションのすべてのイベントを表示する

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。

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。

Web コンソールですべてのイベントのリストを表示する方法

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. ［**イベントの設定**］タブに移動します。
   すべてのイベントのリストが、重要度でフィルタリングされた状態で表示されます。
4. 左側のメニューを使用して、その他の重要度レベルのすべてのイベントを表示します。

管理コンソールですべてのイベントのリストを表示する方法

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。
4. ［**全般設定**］→［**通知設定**］セクションに移動します。
5. ［**通知**］で、［**設定**］をクリックします。
   ［**通知設定**］ウィンドウが開きます。

イベント通知を設定できます。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。

アプリケーションのグラフィカルインターフェイスでのイベントの表示

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。

Web コンソールでポップアップ通知を設定する方法

1. Web コンソールのメインウィンドウで、［**アセット管理**］ → ［**ポリシー**］の順に選択します。
2. Kaspersky Endpoint Security for Linux 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**］タブに移動します。
4. ［**全般設定 → イベントの設定**］の順に選択します。
5. ［**詳細設定**］リンクをクリックします。
   ［**追加設定**］ウィンドウが開きます。
6. ［**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を表示する**］チェックボックスをオンまたはオフにします。既定では、このチェックボックスはオンです。
7. 変更内容を保存します。

管理コンソールでポップアップ通知を設定する方法

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。
4. ［**全般設定**］→［**通知設定**］セクションに移動します。
5. ［**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を表示する**］チェックボックスをオンまたはオフにします。既定では、このチェックボックスはオンです。

コマンドラインでポップアップ通知を設定する方法

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。

グラフィカルインターフェイスでポップアップ通知の表示を有効にする

```
kesl-control --set-app-settings ShowPopUpNotifications=<Yes|No>
```

説明：

- 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。

コマンドラインでの Kaspersky Endpoint Security アプリケーションの現在のイベントの表示

コマンドラインでは、アプリケーション内の現在のすべてのイベント、または指定したタスクに関連する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コンソールに表示する

```
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。

タスクを実行し、そのタスクに関連する現在のイベントに関する情報をコンソールに出力する

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

ここで、`<<task ID|name>` 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。

このコマンドは、指定された ID または名前のタスクを開始し、そ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。イベントは、このタスクによって生成されるとすぐに出力されます。

ID=1 のタスクを開始し、そのイベントの出力を有効にする例

```
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コンソールに表示する

```
kesl-control -W --query "<filter conditions>"
```

ここで、`<filter conditions>` は、`and` 論理演算子で結合された `<field> <comparison operation> '<value>'` 形式の 1 つ以上の 論理式です。

TaskStateChanged イベント出力の例

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

「User」ユーザーによって開始された TaskSettingsChanged イベント出力の例

```
kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'"
```

アプリケーションイベントログからのイベントの表示

コマンドラインを使用して、アプリケーションイベントログ内のイベントに関する情報をコンソールまたはファイルに出力できます。イベントのサブセットを出力するには、フィルタリングを使用します。

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コンソールに出力する

```
kesl-control -E --query [--db <database file>]
```

ここで、`<database file>` 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、アプリケーションはイベントに関する情報を `/var/opt/kaspersky/kesl/private/storage/events.db` データベースに保存します。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、次のコマンドを使用してイベントをコンソールに出力します：

```
kesl-control -E
```

`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アプリケーションイベントログ内のイベントに関する情報をコンソールに表示する

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--json] [--reverse]
```

説明：

- `<filter conditions>` は、クエリの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 `<field> <comparison operator> '<value>'` 形式の 1 つ以上の 論理式を指定します。
- `<number>` は、出力する、選択範囲内の最新イベントの数（つまり、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）。

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ファイルに出力する

```
kesl-control -E --query "<>" [--db <database file>] [-n <number>] --file <path to file> [--json]
```

ここで、`--file <path to file>` は、イベントを出力するファイルへの完全パスです。

役立つ記事

誤検知への対処方法

レポートの表示

レポートの表示は、本製品のグラフィカルインターフェイスでのみ可能です。

*レポート*には、Kaspersky Endpoint Security の各コンポーネントの動作、各スキャンタスク、アップデートタスクおよび整合性チェックタスクの実行、ならびに本製品全体の動作に関する情報が記録されます。

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**。ファイル脅威対策とスキャンタスクの統計。［**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**。本製品の動作中およびユーザーが本製品を操作している間に発生するイベントに関する情報。
- **脅威対策**。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：
  - 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。

製品インターフェイスでレポートを表示する方法

1. アプリケーションの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。

   レポートはウィンドウの右側に表示されます。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。

   既定では、イベントは［**日時**］列の値で昇順にソートされます。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。
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。

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。

アプリケーションが使用するオペレーティングシステムリソースのメトリック収集を設定する

```
kesl-control [-J] --export-metrics [--period <interval in seconds between outputs>|--interactive]
```

説明：

`--period` は、コマンドラインへの結果の定期的な出力を有効にします（出力間隔は秒単位で指定します）。

`--interactive` は、対話型出力を有効にします（**Enter** キーが押されたとき）。

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 ゲージ	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_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 ゲージ	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 ゲージ	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 ゲージ	kesl プロセスによって現在使用されているスワップ領域の量。 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_wd_limits_bytes 「type=virtual」ラベル ゲージ	kesl プロセスによる仮想メモリの使用を制限します。
lfs_system_memory_wd_limits_bytes 「type=resident」ラベル ゲージ	kesl プロセスによる常駐メモリの使用を制限します。
lfs_system_memory_wd_limits_bytes 「type=swap」ラベル ゲージ	kesl プロセスによるスワップ領域の使用を制限します。
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。

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_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 ゲージ	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。
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 ゲージ	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 ゲージ	現在の読み取られた送信ネットワーク接続の数。
lfs_tproxy_connection_processed_count 「direction=inbound」ラベル カウンター	インターセプトされた受信ネットワーク接続の総数。
lfs_tproxy_connection_processed_count 「direction=outbound」ラベル カウンター	インターセプトされた送信ネットワーク接続の総数。
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。

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_tproxy_threadPool_thread_count ゲージ	ネットワークインターセプターの MITM メカニズムを処理するスレッドの数。スレッドは、接続を処理するためにスレッドマネージャーによって作成されます。すべてのスレッドが同じコードを実行し、そのコード内で、新しい接続や確立済みの接続で受信したパケットなどのネットワークイベントを待機します。
lfs_tproxy_threadPool_thread_waiting ゲージ	lfs_tproxy_threadPool_thread_count のうち、空きスレッドの数。ネットワークインターセプターの MITM メカニズムで poll を待機しているスレッド。
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 ゲージ	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 ゲージ	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 ゲージ	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。
lfs_faCache_file_count ゲージ	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 ゲージ	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 ゲージ	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。

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_oas_cache_volume_count ゲージ	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 ゲージ	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 ゲージ	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_doc_prevention_cache_file_count ゲージ	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（ドキュメントを開く時）。
lfs_script_prevention_cache_file_count ゲージ	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（スクリプトを実行する時）。
lfs_doc_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（ドキュメントを開く時）。
lfs_script_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（スクリプトを実行する時）。
lfs_doc_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（ドキュメントを開く時）。
lfs_script_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（スクリプトを実行する時）。
lfs_doc_prevention_cache_volume_count ゲージ	「オブジェクトの実行防止」タスクのドキュメント用マウントポイントキャッシュの現在のサイズ。
lfs_script_prevention_cache_volume_count ゲージ	「オブジェクトの実行防止」タスクのスクリプト用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 ゲージ	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）。
eka_telemetry_metrics_registry_registered_callbacks ゲージ	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 ゲージ	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。

アプリケーションの安定性監視

Kaspersky Endpoint Security のアプリケーションの安定性監視は、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。

Web コンソールでのアプリケーションの安定性監視の設定方法

1. Web コンソールのメインウィンドウで、［**アセット管理**］ → ［**ポリシー**］の順に選択します。
2. Kaspersky Endpoint Security for Linux 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**］タブに移動します。
4. ［**全般設定**］→［**パフォーマンス**］の順に選択します。
5. **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またはオフにします。既定では、このチェックボックスはオフです。

管理コンソールでのアプリケーションの安定性監視の設定方法

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。
4. ［**全般設定**］ → ［**アプリケーション設定**］セクションに移動します。
5. **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またはオフにします。既定では、このチェックボックスはオフです。

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アプリケーションの安定性監視の設定方法

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。

このファイルに変更を加えた後、Kaspersky Endpoint Security を再起動します。

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。

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

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。

アプリケーションパッケージの整合性をチェックする

```
integrity_checker [<path to manifest file>] --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type
kds-with-filename
```

グラフィカルインターフェイスパッケージの整合性をチェックする

```
integrity_checker <path to manifest file> --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

```
integrity_checker.exe [<path to manifest file>]
```

ネットワークエージェントの整合性をチェックする

```
integrity_checker <path to manifest file>
```

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 <directory>` 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 <file name>` は、スキャン中に発生したイベントを、DEBUG ログレベルで指定されたファイルに書き込みます。
- `--signature-type kds` は、検証する署名の種別です（このオプションは、Kaspersky Endpoint Security 管理 Web プラグインのチェックに必要です）。
- `--signature-type kds-with-filename` は、検証する署名の種別です（この設定は、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チェックに必要です）。
- `--single_file <file name>` 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。

整合性チェッカーツールで使用可能なすべてのオプションを表示する

```
integrity_checker --help
```

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。

本製品のアクセスコントロール

Kaspersky Endpoint Security におけるアクセスコントロールは、Role Based Access Control（RBAC）ポリシーに基づいています。ユーザーに特定の権限またはリソースへのアクセス権を付与するには、対応するロールを割り当てる必要があります。*ロール*は、製品の管理に使用する一連の権限や特権です。

ユーザーロールにより、アクセス権の日常的な管理をより簡単かつ迅速に行えます。ロールのアクセス権は、ユーザーの一般的なタスクおよび職務内容に従って設定されます。

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。

事前定義されたロール

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。

オペレーティングシステムに、システムユーザーの 4 つのグループが作成されます：

- kesladmin
- kesluser
- keslaudit
- nokesl

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（下の表を参照してください）。ユーザーからロールを取り消すと、このユーザーは対応するグループから削除されます。

ロールを割り当てた後または取り消した後は、製品を再起動（kesl プロセス）し、グラフィカルインターフェイス（kesl-gui プロセス）も再起動する必要があります。

ロールとユーザーグループ

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。 ユーザーのロールの取り消し（管理者が自身の admin ロールを取り消すことはできません）。 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。 スキャンのためにファイルをサンドボックスに送信 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。

ユーザーロールを割り当てる、または取り消す方法

ロールは、ユーザーがシステム内で実行できる権限と操作を定義します。管理者（kesladmin）ロールを持つユーザーのみがロールを管理できます。root 権限を持つユーザーによってアプリケーションが管理されることを避けるため、保護対象デバイス上に管理者ロールを持つユーザーを少なくとも 1 人作成することを推奨します。

ユーザーとロールのリストの表示

```
kesl-control --get-user-list
```

ユーザーにロールを割り当てる

```
kesl-control --grant-role <admin|user|audit> <user name>
```

audit ロールをユーザー test15 に割り当てる例

```
kesl-control --grant-role audit test15
```

ユーザーからロールを取り消す

```
kesl-control --revoke-role <role> <user name>
```

ユーザー test15 から audit ロールを取り消す例

```
kesl-control --revoke-role audit test15
```

Kaspersky Security Center の RBAC 機能領域

既定では、Kaspersky Security Center 管理システムで「Kaspersky Endpoint Security 管理者」ロールを持つユーザーは、Kaspersky Endpoint Security のすべての機能にアクセスできます。

Kaspersky Endpoint Security のユーザーまたはグループに対して、Kaspersky Endpoint Security の機能へのアクセス権のレベルとして、次の定義済みレベルのいずれかを選択できます：

- **読み取り**では、Kaspersky Endpoint Security の全般設定と Kaspersky Endpoint Security コンポーネントの設定を表示できます。
- **編集**では、Kaspersky Endpoint Security の全般設定と Kaspersky Endpoint Security コンポーネントの設定を表示および編集できます。
- **実行**では、Kaspersky Endpoint Security のタスクを開始および停止できます。
- **デバイスの抽出に対する操作の実行**では、デバイスの抽出に対して Kaspersky Endpoint Security のタスクを開始および停止できます。

高度なアクセス権限を設定して、Kaspersky Endpoint Security の機能へのアクセスを許可または拒否することもできます。

Web コンソールで製品機能へのアクセス権限を設定する方法

1. Web コンソールのメインウィンドウで、［**ユーザーとロール**］→［**ロール**］の順に選択します。

2. 機能領域を設定するロールを選択します。

   必要に応じて、新しいロールを追加できます。詳細については、Kaspersky Security Center のヘルプを参照してください。

3. Kaspersky Endpoint Security アプリケーションへのアクセス権を設定します。

4. ［**保存**］をクリックします。

Kaspersky Endpoint Security の機能へのアクセス権限

機能領域	Kaspersky Endpoint Security の機能
基本機能	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 ロールバック インベントリ 有害 USB 攻撃ブロック システム変更監視 システム整合性チェック 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 テレメトリソースと auditd モード（OS との連携設定） イベントの設定 Light Agent モード ライセンスの追加
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
デバイスコントロール	デバイスコントロール
データ暗号化	デバイスへの一時アクセスを許可（デバイスコントロール）
信頼ゾーン	信頼ゾーン： • 信頼する URL を指定します • 信頼する IP アドレス • 監視対象ポート • 信頼するルート証明書 • 信頼するドメイン • 信頼するマウントポイント • トラフィック読み取りの除外リスト • 信頼するアプリケーション • マルウェアのスキャンの除外 • 信頼するデバイス

機能領域	Kaspersky Endpoint Security の機能
Detection and Response	組み込みエージェント： • Managed Detection and Response • Endpoint Detection and Response • Endpoint Detection and Response Expert（オンプレミス） • Endpoint Detection and Response Expert（クラウド） • Network Detection and Response (KATA) • Sandbox • KUMA との連携 対応処理： • プロセスの終了 • プロセスの開始 • IOC スキャン • デバイスからファイルを受信 • ファイルを隔離する • デバイスからのファイルの削除 • ネットワーク分離 • オブジェクトの実行防止 • テレメトリの設定
ホスト侵入防止	ふるまい検知 脆弱性攻撃ブロック アンチクリプター ネットワーク脅威対策 ファイアウォール管理
保護コンポーネント	マルウェアのスキャン 簡易スキャン ファイル脅威対策 メール脅威対策 リムーバブルドライブのスキャン ウェブ脅威対策
ウェブコントロール	ウェブコントロール

保護対象デバイスの一般的なロールに関する推奨事項

ワークステーション

ワークステーションにアプリケーションをインストールする場合は、アプリケーションのグラフィカルインターフェイスもインストールすることを推奨します。

アプリケーションのインストール後：

- ウェブ脅威対策を有効にします。
- デバイスがインターネットに直接接続されていない場合は、次のいずれかの方法で、ネットワークトラフィックのスキャン設定で証明書のローカル検証を選択します：
  - Web コンソールで、**暗号化された接続のスキャン**の下にある**設定**ボタンをクリックし、**証明書検証ポリシー**を**ローカルチェック**に設定します。
  - 管理コンソールで、**暗号化された接続の設定**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。
  - 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する場合：

```
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。

- 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ているすべてのリモートディレクトリに対して、ファイル操作のインターセプトからの除外（グローバル除外）を設定します。

ファイルサーバー

アプリケーションのインストール後：

1. アーカイブのスキャンがファイル脅威対策の設定で無効になっていることを確認します。既定ではこのオプションが選択されます。
2. 次の設定でマルウェアのスキャンタスクを作成します：
   - アーカイブのスキャン：有効
   - タスクスケジュール：負荷が最小の時間帯

Web サーバー

Kaspersky Endpoint Security は、Web サーバーの保護を目的としていません。Web サーバーを保護するには、Kaspersky NGFW および Kaspersky Web Traffic Security の使用を推奨します。

Web サーバーで Kaspersky Endpoint Security を使用しており、そのサーバーが HTTPS プロトコルを使用していてクライアント負荷が高い場合、ウェブ脅威対策によりシステムリソースの使用率が大幅に増加する可能性があります。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。

ウェブ脅威対策の動作中に、Web サーバーの負荷がどのように変化するかを分析します。設定を最適化し、互換性の問題を解消するために、除外を設定できます。

プロキシサーバー

アプリケーションのインストール後、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、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します。

コンテナ化されたサーバー

アプリケーションのインストール後、コンテナ化サービスに使用されるサーバーで、ウェブ脅威対策、ネットワーク脅威対策、Firewall 管理の各コンポーネントを無効にします。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。

データベースサーバー

データベース管理システムの作業ディレクトリに対して、グローバル除外を設定します。

ご使用のインフラストラクチャ内の作業ディレクトリの一覧については、DBMS 管理者に確認してください。

次のパス例は、Ubuntu オペレーティングシステムを対象としています。他のオペレーティングシステムでは、ディレクトリが異なる場合があります。

一般的な DBMS に関する推奨事項

PostgreSQL。データファイルおよび先行書き込みログ（WAL ファイル）に対するファイル操作の遅延を完全に排除することが極めて重要です。PostgreSQL プロセスおよびテーブルスペースのファイル操作も除外することを推奨します（以下の例を参照）。一般的な PostgreSQL インストール環境では、これらのファイルは次のディレクトリにあります：

- 統計情報と並列クエリ：`/dev/shm`
- データ：`/var/lib/postgresql/<PostgreSQL version>/main`
- WAL ファイル：`/var/lib/postgresql/<PostgreSQL version>/main/pg_wal`
- 実行ファイル：`/usr/lib/postgresql/<PostgreSQL version>/bin/`。

Postgres Pro。PostgreSQL のガイドラインに従ってください。さらに、`/var/lib/pgpro/<Postgres Pro version>/data` ディレクトリを除外リストに追加してください。

Oracle Database。すべてのデータベースの作業ディレクトリの一覧は、`/etc/oratab` 設定情報ファイルから取得できます。

ScyllaDB。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使用する場合は、トラフィックインターセプトの eBPF モードを使用します。Detection and Response ソリューションのキャッシュモードを管理するには、kesl.ini 設定情報ファイルで `UseIncreasedXdrEventsCache=yes` 設定の既定値を使用します。

PostgreSQL 作業ディレクトリのグローバル除外を設定する例

システムイベントをインターセプトするために*fanotify テクノロジー*に基づくメカニズムを使用している場合、DBMS ファイルのディレクトリはマウントポイントである必要があります。システムイベントをインターセプトするために*更新可能なカーネルモジュール*を使用する場合、マウントポイントを作成する必要はありません。

マウントポイントを作成するには：

1. データベースファイルがあるディレクトリがマウントポイントであるかどうかを確認します：

   ```
   mount
   ```

   ディレクトリが mount コマンドの出力に表示されない場合：

   a. マウントポイントを作成します：

   ```
   mount --bind /var/lib/postgresql/<PostgreSQL version>/main/ /var/lib/postgresql/<PostgreSQL version>/main
   ```

   WAL ファイルのディレクトリはデータディレクトリ内にネストされているため、別のマウントポイントを作成する必要はありません。

   b. 新しく作成したマウントポイントが再起動後もシステムに保持されるように、/etc/fstab ファイルに次の行を追加します：

   ```
   /var/lib/postgresql/<PostgreSQL version>/main /var/lib/postgresql/<PostgreSQL version>/main none
   defaults,bind 0 0
   ```

2. PostgreSQL サービスを再起動します：

```
systemctl restart postgresql
```

作業ディレクトリのグローバル除外を設定するには：

1. ディレクトリをグローバル除外リストに追加します：

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=/var/lib/postgresql/<PostgreSQL version>/main
kesl-control --set-app-settings ExcludedMountPoint.item_0001=/var/lib/postgresql/<PostgreSQL
version>/main/pg_wal
kesl-control --set-app-settings ExcludedMountPoint.item_0002=/usr/lib/postgresql/<PostgreSQL version>/bin/
kesl-control --set-app-settings ExcludedMountPoint.item_0003=/usr/lib/postgresql/<PostgreSQL version>
```

2. テーブルスペースを使用している場合は、それらも除外リストに追加します：

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=<tablespace directory>
```

3. グローバル除外を適用するには、アプリケーションを再起動します：

```
systemctl restart kesl
```

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

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。世界では、毎日、新しいウイルスと他の種類のマルウェアが出現しています。Kaspersky Endpoint Security データベースには、脅威に関する情報と脅威を無効化する方法が格納されています。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。

アプリケーションの導入が成功し、初期設定段階で定義データベースのアップデートを選択した場合、アプリケーションのインストール後、定義データベースは最新の状態になります。Kaspersky Security Center でデバイスの保護ステータスを表示するときにクライアントデバイスのステータスを確認するか、コマンドラインで `kesl-control --app-info` コマンドを使用することで、定義データベースのステータスに関する情報を取得できます。定義データベースが最新の状態でない場合は、定義データベースのアップデートを設定して開始する必要があります。

データベースとモジュールのアップデートの設定

1. **アップデートの配信スキームとアップデート元の選択**

   *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。アップデート元には、カスペルスキーのアップデートサーバー、Kaspersky Security Center 管理サーバーのストレージ、FTP、HTTP、HTTPS サーバー、Samba または NFS プロトコルを使用してユーザーがマウントしたローカルディレクトリまたはネットワークディレクトリのいずれかを指定できます。

   Kaspersky Endpoint Security をLight Agent モードで使用する場合、保護対象仮想マシン上の定義データベースは SVM 上のディレクトリからアップデートされます。

2. **定義データベースのアップデートタスクの設定**

   *アップデートタスク*は、アップデートパッケージをダウンロードし、定義データベースと機能のアップデートをデバイスにインストールします。

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。

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：

- Kaspersky Endpoint Security の定義データベース：定義データベースには、マルウェア検知ルール、ネットワーク攻撃の説明、悪意のある URL およびフィッシングサイトの URL 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、その他のデータが含まれます。
- 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。

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。自動パッチには、アプリケーションの修正と改善が含まれます。

アップデート中、コンピューター上の製品モジュールと定義データベースが、アップデート元にある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。

役立つ記事

製品の定義データベースとモジュールのアップデートに関するトラブルシューティング

ステータス「アプリケーションのアップデートまたは cryptossl モジュールのアップデートがインストールされました。本製品を再起動してください。」

アップデート元と配信方式の選択方法

Kaspersky Endpoint Security のアップデート元の選択

*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。

アップデート元には、カスペルスキーのアップデートサーバー、Kaspersky Security Center 管理サーバーのストレージ、ユーザーがマウントしたローカルまたはネットワーク（SMB/NFS）ディレクトリ、FTP、HTTP、HTTPS サーバーのいずれかを使用できます。アップデート元として独自の HTTPS サーバーを選択する場合は、そのサーバーに正しい証明書チェーンがあることを確認する必要があります。自己署名証明書は、証明書チェーンのルート証明書としてのみ使用できます。この場合、その証明書をデバイス上の信頼済み証明書のリストに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、保護対象仮想マシン上の定義データベースは SVM 上のディレクトリからアップデートされます。

複数のリソースがアップデート元として選択されている場合、Kaspersky Endpoint Security はリストの先頭から順に接続を試行し、最初に 使用可能なアップデート元からアップデートパッケージを取得してアップデートタスクを実行します。選択したアップデート元への接続を試行する際の応答タイムアウトを設定できます。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。

アップデートの配布方式の選択

Kaspersky Endpoint Security では、定義データベースと機能のアップデートについて、次の配布方式をサポートしています：

一元化されたアップデート

組織内のデバイスの保護を一元管理するために Kaspersky Security Center を使用している場合は、定義データベースの一元的なアップデートを設定することを推奨します。一元的なアップデートを使用すると、ネットワーク外部とのインターネットトラフィック量を減らすことができ、なおかつアップデートの監視が容易になります。

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*管理サーバーのリポジトリへのアップデートのダウンロード*タスクを使用して、管理サーバーのリポジトリにダウンロードされます。

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。

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。カスペルスキーのアップデートサーバーの詳細については、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。

ユーザーがマウントし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 サーバーからのアップデート

カスタムアップデート元には、事前にダウンロードしたアップデートパッケージが含まれている必要があります（事前ダウンロードは、たとえばKaspersky Update Utilityを使用して行うことができます）。アップデート元として独自の HTTPS サーバーを選択する場合は、そのサーバーに正しい証明書チェーンがあることを確認する必要があります。自己署名証明書は、証明書チェーンのルート証明書としてのみ使用できます。この場合、その証明書をデバイス上の信頼済み証明書のリストに追加する必要があります。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。カスタムアップデート元の作成の詳細については、Kaspersky Security Center のヘルプを参照してください。

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、プロキシサーバーの設定を指定します。

定義データベースのアップデートタスクを設定する方法

アップデートタスクは、アップデートパッケージをダウンロードし、定義データベースと機能のアップデートをデバイスにインストールします。

Kaspersky Security Center で定義データベースをアップデートする

Kaspersky Security Center では、アップデートタスクは管理サーバークイックスタートウィザードによって自動的に作成されます。ウィザードの実行中に*Update*タスクを作成するには、Kaspersky Endpoint Security 管理プラグインをインストールする必要があります。

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するか、Web コンソールまたは管理コンソールを使用してカスタムのグループアップデートタスクおよびローカルアップデートタスクを作成して実行できます。

> Kaspersky Endpoint Security をLight Agent モードで使用している場合、保護対象仮想マシン上の定義データベースは、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。

Web コンソールでアップデートタスクを設定して実行する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。

   タスクのリストが表示されます。

2. タスクのリストで、Kaspersky Endpoint Security のアップデートタスクを選択し、タスク名をクリックします。

   タスクのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. **アップデート元**セクションで、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のアップデートをアプリケーションが受信するアップデート元を選択します。

   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。アップデート元として、FTP、HTTP、および HTTPS サーバー上のディレクトリ、または保護対象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上のディレクトリ（Samba 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上のディレクトリを含む）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. タスクのプロパティウィンドウで、［**スケジュール**］タブを選択し、アップデートタスクの実行スケジュールを設定します。既定では、このタスクには手動で開始するモードが選択されています。

   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ついて詳しくは、Kaspersky Security Center のヘルプを参照してください。

6. 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。

管理コンソールでアップデートタスクを設定して実行する方法

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. タスクのリストで、アップデートタスクを選択し、ダブル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。

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**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。既定では、このタスクには手動で開始するモードが選択されています。

   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ついて詳しくは、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。

コマンドラインで定義データベースをアップデートする

コマンドラインでは、*Update* の事前定義済みタスクを使用するか、Update タイプのユーザータスクを作成して、定義データベースと機能をアップデートできます。

タスクの設定を変更することで、手動アップデートタスクの管理（開始、停止、一時停止、再開）、タスクスケジュールの設定、およびアップデート設定の管理を行うことができます。

コマンドラインでアップデートタスクを作成して設定する方法

コマンドラインでは、カスタムアップデートタスクを次の 2 つの方法で作成して設定できます：

- タスクのすべての設定を設定情報ファイルで指定して、タスクを作成します。
- デフォルト設定でタスクを作成してから、その設定を行います。

設定情報ファイルから取得した設定でアップデートタスクを作成する

```
kesl-control --create-task <task name> --type <task type> --file <path to file> [--json]
```

説明：

- `<path to file>` は、タスクに使用する設定が含まれ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。

設定情報ファイルの例

```
ConnectionTimeout=10
ApplicationUpdateMode=DownloadOnly
[Sources.item_0000]
Enabled=Yes
SourceType=Custom
URL=https://s00.upd.kaspersky.com
```

デフォルト設定でアップデートタスクを作成して設定するには：

1. 次のコマンドを実行してタスクを作成します：

   ```
   kesl-control --create-task <update task name> --type Update
   ```

   ここで、`<update task name>` は、新しいアップデートタスクに設定する名前です。

   このコマンドは、デフォルト設定でアップデートタスクを作成します。

2. 必要に応じて、次のコマンドを実行してアップデートタスクの設定を管理します。

   ```
   kesl-control --set-settings <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

3. 必要に応じて、次のコマンドを実行してアップデートタスクのスケジュール設定を管理します。

```
kesl-control --set-schedule <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

4. 次のコマンドを実行して、タスク設定の現在の値を確認します。

```
kesl-control --get-settings <update task ID|name>
```

アプリケーションのグラフィカルインターフェイスでの定義データベースのアップデート

グラフィカルインターフェイスでアップデートタスクを開始または停止する方法

1. アプリケーションの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。
   - 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。

Kaspersky Update Utility を使用してアップデートする方法

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製品モジュールのアップデートをロールバックする方法

定義データベースと機能が2回目にアップデートされると、定義データベースと機能を以前のバージョンにロールバックする機能が使用可能になります。

ユーザーがアップデートプロセスを開始するごとに、Kaspersky Endpoint Security によって現在の定義データベースと製品機能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、定義データベースと製品機能を前のバージョンにロールバックすることができます。前回のアップデートへのロールバックは、新しい定義データベースのバージョンによって誤検知が発生し、Kaspersky Endpoint Security が安全なアプリケーションをブロックしてしまうような場合に役立ちます。

Kaspersky Endpoint Security をLight Agent モードで使用している場合、タスクを使用して定義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。

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。

コマンドラインでは、次の方法で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：

- *ロールバック*事前定義済みタスクを実行します。
- *ロールバック*カスタムタスクを作成して実行します。

この*ロールバック*タスクには設定がありません。

Web コンソールで定義データベースと製品モジュールのアップデートをロールバックする方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
   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、アプリケーション名を選択します。
   b. ［**タスク種別**］から［**ロールバック**］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**］で、タスクの範囲の定義方法を選択します。
4. 選択したタスク範囲の定義方法に従ってデバイスを選択します。
5. 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。
6. タスクの横のチェックボックスをオンにし、［**開始**］をクリックします。

管理コンソールで定義データベースと製品モジュールのアップデートをロールバックする方法

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で、リストから Kaspersky Endpoint Security を選択し、タスク種別として**ロールバック**を選択します。

3. 複数のデバイスに対するタスクを作成する場合、ウィザードでタスクを割り当てるデバイスの選択を求められます。タスク範囲の定義方法を選択します。

4. 選択したタスク範囲の定義方法に従ってデバイスを選択します。

5. タスクのスケジュールを設定します。

6. 新しいタスクの名前を入力します。

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。

8. タスクのリストでタスクを選択し、タスクのコンテキストメニューを開いて、**開始**を選択します。

コマンドラインで定義データベースと製品モジュールのアップデートをロールバックする方法

次のコマンドを実行します：

定義データベースと機能のアップデートのロールバック

```
kesl-control --start-task 7
```

グラフィカルインターフェイスで定義データベースと製品モジュールのアップデートをロールバックする方法

1. アプリケーションの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. 定義データベースのアップデートをロールバックするには、**アップデートのロールバック**リンクをクリックします。

ホスト脅威対策

ファイル脅威対策

ファイル脅威対策は、コンピュータに最低限のセキュリティレベルを提供します。このコンポーネントは Kaspersky Endpoint Security と同時に起動し、ファイルをリアルタイムでスキャンします。

ファイル脅威対策の仕組み

1. **アプリケーションはファイル操作イベントをインターセプトし、スキャンが完了するまで操作をブロックします。**

   アプリケーションは、ファイル操作インターセプトメカニズムを使用し、スキャンが完了するまでファイルへのすべてのアクセスをブロックします。

2. **アプリケーションはファイルをスキャンします**

   ファイル脅威対策は、次の技術を使用してファイルをスキャンします：

   - 定義データベース。
   - Kaspersky Security Network のクラウドサービス。
   - ヒューリスティック分析技術により、カスペルスキーの定義データベースではまだ対応していない脅威を検知できます。

3. **スキャンの完了**

   スキャン後、アプリケーションは操作を許可するか、操作をブロックして脅威の検知時に指定された処理を実行します。

ファイル脅威対策の初期設定

初期設定には、基本的なエンドポイント保護に必要な手順が含まれます。

1. **システムイベントインターセプトメカニズムを選択する**

   ファイル脅威対策はファイル操作イベントをインターセプトし、スキャンが完了するまで操作をブロックします。

   アプリケーションのインストール時に、システムイベントインターセプトメカニズムを選択しました：

   - 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
   - fanotify に基づくシステムインターセプトメカニズム
   - fanotify がないオペレーティングシステムにおけるファイル脅威対策用のカーネルモジュール

   システムイベントインターセプトメカニズムの選択は、コンピューターの構成によって異なります。最も高いパフォーマンスを提供するインターセプト技術は、更新可能なカーネルモジュールです。アプリケーションの設定で、このメカニズムを有効にできます。

2. **ファイル脅威対策を設定する**

   既定では、ファイル脅威対策は有効になっており、カスペルスキーのエキスパートが推奨する設定で実行されます。既定の設定により、推奨される保護レベルおよび最適なリソースを使用できます。インフラストラクチャのセキュリティに特別な要件がある場合は、これらの設定を変更できます。

3 保護範囲の設定

既定では、本製品は保護対象デバイス上のすべてのファイルをスキャンします。個別のディレクトリ（たとえば、外部ソースからファイルが自動的にダウンロードされるディレクトリ）のみをスキャンする必要がある場合は、そのディレクトリのみを保護範囲として指定できます。それ以外の場合は、既定の保護範囲のままにし、除外を使用して範囲を細かく調整することを推奨します。

4 マウントポイントをスキャン対象から除外する

マウントポイントをスキャン対象から除外すると、特定のディレクトリでのファイル操作をインターセプトしないようにできます。たとえば、共有ネットワークリソースをスキャン対象から除外し、そのリソースが物理的に保存されているデバイス上で Kaspersky Endpoint Security を使用して保護できます。「ファイル脅威対策とスキャンタスクに関する推奨事項」も参照してください。

5 除外を追加する

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取るのに役立ちます。サードパーティ製ソフトウェアを安定して動作させるため、各ソフトウェアのドキュメントに記載されているファイルとディレクトリを除外に追加してください。

次のオブジェクトを除外することを推奨します：

- データベース。大規模なデータベースのスキャンには多くのリソースが必要です。データベースファイルに頻繁にアクセスすると、スキャンが頻繁に実行されます。
- リソースを大量に消費するプロセスが使用するファイル。このようなファイルをスキャンすると、コンピューターの動作が遅くなります。
- ログファイルを含むディレクトリ。オペレーティングシステムは常にログファイルに書き込みます。その結果、ファイル脅威対策はログのスキャンにコンピューターのリソースを無駄に消費します。

> オブジェクトがファイル脅威対策コンポーネントによってスキャン対象から除外されている場合は、マルウェアのスキャンタスクを使用してそのようなオブジェクトをスキャンすることを推奨します。

高負荷サーバー向けの追加設定

追加設定には、ファイル脅威対策を微調整するための手順が含まれます。初期設定後に遅延が発生した場合、または高負荷サーバーを設定する場合は、次の手順に従ってください：

1 スキャン中のファイルアクセスのブロックを無効にする

既定では、ファイル脅威対策はスキャンが完了するまで、スキャン中のファイルへのすべてのアクセスをブロックします。ブロックモードを無効にすると、ファイル脅威対策は通知モードで動作します。このファイル操作インターセプトモードでは、スキャン中のシステムパフォーマンスへの影響は小さくなりますが、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。

> ブロックモードが無効になっている場合、デバイスコントロール、オブジェクトの実行防止処理、およびリムーバブルドライブスキャンタスクも通知モードで動作します。

2. **ファイルスキャン統計情報を収集する**

   コンピューターの主要なパフォーマンス指標（CPU負荷、サードパーティ製ソフトウェアのパフォーマンス、その他の指標など）を監視します。これは、システムの負荷を軽減する方法を判断するのに役立ちます。

   ファイルスキャン統計情報は、アプリケーションパフォーマンス分析ツールを使用して取得できます。独自の監視ツールを使用することもできます。

3. **アプリケーションのパフォーマンスを最適化する**

   収集した情報を分析した後、アプリケーションのパフォーマンスを最適化します：

   - グローバルの除外リストを追加する
   - 除外を追加する
   - アプリケーション設定を最適化する

4. **スキャン中のファイルアクセスのブロックを有効にする**

   スキャン中のファイルアクセスのブロックを有効にします。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選択した処理を実行します。

特別な考慮事項と制限事項

- 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内のファイルにアクセスできない場合、アプリケーションはすべてのユーザーに対してそのファイルへのアクセスをブロックします。
- ファイル脅威対策とコンテナ監視が有効な場合、アプリケーションはすべての名前空間とコンテナもスキャンします。

保護範囲の作成方法

*保護範囲*とは、Kaspersky Endpoint Security が脅威をスキャンするオブジェクトへのパスのリストです。既定では、本製品は保護対象デバイス上のすべてのファイルをスキャンします。個別のディレクトリのみをスキャンする必要がある場合（たとえば、外部ソースからファイルが自動的にダウンロードされるディレクトリなど）は、そのディレクトリを保護範囲として指定できます。それ以外の場合は、既定の保護範囲のままにし、除外を使用して範囲を細かく調整することを推奨します。

Kaspersky Endpoint Security は、オブジェクトのリストに表示される順序でオブジェクトをスキャンします。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。

Web コンソールでの保護範囲の作成方法

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. ［**ホスト脅威対策**］→［**ファイル脅威対策**］に移動します。

5. ［**保護範囲**］ブロックで、［**追加**］をクリックします。

6. ウィンドウが開きます。このウィンドウで、ファイルシステムの種類を選択します：

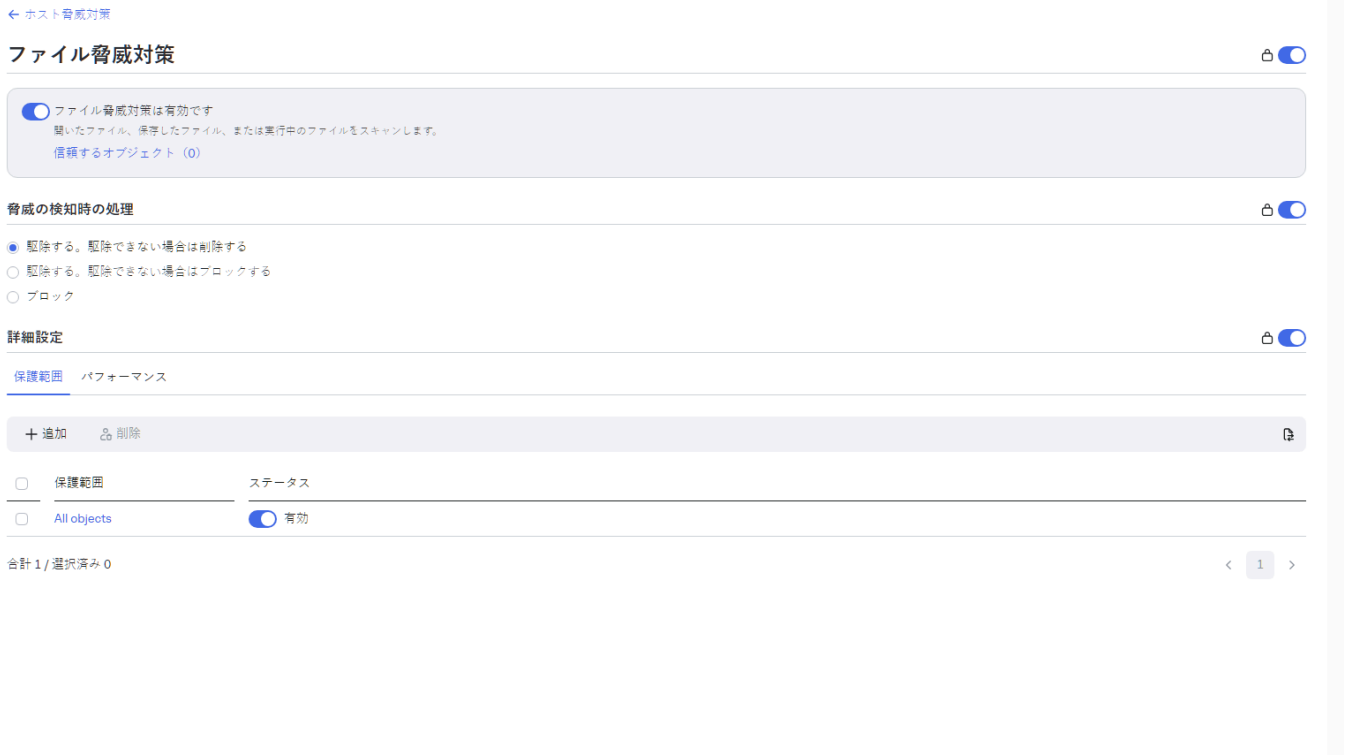
   - **ローカル**ネットワーク接続なしでアクセスできるハードドライブ上のディレクトリ。
   - **マウント済み**マウントされたリモートまたはローカルのディレクトリ。
   - **共有**Samba（SMB）または NFS プロトコルを使用してアクセスできるコンピューターのディレクトリ。
   - **リモートでマウント済みのすべての場所**Samba プロトコルおよび NFS プロトコルを使用してデバイスにマウントされたすべてのリモートディレクトリ。
   - **共有済みのすべての場所**Samba プロトコルおよび NFS プロトコルを使用してアクセスされるすべてのコンピューターのディレクトリ。

7. ローカルファイルシステムの場合は、ディレクトリパスを指定します（例：`/path/to/folder`）。必要に応じて、［**サブフォルダーを含む**］をオンにします。

8. マウント済みまたは共有ファイルシステムのアクセスプロトコルを指定します。

9. オブジェクトの拡張子のマスクを指定します（例：`*.txt`）。マスクはカンマで区切ります。

10. 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。



ファイル脅威対策

コマンドラインでの保護範囲の作成方法

1. 次のコマンドを実行します：

   ```
   kesl-control --set-settings 1 --add-path <path>
   ```

   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。

2. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

   ```
   kesl-control --get-settings 1
   ```

例

```
kesl-control --set-settings 1 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

タスクに次の保護範囲設定が追加されます：

```
[ScanScope.item_0001]
AreaDesc=All object
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

ファイル脅威の検知時の処理を選択する方法

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。ファイル脅威対策の設定では、脅威が検知されたときに Kaspersky Endpoint Security が実行する処理を選択できます。

Web コンソールで脅威の検知時の処理を設定するには

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. ［**ホスト脅威対策**］→［**ファイル脅威対策**］に移動します。

5. 「**脅威の検知時の処理**」で、脅威が検知された場合に本製品が実行する処理を選択します：

- **駆除する。駆除できない場合は削除する**（既定）。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**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**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。

6. 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。

コマンドラインで脅威の検知時の処理を設定するには

1. 次のコマンドを実行します：

```
kesl-control --set-settings 1 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
```

2. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 1
```

記号

コマンドオプション

設定	説明
ActionOnThreat	脅威の検知時の処理： • DisinfectDeleteIfNotPossible（既定）。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。 • DisinfectBlockIfNotPossible 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。 • Block 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。

ファイルスキャンのスマートモードとは

ファイル脅威対策は、開かれた、保存された、または実行されたすべてのファイルをスキャンします。既定では、ファイル脅威対策はスマートモードでファイルをスキャンします。*スマートモード*では、ファイルを開こうとしたときにファイル脅威対策がそのファイルをスキャンします。プロセスが一定期間にわたってファイルに繰り返しアクセスして変更した場合、ファイル脅威対策は、そのプロセスがファイルを閉じたときにのみそのファイルを再スキャンします。これにより、高い保護レベルを提供しながら、本製品がシステムパフォーマンスに与える影響を最小限に抑えます。

スマートモードを機能させるには、更新可能なカーネルモジュールを選択して起動する必要があります。

Web コンソールでは、ファイルスキャンモードを変更できません。

コマンドラインでファイルスキャンモードを選択する方法

1. 次のコマンドを実行します：

```
kesl-control --set-settings 1 ScanByAccessType=<SmartCheck|OpenAndModify|Open>
```

2. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 1
```

記号

コマンドオプション

設定	説明
`ScanByAccessType`	ファイルスキャンモード： • `SmartCheck`（既定値）。ファイル脅威対策はスマートモードでファイルをスキャンします。Kaspersky Endpoint Security は、ファイルが開かれたとき、およびファイルが変更されている場合は閉じられたときに、そのファイルをスキャンします。 スマートモードを使用できない場合、本製品は、ファイルが開かれたとき、およびファイルが変更されるたびにファイルをスキャンします（`OpenAndModify`）。たとえば、更新可能なカーネルモジュールが停止している場合、スマートモードを使用できないことがあります。 • `OpenAndModify` Kaspersky Endpoint Security は、ファイルが閉じられたときだけでなく、ファイルが開かれたとき、およびファイルが変更されるたびに、そのファイルをスキャンします。 • `Open` Kaspersky Endpoint Security は、ファイルを読み取り、実行、または変更のために開こうとしたときに、そのファイルをスキャンします。

ファイルスキャンを最適化する方法

ファイル脅威対策コンポーネントを最適化するには、ファイルスキャンを設定します。これにより、保護対象デバイスの CPU 使用率を低減できます。アーカイブのスキャンを制限し、スキャン可能なオブジェクトの最大サイズとオブジェクトの最大スキャン時間を設定できます。

Web コンソールでファイルスキャンを設定する方法

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. ［**ホスト脅威対策**］→［**ファイル脅威対策**］に移動します。

5. **詳細設定**で、**パフォーマンス**タブを選択し、ファイルスキャンを設定します：

   - **アーカイブのスキャン**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、スキャンは無効になっています。

   - **配布パッケージと自己解凍型アーカイブのスキャン**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。既定では、スキャンは無効になっています。

- **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。既定では、スキャンは無効になっています。

- **メール形式のファイルをスキャン**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。既定では、スキャンは無効になっています。

- **次のサイズを超えるアーカイブをスキャンしない（MB）**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。

- **ファイルの最大スキャン時間（秒）**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。既定では、本製品は1分以内にオブジェクトのスキャンを試行します。

6. 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。

コマンドラインでファイルスキャンを設定する方法

1. 次のコマンドを実行します：

```
kesl-control --set-settings 1 ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<Object size (MB)>
TimeLimit=<Scan time (sec)>
```

2. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 1
```

記号

コマンドオプション

設定	説明
ScanArchived	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、スキャンは無効になっています。
ScanSfxArchived	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。既定では、スキャンは無効になっています。
ScanMailBases	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。既定では、スキャンは無効になっています。
ScanPlainMail	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。既定では、スキャンは無効になっています。
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。最新のスキャン後 10 分以内にテキストファイルが同じプロセスによって再利用された場合、本製品はテキストファイルをスキャンしません。既定では、スキャン対象からの除外は無効になっています。 この設定は、システムイベントをインターセプトする fanotify メカニズムをサポートするデバイスを対象としています。更新可能なカーネルモジュールを搭載したデバイスでは、本製品は負荷を最適化するためにスキャン結果キャッシュを使用します。

設定	説明
`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。最新のスキャン後 10 分以内にジャーナルファイルが同じプロセスによって再利用された場合、本製品はデータベースジャーナルファイルをスキャンしません。既定では、スキャン対象からの除外は無効になっています。 この設定は、システムイベントをインターセプトする fanotify メカニズムをサポートするデバイスを対象としています。更新可能なカーネルモジュールを搭載したデバイスでは、本製品は負荷を最適化するためにスキャン結果キャッシュを使用します。
`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。（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。既定では、本製品は 1 分以内にオブジェクトのスキャンを試行します。（値：`60`）。

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（Soft linkとも呼ばれます）は、別のファイルまたはディレクトリを指すファイルです。シンボリックリンクと、そのリンクが指すファイルは、異なるファイルシステム上に存在できます。また、このようなリンクは存在しないファイルを指す場合があります。対象ファイルを削除しても、リンク自体は削除されませんが、機能しなくなります。

*Hard link*は、基本的にファイルの別名です。ハードリンクは、ファイルのメタデータを含むファイルのインデックス記述子（inode）を指します。ファイルへのハードリンクが少なくとも 1 つ残っている限り、そのファイルはファイルシステム内に存在し続けます。

シンボリックリンクのスキャン

シンボリックリンクが指すファイルがファイル脅威対策の保護範囲内にある場合にのみ、アプリケーションはシンボリックリンクをスキャンします。

ファイルが保護範囲外にある場合、アプリケーションはシンボリックリンクをたどってファイルの内容をスキャンすることはありません。ただし、ファイルに悪意のあるコードが含まれている場合、デバイスのセキュリティは危険な状態になります。

ハードリンクのスキャン

複数のハードリンクが指しているファイルで悪意のあるコードが検知された場合、アプリケーションは元のファイルを駆除します。駆除が 不可能であると判明した場合、アプリケーションは ハードリンクを 削除し、その 場所に ソース ファイルの コピーを、削除された リンクの 名前で バックアップに 作成します。アプリケーションは処理中のハードリンクのみを削除し、同じデータを指している可能性がある残りのハードリンクはそのまま残ります。

バックアップからハードリンクを復元すると、アプリケーションは、復元するハードリンクの名前で元のファイルのコピーを元の場所に作成します。復元されたリンクは元のファイルへのハードリンクにはならず、同じファイルへの他のハードリンクから独立したままになります。

プロセスによる除外でのシンボリックリンクの解決

`ExcludedForProgram` セクションの `ProgramPath` パラメータで指定されたパスがバイナリ実行ファイルへのシンボリックリンクである場合、本製品はリンク先ファイルのパスに除外を適用します。このルールは、明示的に指定されたリンクだけでなく、このファイルへのすべてのリンクに適用されます。このパラメータではプログラムイメージへのパスが使用されるため、スクリプトへのシンボリックリンク（`.sh` など）は解決されません。

タスクの実行時にリンク先ファイルが特定され、設定が適用されます。リンクが存在しないファイルを指している場合、リンク自体のパスが除外に含まれます。リンクが同じ名前の通常の実行ファイルに置き換えられた場合、除外はそのファイルに適用されます。

シンボリックリンクを使用した除外の例

```
[ExcludedForProgram.item_0000]
ProgramPath=/usr/bin/md5sum
UseExcludedForProgram=Yes
Path=/root/s1
```

タスクの開始時点では、`/usr/bin/md5sum` リンクは `/bin/coreutils` を指しているため、`/bin/coreutils` が除外に追加されます。リンクが後で `/bin/false` にリダイレクトされた場合、タスクが再起動されるまで除外は `/bin/coreutils` に適用されたままとなり、`/bin/false` には適用されません。タスクが再起動されると、除外は `/bin/coreutils` ではなく `/bin/false` に適用されます。

マルウェアのスキャン

マルウェアのスキャンは、コンピューターのセキュリティに必要不可欠です。スキャンを定期的に実行することで、セキュリティレベルの設定が低いなどの理由により、保護機能で検知されない悪意のあるソフトウェアが拡散する可能性を排除できます。

Kaspersky Endpoint Security には、標準の *マルウェアのスキャン*タスクがあらかじめ定義されています。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。

管理サーバー初期セットアップウィザードにより、*マルウェアのスキャン*タスクが自動的に作成されます。*マルウェアのスキャン*タスクを作成するには、ウィザードの実行中に Kaspersky Endpoint Security for Linux 管理プラグインをインストールします。必要に応じて、*マルウェアのスキャン*種別のユーザータスクを作成できます。

［マルウェアのスキャン］タスクの設定

1. **タスクの実行スケジュールを設定する**

   スキャン中、Kaspersky Endpoint Security は通常よりも多くのコンピューターリソースを使用する場合があります。スキャンタスクをスケジュールする際は、コンピューターの負荷が最も低い時間帯に設定することを推奨します。

2 スキャンによるシステム負荷の最適化

マルウェアのスキャンタスクの実行中、CPU 使用率を制限できます。これにより、コンピューターのスキャンにかかる時間が長くなる可能性があります。

Kaspersky Endpoint Security では、ノートパソコンがバッテリー電源で動作している場合、スケジュールされたタスクをキャンセルできます。

3 マルウェアのスキャンタスクの設定を構成する

既定では、マルウェアのスキャンタスクでは、カスペルスキーのエキスパートが推奨する設定が使用されます。既定の設定により、推奨される保護レベルおよび最適なリソースを使用できます。インフラストラクチャのセキュリティに関する特別な要件がある場合は、これらの設定を変更できます。

> 既定では、本製品はアーカイブをスキャンします。このため、本製品はアーカイブを /tmp ディレクトリに展開します。アーカイブを展開するための十分な空き容量がコンピューターにあることを確認してください。

4 スキャン範囲を設定する

既定では、本製品は保護対象デバイス上のすべてのファイルをスキャンします。個別のディレクトリ（たとえば、外部ソースからファイルが自動的にダウンロードされるディレクトリ）のみをスキャンする必要がある場合は、そのディレクトリのみをスキャン範囲として指定できます。その他の場合は、既定のスキャン範囲を維持し、除外を使用して範囲を微調整することを推奨します。

> サーバーをスキャンする場合は、スキャン範囲を複数のサブ範囲に分割し、サブ範囲ごとに個別のマルウェアのスキャンタスクを作成することを推奨します。負荷を分散させるため、タスクごとに異なる開始時刻をスケジュールしてください。

5 スキャンの除外を追加する

除外範囲を設定します：

- **スキャンの除外**。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取るのに役立ちます。サードパーティ製ソフトウェアを安定して動作させるには、該当するソフトウェアのドキュメントに記載されているファイルとディレクトリを除外に追加してください。

  ファイル脅威対策コンポーネントの除外範囲を既に作成している場合は、その除外をマルウェアのスキャンタスクにも適用できます。

- **グローバル除外リスト**。マウントポイントを除外（グローバル除外）すると、特定のディレクトリでのファイル操作をインターセプトしないようにできます。共有ネットワークリソースをスキャン範囲から除外します。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。

6 マルウェアのスキャンタスクを実行する

Web コンソールでマルウェアのスキャンタスクを実行する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。

   タスクのリストが表示されます。

2. Kaspersky Endpoint Security の マルウェアのスキャンタスクを選択します。

   タスクのプロパティウィンドウが表示されます。

   マルウェアのスキャンタスクは管理サーバークイックスタートウィザードによって自動で作成されます。マルウェアのスキャンタスクを作成するには、ウィザードの実行中に Kaspersky Endpoint Security for Linux 管理プラグインをインストールします。

必要に応じて、マルウェアのスキャン種別のユーザータスクを作成できます。

3. ［**設定**］タブで、タスク設定を管理します。

4. ［**アプリケーション設定**］タブで、アプリケーションの詳細を設定します（下記の表を参照）。

5. ［**スケジュール**］タブで、タスクの開始方法を設定します。
   デフォルトでは、Kaspersky Endpoint Securityはタスクを手動で実行するように設定されています。

6. 変更内容を保存します。

7. タスクを実行します。

［マルウェアのスキャン］タスクの設定

設定	説明
スキャン範囲	タスクによってスキャンされた範囲を示す表。既定では、アクティブなスキャン範囲は1つだけで、ローカルファイルシステムのすべてのディレクトリが含まれます。スキャン範囲は手動で追加できます。
脅威の検知時の処理	• **駆除する。駆除できない場合は削除する**（既定値）：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。
アーカイブをスキャン	このオプションをオンにすると、本製品はアーカイブをスキャンします。 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。［**ファイルの最大スキャン時間（秒）**］および［**次のサイズを超えるファイルをスキャンしない（MB）**］の設定を指定することで、アーカイブスキャンの所要時間を短縮できます。 既定で、このオプションはオンです。
配布パッケージと自己解凍型アーカイブのスキャン	このオプションをオンにすると、本製品は自己解凍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。 既定で、このオプションはオンです。
メール形式のファイルをスキャン	このオプションを有効にすると、本製品はテキスト形式のメールメッセージをスキャンします。 この機能は既定で無効になっています。
メールデータベースをスキャン	このオプションをオンにすると、本製品は Microsoft Outlook、Outlook Express、The Bat!、その他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します。 この機能は既定で無効になっています。
次のサイズを超えるファイルをスキャンしない（MB）	スキャン可能な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。 可能な値：1～999999。既定では、この制限は無効です。
ファイルの最大スキャン時間（秒）	ファイルごとの最大スキャン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。 可能な値：1～9999。既定では、この制限は無効です。
同時に複数のスキャンタスクを実行しない	スキャンが既に実行中の場合はスキャンタスクの開始を遅延します。現在のスキャンが続行される場合は Kaspersky Endpoint Security は新しいスキャンタスクをエンキューします。これは、コンピューターの負荷の最適化に役立ちます。たとえば、本製品がスケジュールに従って完全スキャンタスクを開始していたとします。ユーザーが製品インターフェイスから簡易スキャンを開始しようとすると、Kaspersky Endpoint Security はこの簡易キャンタスクをエンキューし、完全スキャンタスクの完了後にこのタスクが自動的に開始されます。 この機能は既定で無効になっています。

設定	説明
iChecker を使用する	このオプションをオンにすると、本製品は前回のスキャン以降に新規作成または変更されたファイルのみをスキャンします。 このオプションをオフにすると、本製品は作成日または変更日に関係なくファイルをスキャンします。 既定で、このオプションはオンです。

コマンドラインでマルウェアのスキャンタスクを実行する方法

1. 既定では、本製品には［マルウェアのスキャン］（*Scan_My_Computer*）タスクがあります。新しいマルウェアのスキャン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 <task name> --type ODS
```

ここで、`<task name>`は、新しいタスクに設定する名前です。

このコマンドは、作成されたタスクの ID を返します。

2. 必要に応じて、次のコマンドを使用してタスク設定を変更します（下の表を参照）：

```
kesl-control --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

タスク設定の変更例

```
kesl-control --set-settings 101 ScanFiles=No
```

設定情報ファイルを使用してタスク設定を管理することもできます。

3. 必要に応じて、タスクのスケジュールを設定します。既定では、タスクは手動で開始されます。

4. タスク設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings <task ID|name>
```

5. マルウェアのスキャンタスクを実行するには、次のコマンドを実行します：

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

コマンドの例

```
kesl-control --start-task 2 -W
```

6. マルウェアのスキャンタスクを停止するには、次のコマンドを実行します：

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

記号

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	スキャン対象を self-extracting archivesのみ（実行可能な 解凍モジュールを含むアーカイブ）にします。	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	plain text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。 既定値です：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。 既定値です：0.
QueueScanTasks	以前に開始されたスケジュール済みスキャンがまだ実行中の場合、スケジュール済みスキャンタスクの実行を延期します。現在のスキャンが続行されている場合、Kaspersky Endpoint Security はスケジュール済みスキャンタスクをキューに追加します。これは、コンピューターの負荷の最適化に役立ちます。例えば、スキャンタスクが 18:00 と 20:00 に実行されるようにスケジュールされているとします。18:00 のスキャンがまだ実行中の場合、20:00 に実行されるようにスケジュールされているスキャンタスクは延期されます。延期されたタスクは、18:00 のタスクが完了した後に実行されます。	Yes：現在のスキャンがまだ実行中の場合、スケジュール済みスキャンタスクをキューに追加します。 No（既定値）：現在のスキャンがまだ実行中の場合でも、スケジュール済みスキャンタスクを実行します。

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。	DisinfectDeleteIfNotPossibl（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。 DisinfectInformIfNotPossibl（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。 既定値です：DisinfectDeleteIfNotPossibl
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。 <device name mask> – 指定され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。 既定値です：/** – 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。	既定値です：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。

設定	説明	値
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_0000=*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。	<path to local directory> – 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。 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。	既定値です：* （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。 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た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。

グラフィカルインターフェイスからマルウェアのスキャンタスクを実行する方法

1. アプリケーションの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. ［**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. 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。
4. スキャンタスクを停止するには、停止するスキャンタスクの下にある［**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。
5. 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。

感染したオブジェクトが検知された場合、またはスキャンタスクが完了した場合、対応する通知が表示されます。

［**スキャン**］ウィンドウには、一時的なブートセクタースキャンタスク（*Scan_Boot_Sectors_{ID}*）と一時的なカスタムファイルスキャンタスク（*Scan_File_{ID}*）の進行状況と結果も表示されます。

7 **コンピューターのスキャン統計情報を収集する**

レポートを使用して、コンピューターのスキャン統計情報を取得できます。スキャンの所要時間が許容範囲内であることを確認してください。検知されたオブジェクトを確認し、信頼できるオブジェクトである場合は除外リストに追加します。

特別な考慮事項と制限事項

- 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、本製品はスキャン中に該当するファイルをスキップします。
- 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。
- マルウェアのスキャン中にユーザーまたはウォッチドッグサービスがアプリケーションを再起動した場合、またはスキャン中にコンピューターが再起動された場合、スキャンは停止します。次回マルウェアのスキャンを開始すると、最初から開始されます。

役立つ記事

デバイスの空きディスク容量が不足した場合の対処方法

スキャン範囲を作成する方法

スキャン*範囲*とは、Kaspersky Endpoint Security が脅威の有無をスキャンするオブジェクトへのパスのリストです。既定では、本製品は保護対象デバイス上のすべてのファイルをスキャンします。個別のディレクトリのみをスキャンする必要がある場合（たとえば、外部ソースからファイルが自動的にダウンロードされるディレクトリ）、このディレクトリをスキャン範囲として指定できます。

Kaspersky Endpoint Security は、オブジェクトのリストに表示される順序でオブジェクトをスキャンします。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。

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。

Web コンソールでのスキャン範囲の作成

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。

   タスクのリストが表示されます。

2. スキャン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。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**スキャン範囲**］セクションで、［**追加**］をクリックします。

5. ［**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で、ファイルシステムの種別を選択します：

   - **ローカル**ネットワーク接続なしでアクセスできるハードドライブ上のディレクトリ。
   - **マウント済み**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。
   - **共有**Samba（SMB）または NFS プロトコルを使用してアクセスできるコンピューターのディレクトリ。
   - **リモートでマウント済みのすべての場所**Samba プロトコルおよび NFS プロトコルを使用してデバイスにマウントされた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 プロトコルおよび NFS プロトコルを使用してアクセスされるすべてのコンピューターのディレクトリ。

6. **マウント済み** および **共有** ファイルシステム種別について、アクセスプロトコルを選択します：

   - **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**。NFS または Samba 以外の種別のデバイス上のファイルシステムリソース（例：`ext4` または `parsecfs`）。

7. ディレクトリへのパスまたはパスマスクを指定します。

8. 必要に応じて、オブジェクト名のマスクを指定します（例：`*.txt` または `report_*`）。マスクはカンマで区切ります。

9. ［**追加**］をクリックします。

   新しいオブジェクトがスキャン範囲に追加されます。オブジェクトのリストから削除せずに、スキャン範囲からオブジェクトを除外できます。そのためには、オブジェクトの横にあるトグルスイッチをオフにします。

10. 必要に応じて、スキャン範囲内の定義済みオブジェクトを有効または無効にします：

    - **カーネルメモリ**。 **実行中のプロセスのメモリ**。
    - **実行中のプロセスおよびスタートアップオブジェクト**
    - **ディスクブートセクター**

- **すべてのハードディスク**
- **すべてのネットワークドライブ**

11. 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。

コマンドラインでのスキャン範囲の作成

1. 次のコマンドを実行します：

```
kesl-control --set-settings 2 --add-path <path>
```

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。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す。

例

```
kesl-control --set-settings 2 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=All objects
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

2. NFS または Samba 以外の特定の種別のマウント済みファイルシステムのリソース（例： `parsecfs`）をスキャン範囲に含める場合は、 `Path` パラメータでファイルシステム種別を指定します：Path=<ファイルシステム種別>

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がスキャンされます。

例

```
kesl-control --set-settings 2 ScanScope.item_0002.UseScanArea=Yes ScanScope.item_0002.Path=parsecfs
```

タスクに次のスキャン範囲設定が追加されます：

```
[ScanScope.item_0002]
AreaDesc=All objects
UseScanArea=Yes
Path=parsecfs
AreaMask.item_0000=*
```

3. タスク設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 2
```

スキャンスケジュールを設定する方法

タスク マルウェアのスキャンを実行すると、コンピューターのリソース使用率が増加する可能性があります。使用中のユーザーのコンピューターのパフォーマンスに Kaspersky Endpoint Security が与える影響を最小限に抑えるため、最適な時間にタスクを実行するようにスケジュール設定できます。

たとえば、組織の従業員が一定の勤務時間で働いている場合、スキャンを夜間または週末に実行するように設定できます。何らかの理由（その時刻にコンピューターの電源が入っていない場合など）でスキャンを実行できない場合、スキップされたタスクが実行可能になり次第自動的に実行されるように設定できます。

コンピュータのスキャンを実行する最適なスケジュールを決定できない場合は、 マルウェアのスキャンタスクを特定の時刻だけでなく、アプリケーションの起動時、アップデートのリポジトリへのダウンロード時、ウイルス攻撃の検知時、別のタスクの完了時など、特定の条件に基づいて実行することもできます。また、Wake-on-LAN機能を使用して、タスクの開始直前に、電源がオフになっているコンピュータの電源をオンにすることもできます。Wake-on-LAN を使用したスキャンの実行を設定できるのは、 Kaspersky Security Center の マルウェアのスキャンのみです。製品インターフェイスではコンピューターのスキャンの Wake-on-LAN を有効にすることはできません。

Web コンソールでマルウェアのスキャンタスクを実行する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。

   タスクのリストが表示されます。

2. スキャン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。

3. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。

4. スキャンタスクのスケジュールを設定します。

5. 選択した頻度に応じて、タスクの実行スケジュールの詳細設定を指定します（下の表を参照してください）。

6. 変更内容を保存します。

スキャンスケジュールの設定

設定	説明
タスク開始	**手動**都合の良いときに手動でスキャンを開始できる実行方法です。 スケジュールで指定：このスキャンタスク実行方法では、スキャンタスクは作成したスケジュールに従って実行されます。このスキャンタスク実行方法を選択した場合でも、スキャンタスクを手動で開始することもできます。
未実行のタスクを実行する	このチェックボックスをオンにすると、スキップされたタスクは実行可能になると同時に開始されます。タスクの開始時間にコンピューターの電源がオフになっていた場合などに、タスクがスキップされることがあります。本製品は、実行されなかったタスクを実行する機会を得ると、コンピューターの負荷を分散するために、一定の期間内でランダムにタスクを実行します。 このチェックボックスをオフにすると、スキップされたタスクは開始されません。代わりに、現在のスケジュールに従って、次のタスクが実行されます。
タスクの開始を自動的かつランダムに遅延させる	このチェックボックスがオンの場合、タスクはスケジュールに厳密に従わず、特定の間隔でランダムに、つまりタスクの開始時刻は分散して実行されます。ランダムに開始することで、タスクがスケジュール通りに実行されることにより、多数のコンピューターから同時に管理サーバーにアクセスが集中することを避けられます。 ランダムに開始されるタスクの開始時刻の範囲は、タスクが作成された際、そのタスクが割り当てられたコンピューターの数に基づいて自動的に計算されます。それ以降、タスクは算出された開始時刻に実行されます。しかし、タスクの設定が変更されたり手動で実行された場合は、計算される開始時刻は変更されます。 チェックボックスがオフの場合、タスクはスケジュールされた時刻に実行されます。
タスクの開始を次の時間範囲内で自動的かつランダムに遅延させる（分）	このチェックボックスをオンにすると、タスクは特定の時間枠内のランダムな時間にコンピューター上で実行されます。ランダムに開始することで、タスクがスケジュール通りに実行されることにより、多数のコンピューターから同時に管理サーバーにアクセスが集中することを避けられます。 チェックボックスがオフの場合、タスクはスケジュールされた時刻に実行されます。
Wake on LAN の機能を使用してタスク開始前にデバイスを起動する	このチェックボックスがオンの場合、コンピューターのオペレーティングシステムの起動が完了するまで指定した時間をおいてからタスクが実行されます。既定の時間は 5 分です。 電源がオフのコンピューターも含めてすべてのコンピューターでタスクを実行する場合はこのチェックボックスをオンにしてください。

設定	説明
タスク完了後にデバイスをシャットダウンする	このチェックボックスをオンにすると、タスクの完了後にコンピューターがシャットダウンします。たとえば、この機能を有効にして、金曜日の勤務時間後にコンピューターをスキャンできます。タスクが終了すると、本製品によって週末の間コンピューターの電源がオフになります。
次の時間を超える場合はタスクを停止する	タスクの実行時間を制限します。指定した時間が経過すると、Kaspersky Endpoint Security のタスクが停止します。タスクは完了としてマークされません。次回 Kaspersky Endpoint Security でタスクを実行する際に、タスクは最初からスケジュール通り実行されます。

コマンドラインでマルウェアのスキャンタスクのスケジュールを設定する方法

タスクを特定の時刻に 1 回だけ実行するには、次のコマンドを実行します：

```
kesl-control --set-schedule 2 RuleType=Once StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>'
```

タスクを毎月実行するには、次のコマンドを実行します：

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='<hh>:<mm>:<ss>;<day of the month>'
```

タスクを特定の曜日に実行するには、次のコマンドを実行します：

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='<hh>:<mm>:<ss>;<day of the week>'
```

タスクを一定の日数間隔で実行するには、次のコマンドを実行します：

```
kesl-control --set-schedule 2 RuleType=Daily StartTime='<hh>:<mm>:<ss>;<interval between runs (in days)>'
```

特定の日付から一定の時間間隔でタスクを実行するには、次のコマンドを実行します：

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>;
<interval between runs (in hours)>'
```

特定の日付から一定の間隔でタスクを実行するには、次のコマンドを実行します：

```
kesl-control --set-schedule 2 RuleType=Minutely StartTime='<hh>:<mm>:<ss>;<interval between runs (in minutes)>'
```

本製品の起動直後にタスクを実行するには、次のコマンドを実行します：

```
kesl-control --set-schedule 2 RuleType=PS
```

定義データベースがアップデートされた直後にタスクを実行するには、次のコマンドを実行します：

```
kesl-control --set-schedule 2 RuleType=BR
```

タスクのスケジュール設定を無効にするには、次のコマンドを実行します：

```
kesl-control --set-schedule 2 RuleType=Manual
```

タスクのその他のスケジュール設定を管理するには、次のコマンドを実行します：

```
kesl-control --set-schedule 2 RandomInterval=<time interval (minutes)> RunMissedStartRules=<Yes|No>
UseWorkingTimeout=<Yes|No> WorkingTimeout=<maximum task completion time (minutes)> QueueScanTasks=<Yes|No>
```

タスク設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-schedule 2
```

記号

タスクの開始スケジュール設定

設定	説明
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。この設定の形式は、RuleType によって異なります。 可能な値： • <year>：1970 から 2099 • <month>：JAN、FEB、MAR、APR、MAY、JUN、JUL、AUG、SEP、OCT、NOV、DEC。 • <day of the month>：1 から 31 • <day of the week>：Mon、Tue、Wed、Thu、Fri、Sat、Sun。 • <hh>：0 から 23 • <mm>：0 から 59 • <ss>：0 から 59 • <interval between runs (in days)>：0 から 364 • <interval between runs (in hours)>：0 から 23 • <interval between runs (in minutes)>：0 から 59
RandomInterval	一定の時間間隔内（0 から指定値まで）で、コンピューター上のタスクをランダムに実行します。これにより、複数のタスクが同時に開始されることを回避できます。 既定値です：99 分。 可能な値：0～999。
RunMissedStartRules	本製品を起動後にミスタスクを実行します。 • Yes（既定値）は、未実行のタスクの実行が有効になっていることを意味します。スケジュールされたタスクの実行中に製品が停止した場合、またはコンピューターの電源がオフになった場合、Kaspersky Endpoint Security は製品の起動直後にそのタスクを開始します。これにより、重要なタスクの実行漏れを防ぐことができます。 • No は、未実行のタスクの実行が無効になっていることを意味します。スケジュールされたタスクの実行中に製品が停止した場合、またはコンピューターの電源がオフになった場合、製品はそのタスクをスキップします。これにより、製品の起動時に余分な負荷が発生することを回避できます。
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。

設定	説明
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）。 既定値です：120 分。 可能な値：1～999。

スキャンタスクを 10 時間ごとに実行する例

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='2030/May/28 12:00:00;10'
```

毎月 15 日にスキャンタスクを実行する例

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='12:00:00;15'
```

毎週火曜日にタスクを実行する例

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='12:00:00;Tue'
```

個々のファイルまたはディレクトリをスキャンする方法

Kaspersky Endpoint Security では、コマンドラインを使用して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実行できます。たとえば、ファイル脅威対策によるスキャンが既定で無効になっているアーカイブを選択してスキャンできます。

既定では、本製品は、カスペルスキーのエキスパートが推奨する*Scan_File（ID：3）タスクの設定*を使用してファイルをスキャンします。既定の設定により、推奨される保護レベルと最適なリソース使用量が提供されます。既定では、本製品は感染したオブジェクトのコピーをバックアップに保存し、その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。脅威の検知時に別の処理を選択し、その他のタスク設定を管理できます。

コマンドラインで個別のファイルまたはディレクトリのスキャンを開始する方法

```
kesl-control --scan-file <path to the file or directory>
```

その結果、Kaspersky Endpoint Security は次の形式のレポートを生成します：

スキャン済みのオブジェクト： N

検知されたオブジェクトの総数： N

感染したオブジェクトとその他のオブジェクト： N

駆除されたオブジェクト： N

バックアップに移動： N

削除されたオブジェクト： N

駆除されていないオブジェクト： N

スキャンでエラーが発生した： N

パスワードで保護されているオブジェクト: N

スキップされたオブジェクト: N

Cloud Sandbox による検知: N

オブジェクトスキャンタスクを最適化する方法

オブジェクトスキャンを最適化するため、複数のタスクの同時起動を制限できます。ユーザーが同時に多数のオブジェクトスキャンタスクを実行しようとした場合、アプリケーションは上限を超えるタスクを実行しません。これにより、クライアントデバイスのリソース使用率を制御し、たとえばサーバーへの過剰な負荷を回避できます。既定では、オブジェクトスキャンタスク数の上限は 100 に設定されています。

Kaspersky Endpoint Security は、非特権ユーザーに対してのみタスクを制限します。root 権限を持つユーザーは、制限なしでオブジェクトスキャンタスクを実行できます。

コマンドラインで、アプリケーションの全般設定を使用してオブジェクトスキャンタスクの上限を設定できます。管理コンソールまたは Web コンソールでは、タスクの上限を設定できません。

コマンドラインでオブジェクトスキャンタスクを最適化する方法

```
kesl-control --set-app-settings LimitNumberOfScanFileTasks=<number of tasks>
```

簡易スキャン

特別なスキャンタスクを使用すると、コンピューターの重要な領域のみをスキャンできます：*簡易スキャン*簡易スキャンは、マルウェアが最も頻繁に検知されるコンピューターの領域をすばやくスキャンします。このタスクのスキャン範囲には、ブートセクター、スタートアップオブジェクト、カーネルメモリ、実行中のプロセスが含まれます。

コンピューターの重要な領域の侵害に成功したマルウェアは、検知を回避しながらその機能を実行できます。既定では、本製品はカスペルスキーのエキスパートが推奨する設定でタスクを実行します。既定の設定により、推奨される保護レベルと最適なリソース使用量が提供されます。

カスペルスキーのエキスパートは、*簡易スキャン*タスクの既定の設定を変更しないことを推奨しています。

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、本製品はスキャン中に該当するファイルをスキップします。

管理サーバー初期セットアップウィザードにより、*簡易スキャン*タスクが自動的に作成されます。*簡易スキャン*タスクを作成するには、ウィザードの実行中に Kaspersky Endpoint Security for Linux 管理プラグインをインストールします。必要に応じて、*簡易スキャン*種別のユーザータスクを作成できます。

Web コンソールで簡易スキャンを実行する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。

   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、**Kaspersky Endpoint Security for Linux** を選択します。

   b. ［**タスク種別**］から［**簡易スキャン**］を選択します。

   c. ［**タスク名**］に、たとえば *コンピューター感染後の簡易スキャン* などの簡単な説明を入力します。

   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

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。次のステップに進みます。

5. ウィザードを終了します。

6. スキャン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。

7. ［**アプリケーション設定**］タブを選択します。

8. スキャンタスクを設定します（下の表を参照）。

9. 必要に応じて、［**スケジュール**］タブでタスクの開始スケジュールを設定します。

10. 変更内容を保存します。

11. スキャンタスクを実行します。

［簡易スキャン］タスクの設定

設定	説明
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。既定では、スキャン範囲には、ローカルファイルシステムのすべてのディレクトリ、カーネルメモリ、実行中のプロセスのメモリ、スタートアップオブジェクト、ブートセクターが含まれます。
脅威の検知時の処理	• **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。
アーカイブをスキャン	このオプションをオンにすると、本製品はアーカイブをスキャンします。 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。［**ファイルの最大スキャン時間（秒）**］および［**次のサイズを超えるファイルをスキャンしない（MB）**］の設定を指定することで、アーカイブスキャンの所要時間を短縮できます。 既定で、このオプションはオンです。
配布パッケージと自己解凍型アーカイブのスキャン	このオプションをオンにすると、本製品は自己解凍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。 既定で、このオプションはオンです。
メール形式のファイルをスキャン	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。 この機能は既定で無効になっています。

設定	説明
メールデータベースをスキャン	このオプションをオンにすると、本製品は Microsoft Outlook、Outlook Express、The Bat!、その他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します。 この機能は既定で無効になっています。
次のサイズを超えるファイルをスキャンしない（MB）	スキャン可能な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。 可能な値：0～9999。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。 この機能は既定で無効になっています。
ファイルの最大スキャン時間（秒）	ファイルごとの最大スキャン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。 可能な値：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。 この機能は既定で無効になっています。
同時に複数のスキャンタスクを実行しない	スキャンが既に実行中の場合はスキャンタスクの開始を遅延します。現在のスキャンが続行される場合は Kaspersky Endpoint Security は新しいスキャンタスクをエンキューします。これは、コンピューターの負荷の最適化に役立ちます。たとえば、本製品がスケジュールに従って完全スキャンタスクを開始していたとします。ユーザーが製品インターフェイスから簡易スキャンを開始しようとすると、Kaspersky Endpoint Security はこの簡易キャンタスクをエンキューし、完全スキャンタスクの完了後にこのタスクが自動的に開始されます。 この機能は既定で無効になっています。
iChecker を使用する	このオプションをオンにすると、本製品は前回のスキャン以降に新規作成または変更されたファイルのみをスキャンします。 このオプションをオフにすると、本製品は作成日または変更日に関係なくファイルをスキャンします。 既定で、このオプションはオンです。

コマンドラインで簡易スキャンタスクを実行する方法

1. 必要に応じて、タスクの設定を行います（下の表を参照）。

```
kesl-control --set-settings 4 <setting name>=<setting value>
```

2. 必要に応じて、タスクのスケジュールを設定します。

3. タスク設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 4 [--json]
```

`--json` はJSON形式でのデータ出力を意味します。

4. タスクを実行するには、次のコマンドを実行します：

```
kesl-control --start-task 4 [-W] [--progress]
```

説明：

- `[-W]` は、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]`：タスクの進行状況を表示します。

必要に応じて、*簡易スキャンタイプの*ユーザータスクを作成することができます。

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	スキャン対象を self-extracting archivesのみ（実行可能な 解凍モジュールを含むアーカイブ）にします。	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	plain text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。 既定値です：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。 既定値です：0.
QueueScanTasks	以前に開始されたスケジュール済みスキャンがまだ実行中の場合、スケジュール済みスキャンタスクの実行を延期します。現在のスキャンが続行されている場合、Kaspersky Endpoint Security はスケジュール済みスキャンタスクをキューに追加します。これは、コンピューターの負荷の最適化に役立ちます。例えば、スキャンタスクが 18:00 と 20:00 に実行されるようにスケジュールされているとします。18:00 のスキャンがまだ実行中の場合、20:00 に実行されるようにスケジュールされているスキャンタスクは延期されます。延期されたタスクは、18:00 のタスクが完了した後に実行されます。	Yes：現在のスキャンがまだ実行中の場合、スケジュール済みスキャンタスクをキューに追加します。 No（既定値）：現在のスキャンがまだ実行中の場合でも、スケジュール済みスキャンタスクを実行します。

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。 既定値です：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。 <device name mask> – 指定され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。 既定値です：/** – 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。	既定値です：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。

設定	説明	値
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_<item number>=*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。	<path to local directory> – 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。 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。	既定値です：*（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。 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。

役立つ記事

マスクを指定する方法

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：/dir/*/file または /dir/*/*/file。

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：/dir/**/file*/ または /dir/file**/。

アスタリスク記号を 2 文字連続させた「`**`」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「`/dir/**/**/file`」は不適切なマスク表現となります。

ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。

コンテナスキャン

Kaspersky Endpoint Security は、コンテナとイメージに対して、マルウェアのスキャンをリアルタイムまたはオンデマンドで実行できます。

> 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。

> このコンポーネントは、Elbrus CPU を搭載したデバイスでは使用できません。

コンテナの監視

*コンテナ監視*コンポーネントは、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は既定で有効になっています。

> 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。

推奨されるコンテナ監視の設定シナリオには、次の手順が含まれます：

1. **アプリケーションとコンテナ管理ツールの連携の設定**

   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。

2. **保護範囲の作成**

   コンテナと名前空間をスキャンする対象のデバイスを決定します。

3. **コンテナ監視設定で、［コンテナをスキップ］処理を選択します。**

   コンテナ内で感染したオブジェクトが検知された場合、Kaspersky Endpoint Security は、コンテナを直ちに停止する、何も実行しない、またはオブジェクトの駆除や脅威の排除が不可能であることが判明した場合にコンテナを停止することができます。コンポーネントをテストするには、**コンテナをスキップ**処理を選択します。感染したオブジェクトが検知されても、アプリケーションはコンテナに対して処理を実行しませんが、検知された脅威に関する情報をログに記録します。

4. **コンテナ監視の統計情報の収集**

   レポートを使用して、コンテナ監視の統計情報を取得できます。

5. **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。**

   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。

コンテナのオンデマンドスキャン

本製品では、必要に応じてコンテナやイメージをスキャンし、ウイルスやその他のマルウェアを検知できます。これは、事前定義済みの コンテナスキャン（*Container_Scan*）タスクを使用して実行します。コマンドライン、Web コンソール、または管理コンソールで、事前定義済みタスクを設定したり、コンテナをスキャンするためのユーザータスクを作成したりできます。

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。

推奨されるコンテナスキャンの設定シナリオには、次の手順が含まれます：

1. **アプリケーションとコンテナ管理ツールの連携の設定**

   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。

2. **スキャン範囲の設定**

   既定では、本製品は保護対象デバイス上のすべてのコンテナをスキャンします。個別のコンテナのみをスキャンする場合は、コンテナの名前または名前マスクを指定できます。

3. **コンテナスキャン設定で、［コンテナをスキップ］処理と［イメージをスキップ］処理を選択します。**

   コンテナ内で感染したオブジェクトが検知された場合、Kaspersky Endpoint Security は、コンテナを直ちに停止する、何も実行しない、またはオブジェクトの駆除や脅威の排除が不可能であることが判明した場合にコンテナを停止することができます。コンテナイメージ内で感染したオブジェクトが検知された場合、Kaspersky Endpoint Security は、コンテナイメージを削除するか、コンテナイメージに対して処理を行わないことができます。タスクをテストするには、**コンテナをスキップ**処理と**イメージをスキップ**処理を選択します。感染したオブジェクトが検知された場合、本製品はコンテナとイメージに対して処理を行いませんが、検知された脅威に関する情報をログに記録します。

4. **コンテナスキャンの統計情報の収集**

   コンテナスキャンの統計は、レポートを使用して取得できます。

5. **アプリケーションのパフォーマンスを最適化する**

   収集した情報を分析した後、アプリケーションのパフォーマンスを最適化します：

   - グローバルの除外リストを追加する
   - スキャンの除外リストを追加します
   - コンテナスキャンを最適化します

6. **感染したオブジェクトの検知時にコンテナとそのイメージに対して実行する処理の選択**

   感染したオブジェクトを検知した際に、本製品がコンテナとそのイメージに対して実行する処理を選択します。

コンテナのカスタムスキャン

カスタムコンテナスキャンタスクでは、指定したコンテナとイメージを次のコマンドを使用してスキャンする際に使用する設定を、構成して保存できます：

```
kesl-control --scan-container
```

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。

このコマンドは、コンテナとイメージをスキャンするための一時タスクを作成して実行します。このタスクは完了後に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。

特別な考慮事項と制限事項

- 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。
- コンテナ監視の処理は、本製品のライセンスにこの機能が含まれている場合にのみ選択できます。

コンテナ管理ツールとの統合を設定する方法

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。これらのコンテナ管理ツールとの統合を設定できます。

Web コンソールでコンテナ管理ツールとの統合を設定する方法

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. ［**全般設定** → **コンテナスキャン設定**］に移動します。
5. コンテナ監視コンポーネントのトグルスイッチが **名前空間およびコンテナの監視が有効です** の位置にあることを確認します。
6. ［**コンテナスキャン設定**］ブロックの［**設定する**］をクリックします。

7. **スキャン設定** ウィンドウが開きます。このウィンドウで、保護対象デバイスのオペレーティングシステムにインストールされ、使用されているコンテナ管理ツールの横にあるチェックボックスをオンにし、必要に応じて設定を管理します：

   - **Docker を使用する**チェックボックスをオンにすると、Docker コンテナ管理システムが有効になります。既定では、このチェックボックスはオンです。

     - **Docker ソケットのパス**は、Docker ソケットのパスまたは URI（Uniform Resource Identifier）を入力するフィールドです。既定値：/var/run/docker.sock

   - **CRI-O を使用する**チェックボックスをオンにすると、CRI-O 環境が有効になります。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**は、CRI-O 設定情報ファイルのパスを入力するフィールドです。既定値：/etc/crio/crio.conf

   - **Podman を使用する**チェックボックスをオンにすると、Podman ユーティリティが有効になります。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**は、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です。既定値：/usr/bin/podman

     - **ルートディレクトリ**は、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です。

   - **runc を使用する**チェックボックスをオンにすると、runc ユーティリティが有効になります。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**は、runc 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です。既定値：/usr/bin/runc

     - **ルートディレクトリ**は、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です。既定値：/run/runc

8. 変更内容を保存します。

コマンドラインでコンテナ管理ツールとの統合を設定する方法

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監視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。

コマンドラインオプションを使用して名前空間とコンテナの監視を有効にする

```
kesl-control --set-app-settings NamespaceMonitoring=Yes
```

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、コンテナスキャン設定が適用されます。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、すべてのコンテナスキャン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、`<setting name>=<setting value>` の形式で個々の設定を管理できます。コンテナスキャン設定を出力するコマンドを使用して、設定の現在の値を取得できます。

コンテナスキャン設定の現在の値をコンソールに出力する

```
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。

コンテナスキャン設定の現在の値をファイルに出力する

```
kesl-control --get-container-settings --file <path to configuration file> [--json]
```

説明：

- `--file <path to configuration file>` は、コンテナスキャン設定を保存す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設定の値を変更するには、次の手順を実行します：

1. 上で説明したように、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 <path to configuration file> [--json]
   ```

   説明：

   - `--file <path to configuration file>` は、コンテナスキャン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。

ファイルで指定されたコンテナスキャン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。

コマンドラインオプションを使用してコンテナスキャン設定の値を変更する

```
kesl-control --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

ここで、`<setting name>=<setting value>` は、コンテナスキャン設定の名前と値です。

指定されたコンテナスキャン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範囲の作成方法

スキャン範囲

*スキャン範囲*とは、Kaspersky Endpoint Security がコンテナスキャンタスクの実行中にスキャンするコンテナ名のリストです。

既定では、コンテナスキャンタスクは保護対象デバイス上のすべてのコンテナをスキャンします。個別のコンテナのみをスキャンする場合は、コンテナの名前または名前マスクを指定できます。

Web コンソールでのスキャン範囲の作成

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。

   タスクのリストが表示されます。

2. タスクの一覧で、「Kaspersky Endpoint Security コンテナスキャン」タスクを選択し、タスク名をクリックします。

   タスクのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. **スキャンの詳細設定 → コンテナスキャン設定** の **名前のマスク** フィールドに、スキャンするコンテナの名前または名前マスクを入力します。既定では、すべてのコンテナがスキャンされます。

5. **スキャンの詳細設定 → イメージのスキャン設定** の **名前のマスク** フィールドに、スキャンするコンテナイメージの名前または名前マスクを入力します。既定では、すべてのイメージがスキャンされます。

6. 変更内容を保存します。

コマンドラインでのスキャン範囲の作成

1. 次のコマンドを使用してスキャン範囲を設定します：

   ```
   kesl-control --set-settings <task ID|name> ScanContainers=Yes ContainerNameMask=<container name or mask>
   ScanImages=Yes ImageNameMask=<image name or mask>
   ```

   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。
   - `<container name or mask>` は、スキャンするコンテナの名前または名前マスクです。マスクはコマンドシェル形式で指定されます。`?` および `*` 記号を使用できます。既定では、すべてのコンテナがスキャンされます。
   - `<image name or mask>` は、スキャンするイメージの名前または名前マスクです。マスクはコマンドシェル形式で指定されます。`?` および `*` 記号を使用できます。既定では、すべてのイメージがスキャンされます。

2. 設定情報ファイルを使用してスキャン範囲を設定することもできます：

   a. 次の コマンドを実行して、タスク設定 を 設定情報ファイルに 出力します：

```
kesl-control --get-settings <task ID|name> [--json]
```

   b. 設定情報ファイルを編集のために開きます。

   c. ファイルに次の設定を追加します：

   - `ScanContainers=Yes` を指定すると、指定したコンテナのスキャンが有効になります。
   - `ContainerNameMask=<container name or mask>` は、スキャンするコンテナの名前または名前マスクです。マスクはコマンドシェル形式で指定されます。`?` および `*` 記号を使用できます。既定では、すべてのコンテナがスキャンされます。
   - `ScanImages=Yes` を指定すると、指定したイメージのスキャンが有効になります。
   - `ImageNameMask=<image name or mask>` は、スキャンするイメージの名前または名前マスクです。マスクはコマンドシェル形式で指定されます。`?` および `*` 記号を使用できます。既定では、すべてのイメージがスキャンされます。

my_container という名前のコンテナに対して実行されたコンテナスキャンの例

```
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例

```
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、任意の文字列で終わるすべてのコンテナに対して実行されたコンテナスキャンの例

```
ContainerNameMask=my_?????_container*
```

「my_image」という名前で、「latest」タグを持つイメージに対して実行されたイメージスキャンの例

```
ImageNameMask=my_image:latest
```

名前が my_image_ で始まり、任意のタグを持つすべてのイメージに対して実行されたイメージスキャンの例

```
ImageNameMask=my_image*
```

   d. 変更内容を設定ファイルに保存します。

   e. 次のコマンドを使用して、設定情報ファイルからタスクに設定をインポートします：

```
kesl- <task ID|name> --file <path> [--json]
```

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。
- `--file <path>` は、タスク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、アプリケーションは INI ファイルからインポートを試みます。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本製品にインポートされます。

信頼するオブジェクト

*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。

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、信頼できる特定のディレクトリをスキャン範囲から除外することもできます。

次の方法を使用して、スキャンからオブジェクトを除外できます：

- **マスクによる除外**。マスクを指定してファイル名を入力します。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。

  マスクを使用する

  - 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはディレクトリのパスにおけるファイル名またはディレクトリ名の区切り文字）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「`/dir/*/*.txt`」には、dir ディレクトリ内のディレクトリにある拡張子が TXT のすべてのファイルへのパスが含まれますが、サブディレクトリにあるファイルへのパスは含まれません。
  - 連続する 2 つの「`*`」文字。ファイル名またはディレクトリ名内の、「`\`」および「`/`」（ファイルまたはディレクトリのパスにおけるファイル名またはディレクトリ名の区切り文字）を含む任意の文字列（空の文字列を含む）に置き換えられます。たとえば、マスク「`/dir/**/*.txt`」には、dir ディレクトリ内にネストされたディレクトリにある拡張子が TXT のすべてのファイルへのパスが含まれますが、dir ディレクトリ自体にあるファイルへのパスは含まれません。
  - 「`?`」（クエスチョンマーク）文字。「`\`」および「`/`」（ファイルまたはディレクトリのパスにおけるファイル名またはディレクトリ名の区切り文字）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「`/dir/???.txt`」には、dir ディレクトリにある、拡張子が TXT でファイル名が 3 文字のすべてのファイルへのパスが含まれます。

- **脅威名による除外** カスペルスキー百科事典の分類に従って、オブジェクトタイプの名前を入力します（例：`Email-Worm`、`Rootkit`、`RemoteAdmin`）。任意の 1 文字を置き換える「`?`」と複数の文字を置き換える「`*`」を使用してマスクを使用することができます。たとえば、マスク「`Client*`」を使用すると、「`Client-IRC`」、「`Client-P2P`」および「`Client-SMTP`」がスキャンから除外されます。

Kaspersky Endpoint Security では、特定の形式のファイルをスキャン対象から除外することもできます：アーカイブ、メールデータベース、テキストファイル、データベースログファイル。

Web コンソールでスキャン除外を追加する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。

   タスクのリストが表示されます。

2. タスクの一覧で、「Kaspersky Endpoint Security コンテナスキャン」タスクを選択し、タスク名をクリックします。

   タスクのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**除外範囲**］に移動します。

5. 必要に応じて、マスクによる除外を追加します：

   a. ［**マスクによる除外**］ブロックの［**追加**］をクリックします。

   b. ウィンドウが開きます。このウィンドウで、Kaspersky Endpoint Security のスキャン対象から除外するファイル名のテンプレートを指定します。

   c. ［**追加**］をクリックします。

      除外がリストに追加されます。

6. 必要に応じて、脅威名による除外を追加します：

   a. ［**脅威の名前別除外**］ブロックの［**追加**］をクリックします。

   b. ウィンドウが開きます。このウィンドウで、脅威名のテンプレートを指定します。指定された脅威はブロックされません。

   たとえば、ネットワークをスキャンするツールを使用する場合、そのツールに対応する脅威の完全な名前を、スキャン対象から除外する脅威のリストに追加します。

   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。

7. 必要に応じて、各リストの除外をインポートまたはエクスポートできます：

   - 除外リストをエクスポートするには、［**エクスポート**］をクリックします。

     Kaspersky Endpoint Security は、export.json ファイルを標準のダウンロードフォルダーに保存します。

   - 除外リストをインポートするには：

     a. ［**インポート**］をクリックします。

     b. 除外範囲のインポート元となる JSON ファイルを選択します。

     c. ファイルを開きます。

     d. インポート方法を選択します：既存のリストに除外を追加するか、除外リストを置き換えるか。

e. 変更内容を保存します。

JSON ファイルのルールがリストに表示されます。

8. 変更内容を保存します。

コマンドラインでスキャン除外を追加する方法

1. 次のコマンドを使用して除外範囲を追加します：

```
kesl-control --set-settings <タスク ID|名前> --add-exclusion <パス>
```

説明：

- `<task ID|name>` は、タスク作成時に割り当てられた ID、またはコマンドライン上のタスク名です。
- `--add-exclusion <path>` 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。

2. 設定情報ファイルを使用して除外範囲を追加することもできます：

a. 次の コマンドを実行して、 タスク設定を 設定情報ファイルに 出力します：

```
kesl-control --get-settings <task ID|name> [--json]
```

b. 設定情報ファイルを編集のために開きます。

c. 次の設定を使用して、ファイルに `[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=*
```

d. `[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。

e. 変更内容を設定ファイルに保存します。

f. 次のコマンドを使用して、設定情報ファイルからタスクに設定をインポートします：

```
kesl-control --set-settings <task ID|name> --file <path>
```

3. 必要に応じて、次のコマンドを実行して除外範囲を削除できます：

```
kesl-control --set-settings <task ID|name> --del-exclusion <path>
```

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。
- `--del-exclusion <path>` 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。

コンテナスキャンを最適化する方法

ファイルスキャンを設定して、タスクのパフォーマンスを最適化します。これにより、保護対象デバイスの CPU 使用率を低減できます。アーカイブのスキャンを制限し、スキャン可能なオブジェクトの最大サイズとオブジェクトの最大スキャン時間を設定できます。Kaspersky Endpoint Security では、アーカイブ、メールデータベース、テキストファイル、プレーンテキスト形式のメールメッセージなど、特定の形式のファイルをスキャンから除外することもできます。

Web コンソールでファイルスキャンを設定する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。

   タスクのリストが表示されます。

2. タスクの一覧で、「Kaspersky Endpoint Security コンテナスキャン」タスクを選択し、タスク名をクリックします。

   タスクのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. **スキャン設定** で、ファイルスキャンを設定します：

   - **アーカイブをスキャン**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、スキャンは無効になっています。
   - **SFX アーカイブをスキャン**実行可能な解凍モジュールを含む自己解凍型アーカイブのスキャン。既定では、スキャンは無効になっています。

- **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。既定では、スキャンは無効になっています。

- **メール形式のファイルをスキャン**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。既定では、スキャンは無効になっています。

- **ファイルの最大スキャン時間（秒）**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。既定では、本製品は1分以内にオブジェクトのスキャンを試行します。

- **ファイルのサイズが次を超えたらスキップする（MB）**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。

- **ファイルのサイズが次を超えたらスキップする（MB）**スキャンが既に実行中の場合はスキャンタスクの開始を遅延します。現在のスキャンが続行される場合は Kaspersky Endpoint Security は新しいスキャンタスクをエンキューします。これは、コンピューターの負荷の最適化に役立ちます。たとえば、本製品がスケジュールに従って完全スキャンタスクを開始していたとします。ユーザーが製品インターフェイスから簡易スキャンを開始しようとすると、Kaspersky Endpoint Security はこの簡易キャンタスクをエンキューし、完全スキャンタスクの完了後にこのタスクが自動的に開始されます。

5. 変更内容を保存します。

コマンドラインでファイルスキャンを設定する方法

1. 次のコマンドを実行します：

```
kesl --set-settings <task ID|name> ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<object size (MB)>
TimeLimit=<scan time (sec)> QueueScanTasks=<Yes|No>
```

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。

- `<object size (MB)>` は、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）です。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。既定値：`0`。

- `<scan time (sec)>` は、オブジェクトの最大スキャン時間（秒単位）です。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。既定値：`0`。

2. 設定情報ファイルを使用して設定することもできます：

   a. 次の コマンドを実行して、タスク設定 を 設定情報ファイルに 出力します：

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. 設定情報ファイルを編集のために開きます。

   c. このファイルに、コンテナおよびイメージ内のオブジェクトに適用される次の コンテナスキャンタスク設定を追加します：`ScanArchived`、`ScanSfxArchived`、`ScanMailBases`、`ScanPlainMail`、`SizeLimit`、`TimeLimit`、`QueueScanTasks`。

   d. 変更内容を設定ファイルに保存します。

e. 次のコマンドを使用して、設定情報ファイルからタスクに設定をインポートします：

```
kesl-control --set-settings <task ID|name> --file <path> [--json]
```

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。
- `--file <path>` は、タスク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。

ファイルで定義されたタスク設定のすべての値が本製品にインポートされます。

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する方法

コンテナ内で感染したオブジェクトが検知された場合、Kaspersky Endpoint Security は、コンテナを直ちに停止する、何も実行しない、またはオブジェクトの駆除や脅威の排除が不可能であることが判明した場合にコンテナを停止することができます。*コンテナ監視*コンポーネントによるリアルタイムスキャンの一環として、またはオンデマンドの*コンテナスキャン*タスクの一環として感染したオブジェクトが検知された場合に、Kaspersky Endpoint Security がコンテナに対して実行する処理を選択できます。

コンテナイメージ内で感染したオブジェクトが検知された場合、Kaspersky Endpoint Security はイメージを削除するか、イメージに対して何も実行しません。オンデマンドの*コンテナスキャン*タスクの一環として感染したオブジェクトが検知された場合に、Kaspersky Endpoint Security がコンテナイメージに対して実行する処理を選択できます。

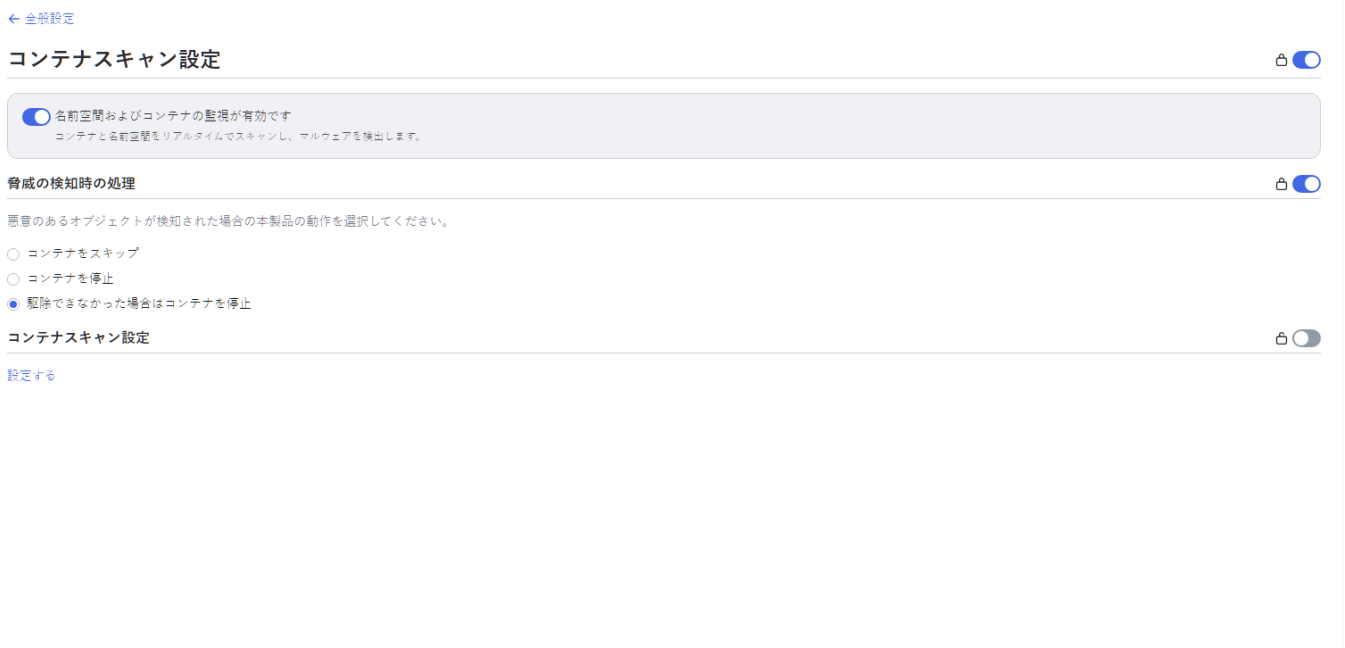
Web コンソールで脅威の検知時のコンテナ監視の処理を選択する方法

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. ［**全般設定**］→［**コンテナスキャン設定**］に移動します。
5. コンテナ監視コンポーネントのトグルスイッチが **名前空間およびコンテナの監視が有効です** の位置にあることを確認します。
6. **脅威の検知時の処理** で、コンテナ内で感染したオブジェクトが検知された場合にアプリケーションが実行する処理を選択します：
   - **コンテナをスキップ**コンテナ内で感染したオブジェクトが検知された場合、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**コンテナ内で感染したオブジェクトが検知された場合、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**（既定）。コンテナ内で感染したオブジェクトが検知された場合、アプリケーションは感染したオブジェクトの駆除を試行します。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。

> CRI-O 環境の仕組みにより、感染したオブジェクトは CRI-O 環境のコンテナ内で駆除または削除されません。**コンテナを停止**操作を選択することをお勧めします。

7. 変更内容を保存します。



コンテナスキャン設定

コマンドラインで脅威の検知時のコンテナ監視の処理を選択する方法

1. 次のコマンドを実行します：

```
kesl-control --set-container-settings OnAccessContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
```

> 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のみ設定できます。

2. コンテナスキャン設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings container-settings
```

Web コンソールで脅威の検知時のコンテナスキャン処理を選択する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。

   タスクのリストが表示されます。

2. タスクの一覧で、「Kaspersky Endpoint Security コンテナスキャン」タスクを選択し、タスク名をクリックします。

   タスクのプロパティウィンドウが表示されます。

3. ［**アプリケーション設定**］タブを選択します。

4. **スキャンの詳細設定 → コンテナスキャン設定 → 脅威の検知時の処理** で、コンテナ内で感染したオブジェクトが検知された場合にアプリケーションが実行する処理を選択します：

   - **コンテナをスキップ**コンテナ内で感染したオブジェクトが検知された場合、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**コンテナ内で感染したオブジェクトが検知された場合、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**（既定）。コンテナ内で感染したオブジェクトが検知された場合、アプリケーションは感染したオブジェクトの駆除を試行します。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。

     > CRI-O 環境の仕組みにより、感染したオブジェクトは CRI-O 環境のコンテナ内で駆除または削除されません。**コンテナを停止**操作を選択することをお勧めします。

5. **スキャンの詳細設定 → イメージのスキャン設定 → 脅威の検知時の処理** で、コンテナ内で感染したオブジェクトが検知された場合にアプリケーションが実行する処理を選択します：

   - **イメージをスキップ**（既定）。イメージ内で感染したオブジェクトが検知された場合、アプリケーションはイメージに対して操作を実行しません。

   - **イメージを削除**（推奨されません）。イメージ内で感染したオブジェクトが検知された場合、アプリケーションはイメージを削除します。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。

6. 変更内容を保存します。

コマンドラインで脅威の検知時のコンテナスキャン処理を選択する方法

1. 次のコマンドを実行します：

   ```
   kesl-control --set-settings <task ID|name> ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
   ImageAction=<Skip|Delete>
   ```

   ここで、`<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。

   > 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。

2. 設定情報ファイルを使用して処理を設定することもできます：

   a. 次の コマンドを実行して、タスク設定 を 設定情報ファイルに 出力します：

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. 設定情報ファイルを編集のために開きます。

c. ファイルにコンテナスキャンタスクの次の設定を追加します：

- `ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>` – 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。既定値：`StopContainerIfFailed`。
- `ImageAction=<Skip|Delete>` – 感染したオブジェクトの検知時に、コンテナイメージに対して実行する処理。既定値：`Skip`。

d. 変更内容を設定ファイルに保存します。

e. 次のコマンドを使用して、設定情報ファイルからタスクに設定をインポートします：

```
kesl-control --set-settings <task ID|name> --file <path> [--json]
```

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。
- `--file <path>` は、タスク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。

ファイルで定義されたタスク設定のすべての値が本製品にインポートされます。

コンテナとイメージのオブジェクトスキャンを実行する方法

カスタムコンテナスキャンタスクをコマンドラインで開始するには、次のコマンドを実行します：

```
kesl-control --scan-container <id|name[:tag]>
```

ここで、`<id|name[:tag]>` 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。

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。

`my_container` という名前のコンテナに対して実行されたコンテナスキャンの例

```
kesl-control --scan-container my_container
```

`my_image` という名前のイメージ（すべてのタグ）に対して実行されたイメージスキャンの例

```
kesl-control --scan-container my_image*
```

役立つ記事

マスクを指定する方法

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。

リムーバブルドライブのスキャン

Kaspersky Endpoint Security は、ファイルがリムーバブルドライブ上にある場合でも、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。本製品は、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上のファイルをスキャンします。既定では、リムーバブルドライブスキャンは無効です。

リムーバブルドライブスキャンの仕組み

リムーバブルドライブが接続されると、本製品は既定の設定で次のスキャンタスクを自動的に作成して開始します：簡易スキャンの場合は *簡易スキャン*、詳細スキャンの場合は *マルウェアのスキャン*。これらのタスクは停止できません。リムーバブルドライブで脅威が検知されると、Kaspersky Endpoint Security は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、本製品は感染したオブジェクトを削除します。スキャンが完了すると、本製品はこれらのタスクを自動的に削除します。

スキャン種別

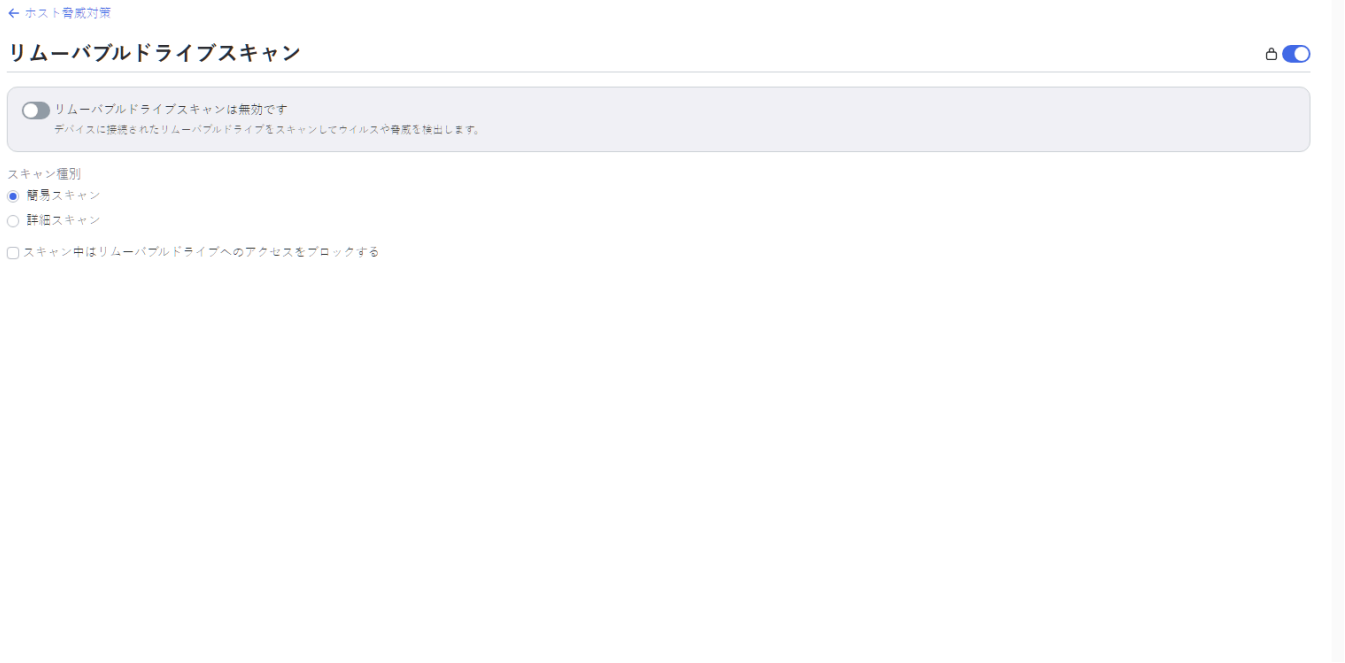
- **簡易スキャン**Kaspersky Endpoint Security は、指定された拡張子のファイルのみをスキャンし、複合オブジェクトは展開しません。本製品は、*簡易スキャン* タスクの既定の設定で簡易スキャンを実行します。
- **詳細スキャン**Kaspersky Endpoint Security は、リムーバブルドライブ上のすべてのファイルをスキャンします。本製品は、*マルウェアのスキャン* タスクの既定の設定で詳細スキャンを実行します。

Web コンソールでリムーバブルドライブスキャンの種別を選択する方法

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. ［**ホスト脅威対策**］→［**リムーバブルドライブスキャン**］に移動します。
5. コンポーネントのトグルスイッチが **リムーバブルドライブスキャンは有効です** の位置にあることを確認します。
6. **スキャン種別** で、リムーバブルドライブスキャンの種別として **簡易スキャン** または **詳細スキャン** を選択します。
7. 必要に応じて、［**スキャン中のファイルへのアクセスのブロック**］をオンにします。
   ファイルへのアクセスをブロックすると、スキャンの実行中にユーザーがマルウェアを実行するのを防ぐことができます。

   ブートセクターのスキャン中、本製品はファイルをブロックしません。

8. 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。



リムーバブルドライブのスキャン

コマンドラインでリムーバブルドライブスキャンの種別を選択する方法

1. リムーバブルドライブの接続時に実行するスキャンの種別を選択します：

```
kesl-control --set-settings 16 ScanRemovableDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

2. CD/DVD ドライブまたは Blu-ray ディスクの挿入時に実行するスキャンの種別を選択します：

```
kesl-control --set-settings 16 ScanOpticalDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

3. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 16
```

記号

コマンドオプション

設定	説明
ScanRemovableDrives	リムーバブルドライブの接続時のスキャンの種別： • DetailedScan 詳細スキャン。 • QuickScan 簡易スキャン • NoScan（既定）。本製品はスキャンを実行しません。
ScanOpticalDrives	CD/DVD ドライブまたは Blu-ray ディスクの挿入時に実行するスキャンの種別： • DetailedScan 詳細スキャン。 • QuickScan 簡易スキャン • NoScan（既定）。本製品はスキャンを実行しません。
BlockDuringScan	スキャン中は、接続されたディスク上のファイルへのアクセスをブロックします。既定では、本製品はファイルへのアクセスをブロックしません。 ファイルへのアクセスをブロックすると、スキャンの実行中にユーザーがマルウェアを実行するのを防ぐことができます。 ブートセクターのスキャン中、本製品はファイルをブロックしません。

ふるまい検知

ふるまい検知コンポーネントを使用すると、コンピューターまたはユーザーデータを侵害する可能性があるアプリケーションの活動（ファイルを開く、接続を確立するなど）を監視できます。このコンポーネントはアプリケーションのふるまいを監視し、危険なパターンを検出します。アプリケーションの活動がこのようなパターンのいずれかと一致した場合、Kaspersky Endpoint Security は選択した対応処理を実行します。Kaspersky Endpoint Security のこの機能により、コンピューターをプロアクティブに保護できます。

行動検知コンポーネントの最適なパフォーマンスを得るためには、ウェブ脅威対策コンポーネントを有効にすることをお勧めします。

ふるまい検知の仕組み

1. **アプリケーションはオペレーティングシステム内のイベントを監視します**

   アプリケーションは、プロセスの作成と終了、開かれたファイル、確立された接続などのイベントで構成されるテレメトリのストリームを受信します。また、アプリケーションはイベントに関連するメタデータ（プロセス名、PID、IPアドレスなど）を追加します。

2 アプリケーションはテレメトリのストリームを危険なふるまいのパターンと比較します

サードパーティ製アプリケーションの動作が危険なふるまいのパターンと一致した場合、Kaspersky Endpoint Securityは脅威対応処理を実行します（たとえば、サードパーティ製アプリケーションを停止できます）。

3 本製品はテレメトリを KSN に送信します

本製品はイベントをフィルタリングし、さらなる分析のために KSN に送信します。

ふるまい検知の設定

1 ふるまい検知設定で、［通知］処理を選択します

既定では、ふるまい検知コンポーネントは有効になっています。ふるまい検知設定では、脅威の検知時の処理として**通知する**を選択し、インストールされているアプリケーションが正常に動作するか確認することを推奨します。Kaspersky Endpoint Security は、アプリケーションのすべての動作を許可し、コンポーネントの動作ログを記録します。

Web コンソールでマルウェア活動の検知時に実行する処理を選択する方法

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. ［**ホスト脅威対策**］→［**ふるまい分析**］→［**ふるまい検知**］に移動します。
5. ［**脅威の検知時の処理**］ブロックで関連する操作を選択します。
   - **通知する**悪意のある活動が検知された場合、Kaspersky Endpoint Security はこのアプリケーションを停止せず、イベントログに悪意のある活動の検知に関するイベントのみを記録します。
   - **ブロックする**悪意のある活動が検知された場合、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のプロセスを停止し、検知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。

6. 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。

ふるまい検知

コマンドラインでマルウェア活動の検知時に実行する処理を選択する方法

1. 次のコマンドを実行します：

```
kesl-control --set-settings 20 TaskMode=<Block|Notify>
```

2. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 20
```

記号

コマンドオプション

設定	説明
TaskMode	マルウェア活動の検知時に実行する処理： • Block（既定）。悪意のある活動が検知された場合、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のプロセスを停止し、検知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。 • Notify 悪意のある活動が検知された場合、Kaspersky Endpoint Security はこのアプリケーションを停止せず、イベントログに悪意のある活動の検知に関するイベントのみを記録します。

2 ふるまい検知の統計情報を収集する

ふるまい検知の統計情報は、レポートを使用して取得できます。

3 アプリケーションのパフォーマンスを最適化する

収集した情報を分析した後、アプリケーションのパフォーマンスを最適化し、除外を追加します。

4 ふるまい検知設定で、［ブロック］処理を選択します

アプリケーションの悪意のある活動をブロックする機能をオンにします。その後、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のプロセスを停止します。

特別な考慮事項と制限事項

- 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している場合に、ふるまい検知コンポーネントを正しく動作させるには、設定情報ファイルで auditd が設定ブロックなしモード `enabled 1` に設定されていることを確認してください。

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。

脆弱性攻撃ブロックコンポーネントが機能するには、次のコンポーネントを有効にする必要があります：

- ふるまい検知
- 更新可能なカーネルモジュール

> このコンポーネントは、Elbrus CPU を搭載したデバイスでは使用できません。

脆弱性攻撃ブロックの仕組み

1. **アプリケーションはオペレーティングシステム内のイベントを監視します**

   アプリケーションは、プロセスの作成と終了、開かれたファイル、確立された接続などのイベントで構成されるテレメトリのストリームを受信します。また、アプリケーションはイベントに関連するメタデータ（プロセス名、PID、IPアドレスなど）を追加します。

2. **アプリケーションはテレメトリのストリームを危険なふるまいのパターンと比較します**

   サードパーティ製アプリケーションの動作が危険なふるまいのパターンと一致した場合、Kaspersky Endpoint Securityは脅威対応処理を実行します（たとえば、サードパーティ製アプリケーションを停止できます）。

脆弱性攻撃ブロックの設定

1. **脆弱性攻撃ブロック設定で、［通知］を選択します**

   既定では、脆弱性攻撃ブロックコンポーネントは無効になっています。脆弱性攻撃ブロック設定で、脅威の検知時の処理として**通知**を選択し、インストールされているアプリケーションが正常に動作するかどうかを確認します。Kaspersky Endpoint Security は、アプリケーションのすべての動作を許可し、検知された脅威に関する情報をログに記録します。

Web コンソールで脆弱性攻撃の検知時の処理を選択する方法

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. ［**ホスト脅威対策**］→［**ふるまい分析**］→［**脆弱性攻撃ブロック**］に移動します。
5. ［**脆弱性攻撃ブロック**］トグルスイッチを使用して機能を有効または無効にします。
6. ［**脅威の検知時の処理**］ブロックで関連する操作を選択します。
   - **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。
   - **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。
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。

コマンドラインで脅威の検知時の処理を選択する方法

1. 脆弱性攻撃ブロックを有効にするには、次のコマンドを実行します：

```
kesl-control --set-settings 20 UseAEP=Yes
```

2. 脆弱性攻撃の検知時の処理を選択します：

```
kesl-control --set-settings 20 AEPMode=<Block|Notify>
```

3. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 20
```

記号

コマンドオプション

設定	説明
UseAEP	コンポーネントを有効にする： • 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	脆弱性攻撃の検知時の処理： • Block（既定）。Kaspersky Endpoint Security は、この脆弱性攻撃による操作をブロックし、この脆弱性攻撃に関する情報をログに記録します。 • Notify Kaspersky Endpoint Security は脆弱性攻撃を検知すると、その脆弱性攻撃に関する情報をログに記録し、アクティブな脅威のリストにこの脆弱性攻撃に関する情報を追加します。

2. **脆弱性攻撃ブロックの統計情報を収集する**

   レポートを使用して脆弱性攻撃ブロックの統計情報を取得できます。

3. **アプリケーションのパフォーマンスを最適化する**

   収集した情報を分析した後、アプリケーションのパフォーマンスを最適化します：

   - グローバルの除外リストを追加する
   - 除外を追加する

4. **脆弱性攻撃ブロック設定で、［ブロック］を選択します**

   オペレーティングシステムでのアプリケーションの悪意のある動作のブロックを有効にします。

アンチクリプター

アンチクリプターコンポーネントは、コンピューターの共有ネットワークディレクトリにおけるリモートデバイスの動作を分析することで、リモートからの暗号化に対する保護を提供します。アンチクリプターは、NFS および SMB プロトコルを介して保護対象のコンピューターに送信されるファイルを分析します。

動作が外部からの暗号化に典型的な動作ストリームのシグネチャと一致する場合、Kaspersky Endpoint Security はこの動作をブロックするか、そのことを通知します。

アンチクリプターの仕組み

1. **アプリケーションは NFS および SMB リクエストをインターセプトします**

   アプリケーションは、NFS および SMB プロトコルを介して送信されるファイルの作成と変更に関するテレメトリのストリームを受信します。

2. **アプリケーションは、テレメトリのストリームをシグネチャデータベースと比較します。**

   サードパーティ製アプリケーションの動作がランサムウェアの動作と一致する場合、Kaspersky Endpoint Security は脅威の検知時の処理で選択した処理を実行します（たとえば、リモートコンピューターへの接続をブロックします）。

アンチクリプターの設定

1. **保護範囲の設定**

   既定では、アプリケーションはすべての共有ディレクトリをスキャンします。個別のディレクトリ（たとえば、外部ソースからファイルが自動的にダウンロードされるディレクトリ）のみをスキャンする必要がある場合は、そのディレクトリのみを保護範囲として指定できます。それ以外の場合は、既定の保護範囲のままにし、除外を使用して範囲を細かく調整することを推奨します。

2. **アンチクリプターの設定で、処理として「通知」を選択します。**

   既定では、アンチクリプターは無効になっています。アンチクリプターを有効にし、脅威の検知時の処理として **通知** を選択して、すべての企業リソースへのアクセスを確認することを推奨します。Kaspersky Endpoint Security は、共有ディレクトリ内のすべてのリソースへのアクセスを許可し、検知された脅威に関する情報をログに記録します。

3. **アンチクリプターの統計情報を収集する**

   アンチクリプターの統計情報は、レポートを使用して取得できます。

4. **アプリケーションのパフォーマンスを最適化する**

   収集した情報を分析した後、アプリケーションのパフォーマンスを最適化します：

   - グローバルの除外リストを追加する。
   - 除外を追加する。

5. **アンチクリプターの設定で、処理として「接続をブロック」を選択します。**

   リモートの攻撃元デバイスからのネットワークトラフィックのブロックを有効にします。

特別な考慮事項と制限事項

- 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 プロトコルで正常に動作します。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にサーバーを設定することを推奨します。
- アンチクリプターコンポーネントが正常に動作するには、オペレーティングシステムに少なくとも 1 つのサービス（Samba または NFS）がインストールされている必要があります。NFS サービスの場合、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。
- Kaspersky Endpoint Security では、リモート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。

悪意のある暗号化の検知時に実行する処理の選択方法

悪意のある暗号化が検知された場合、本製品はリモートの攻撃元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か、悪意のある暗号化の検知を通知するだけにすることができます。

ネットワークトラフィックをブロックするため、Kaspersky Endpoint Security は動的 Firewall ルールを作成します。Firewall は、攻撃元デバイスのネットワークトラフィックを一時的にブロックします。本製品は、攻撃元デバイスをブロックされたデバイスのリストにも追加します。ブロックされたデバイスは、共有ネットワークディレクトリへのアクセスを拒否されます。

管理者に悪意のある暗号化の検知を通知するため、本製品は*暗号化が検知されました*イベントを生成します。

既定では、本製品は攻撃元デバイスのネットワークトラフィックを60 分間ブロックします。ブロック時間が終了すると、本製品は侵害されたデバイスをブロックされたデバイスのリストから削除し、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復元されます。

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ユーザーのコンピュータでローカルに手動で解除できます。Kaspersky Security Center には、*暗号化が検知されました*イベント以外に、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。

Web コンソールで悪意のある暗号化の検知時に実行する処理を設定する方法

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. ［**ホスト脅威対策**］→［**ふるまい分析**］→［**アンチクリプター**］に移動します。
5. コンポーネントのトグルスイッチが **アンチクリプターは有効です** の位置にあることを確認します。
6. **脅威の検知時の処理**で、脅威が検知されたときにアプリケーションが実行する処理（**通知する**または**接続をブロックする時間（分）**）を選択します。
7. **接続をブロックする時間（分）**が選択されている場合は、攻撃元デバイスのブロック期間を分単位で設定します。既定では、デバイスは60 分間ブロックされます。
8. 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。

アンチクリプター

コマンドラインで悪意のある暗号化の検知時に実行する処理を設定する方法

1. 次のコマンドを実行します：

```
kesl-control --set-settings 13 ActionOnDetect=<Block|Notify>
```

2. `Block`処理のブロック期間を選択します。

```
kesl-control --set-settings 13 BlockTime=<Blocking period>
```

3. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 13
```

記号

コマンドオプション

設定	説明
ActionOnDetect	外部からの暗号化の検知時の処理： • Block（既定）は、攻撃元デバイスのネットワークトラフィックをブロックし、*暗号化が検知されました*イベントを作成します。 • Notifyは、ネットワークトラフィックをブロックせずに*暗号化が検知されました*イベントを作成します。
BlockTime	攻撃元デバイスのブロック期間（分単位）。

保護範囲の作成方法

*保護範囲*は、Kaspersky Endpoint Security がファイルの動作を監視する共有ネットワークディレクトリへのパスのリストです。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。既定では、本製品は共有ネットワークディレクトリを自動的に識別し、これらのディレクトリ内のファイルの動作を監視します。

必要に応じて、悪意のある暗号化に対するファイルの動作の監視を、一部のディレクトリのみに制限できます。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。

組織で、共有ネットワークディレクトリを介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、保護範囲からディレクトリを除外することで誤検知の量を減らすことができます。たとえば、ユーザーが共有フォルダーで拡張子 ENC のファイルを操作していると、アンチクリプターで誤検知が発生することがあります。このような操作は、外部からの暗号化攻撃に典型的な動作と一致します。データを保護するために共有ネットワークディレクトリに暗号化されたファイルがある場合は、そのディレクトリを除外リストに追加します。

Web コンソールでの保護範囲の作成方法

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. ［**ホスト脅威対策**］→［**ふるまい分析**］→［**アンチクリプター**］に移動します。
5. コンポーネントのトグルスイッチが **アンチクリプターは有効です** の位置にあることを確認します。
6. ［**保護範囲**］で、［**指定した共有フォルダーのみ**］を選択します。
7. ディレクトリのリストで、［**追加**］をクリックします。

8. ウィンドウが開きます。このウィンドウで、ファイルシステムの種類を選択します：

- **ローカル**ネットワーク接続なしでアクセスできるハードドライブ上のディレクトリ。
- **共有**Samba（SMB）または NFS プロトコルを使用してアクセスできるコンピューターのディレクトリ。
- **共有済みのすべての場所**Samba プロトコルおよび NFS プロトコルを使用してアクセスされるすべてのコンピューターのディレクトリ。

9. ローカルファイルシステムの場合は、ディレクトリパスを指定します（例：`/path/to/folder`）。

10. オブジェクトの拡張子のマスクを指定します（例：`*.txt`）。マスクはカンマで区切ります。

11. 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。

コマンドラインでの保護範囲の作成方法

1. 次のコマンドを実行します：

```
kesl-control --set-settings 13 ScanScope.item_#.UseScanArea=Yes \
        [ScanScope.item_#.AreaDesc=<description of the area>] \
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>] \
        [ScanScope.item_#.Path=<path to the directory>]
```

2. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 13
```

記号

コマンドオプション

設定	説明
`ScanScope.item_#.UseScanArea=Yes`	保護範囲番号 `#` を有効にします。 保護範囲を削除する代わりに、一時的に除外できます。これを行うには、`ScanScope.item_#.UseScanArea=No` を設定します。
`ScanScope.item_#.AreaDesc`	保護範囲の説明。保護範囲 `#` に関する追加情報を含みます。
`ScanScope.item_#.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。 **例** `ScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt.`
`ScanScope.item_#.Path`	保護するオブジェクトがあるディレクトリのパス。可能な値： • `AllShared`（既定）。Samba プロトコルおよび NFS プロトコルを使用してアクセスされるすべてのコンピューターのディレクトリ。 • `Shared:SMB` Samba（SMB）プロトコルを介してアクセス可能なディレクトリ。 • `Shared:NFS` NFS プロトコルを介してアクセス可能なディレクトリ。 • `<path to local directory>` ネットワーク接続なしでアクセスできるハードドライブ上のディレクトリ。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。

`/home` ディレクトリのみを含む保護範囲の例

```
kesl-control --set-settings 13 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

有害 USB 攻撃ブロック

攻撃者は、USB デバイス（フラッシュドライブなど）のファームウェアの脆弱性を悪用し、接続時にオペレーティングシステムがこのデバイスをキーボードとして認識するようにデバイスを再プログラムする可能性があります。その結果、感染した USB デバイスは、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。

有害 USB 攻撃ブロック保護コンポーネントを使用すると、感染した USB デバイスの接続を防止できます。

このコンポーネントは、Elbrus CPU を搭載したデバイスでは使用できません。

有害 USB 攻撃ブロックの仕組み

1. **アプリケーションにより、USB デバイスの認証を求められます**

   USB デバイスが端末に接続されると、本製品は、本製品によって生成された数値コードの入力をユーザーに要求します。この手順を*承認*と呼びます。

2. **ユーザーが承認コードを入力します**

   ユーザーは、接続されている USB デバイス自体（キーボードまたはバーコードスキャナー）、あるいは利用可能な場合はオンスクリーンキーボードを使用してコードを入力できます。すでに接続されている USB デバイスを使用してコードを入力することはできません。

3. **本製品は、承認済みの USB デバイスを許可し、未承認の USB デバイスをブロックします**

   数値コードが正しく入力されると、本製品は識別パラメータ（USB デバイスの VID/PID および接続されているポート番号）を、承認済み USB デバイスのリストに保存します。この USB デバイスは、再接続された場合またはオペレーティングシステムを再起動した場合、再度承認する必要はありません。

   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。数値コードの最大入力試行回数を設定できます。数値コードが数回誤って入力されると、本製品はこの USB デバイスからの入力を一定時間ブロックします。USB デバイスのロックアウト時間が経過するまで待機した後、USB デバイスの承認を再度試行できます。承認コードの入力試行を再開できるまでの時間を設定できます。

承認済みの USB デバイスが別の USB ポートに接続されると、本製品により再度承認が求められます。

有害 USB 攻撃ブロックの設定

1. **BadUSB 脅威対策の有効化**

   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。信頼できない人物が物理的にアクセスでき、外部の攻撃者から保護する必要がある端末を特定し、それらの端末で有害 USB 攻撃ブロックコンポーネントを有効にします。有害 USB 攻撃ブロックを有効にすると、本製品では接続された USB デバイスの承認が必要になり、ユーザーは承認されるまで未承認の USB デバイスを使用できません。ただし、有害 USB 攻撃ブロックが有効になる前に接続されていた USB デバイスは、既定で承認済みと見なされ、承認は不要です。

   > 有害 USB 攻撃ブロックを有効にして設定するまでは、信頼できない USB デバイスを端末に接続しないでください。

2. **有害 USB 攻撃ブロックを設定する**

   接続する USB デバイスの種類（キーボードまたはバーコードスキャナー）に応じて、承認コードをバーコードとして表示するか、数値コード（既定の設定）として表示するかを設定します。

   必要に応じて、USB デバイスの認証を設定します：

   - 承認コードの最大入力試行回数
   - 最大試行回数に達した場合の USB デバイスのブロック期間。

USB デバイスの認証を設定する方法

オペレーティングシステムが入力デバイスとして認識する USB デバイスが管理対象デバイスに接続されると、本製品は数値コードまたはバーコードを使用して USB デバイスを認証するよう提案します。認証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。認証コードが複数回間違って入力された場合、または認証ウィンドウが閉じられた場合、本製品はこの USB デバイス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が経過した場合、またはオペレーティングシステムが再起動された場合、本製品はユーザーに認証を再度実行するよう要求します。

Kaspersky Endpoint Security では、USB デバイスの認証を設定できます

- 認証試行の最大回数。
- 最大試行回数に達した場合の USB デバイスのブロック期間。

Web コンソールで USB デバイスの認証を設定する方法

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. ［**ホスト脅威対策**］→［**有害 USB 攻撃ブロック**］に移動します。
5. コンポーネントのトグルスイッチが **有害 USB 攻撃ブロックは有効です** の位置にあることを確認します。

6. ［**USB デバイスの認証**］で、認証設定を行います：

- **USB デバイスの最大認証試行回数**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。

- **最大試行回数に達した場合のタイムアウト（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）

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。

有害 USB 攻撃ブロック

コマンドラインで USB デバイスの認証を設定する方法

1. 次のコマンドを実行します：

```
kesl-control --set-settings 37 MaxAuthAttempts=<number of attempts> TimeoutAfterAttempts=<timeout (minutes)>
```

2. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 37
```

記号

コマンドオプション

設定	説明
`MaxAuthAttempts`	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
`TimeoutAfterAttempts`	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 分。

オンスクリーンキーボードを使用した USB デバイスの接続を許可する方法

セキュリティキーボードは、任意の文字の入力をサポートしない USB デバイス（バーコードスキャナーなど）の認証時にのみ使用してください。未知の USB デバイスの認証時に、セキュリティキーボードを使用しないでください。既定では、オンスクリーンキーボードの使用が許可されています。

オンスクリーンキーボードは、ユーザーが認識している USB デバイスの認証にのみ使用することを推奨します。

Web コンソールでオンスクリーンキーボードを使用した USB デバイスの認証を有効にする方法

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. ［**ホスト脅威対策**］→［**有害 USB 攻撃ブロック**］に移動します。
5. コンポーネントのトグルスイッチが **有害 USB 攻撃ブロックは有効です** の位置にあることを確認します。
6. ［**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**］がオフになっていることを確認してください。この切り替えボタンは既定でオフになっています。
7. ポリシーをデバイスに適用するには、🔒 南京錠のアイコンを閉じて変更を保存します。

コマンドラインでオンスクリーンキーボードを使用した USB デバイスの認証を有効にする方法

次のコマンドを実行します：

```
kesl-control --set-settings 37 ProhibitOnScreenKeyboard=No
```

バーコードスキャナーを使用した USB デバイスの接続を許可する方法

バーコードスキャナーをデバイスに接続すると、有害 USB 攻撃ブロックは、このスキャナーを入力デバイスとして識別し、認証の実行を求めます。バーコードスキャナーを認証するには、画面に表示されるバーコードをスキャンする必要があります。製品は Code39 形式のバーコードを生成します。ほとんどのバーコードスキャナーと QR コードスキャナーはこの形式に対応しています。

製品は、バーコードスキャナーを認証する別の方法にも対応しています。タッチスクリーンデバイスを使用している場合は、セキュリティキーボードを使用してコードを入力できます。そのためには、セキュリティキーボードを許可する必要があります。この方法は、たとえばレジに組み込まれた固定式のバーコードスキャナーの場合に便利です。その他のバーコードスキャナーの認証方法は禁止されています。既定では、本製品は USB デバイスの認証にバーコードを使用しません。

Web コンソールでバーコードスキャナーを使用した USB デバイス認証を有効にする方法

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. ［**ホスト脅威対策**］→［**有害 USB 攻撃ブロック**］に移動します。
5. コンポーネントのトグルスイッチが **有害 USB 攻撃ブロックは有効です** の位置にあることを確認します。
6. **USB デバイスの認証時にバーコードの使用を禁止する** トグルスイッチをオフにします。
7. ポリシーをデバイスに適用するには、南京錠のアイコンを閉じて変更を保存します。

コマンドラインでバーコードスキャナーを使用した USB デバイス認証を有効にする方法

次のコマンドを実行します：

```
kesl-control --set-settings 37 ProhibitBarcodeScanner=No
```

通信と危険サイト対策

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、次のメールクライアントで POP3、SMTP、IMAP をサポートします。また、本製品は、プロトコルの拡張版である POP3S、SMTPS、IMAPS もサポートします。

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。

> 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、110、143、465、587、993、および 995 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。

メール脅威対策の仕組み

Kaspersky Endpoint Security をインストールすると、本製品は自己署名証明書 *カスペルスキーアンチウイルス個人用ルート証明書* を追加します。本製品はこの証明書をローカルの信頼済み証明書ストア（`/etc/ssl/certs`）に配置します。本製品は起動するたびに、証明書が存在するかどうかを確認します。証明書が削除されている場合、本製品は証明書を自動的に復元します。

1. **本製品がメールトラフィックをインターセプトします**

   Kaspersky Endpoint Security は、POP3、SMTP、IMAP プロトコルによる接続をチェックします。

2. **本製品は受信メッセージと送信メッセージをスキャンします**

   メール脅威対策は、次の技術を使用してトラフィックをスキャンします：

   - 定義データベース。
   - Kaspersky Security Network のクラウドサービス。
   - ヒューリスティック分析技術により、カスペルスキーの定義データベースではまだ対応していない脅威を検知できます。

3. **本製品がスキャンを完了します**

   受信メッセージの添付ファイルまたはメッセージ本文に脅威が含まれている場合、Kaspersky Endpoint Security は脅威の検知時の処理を実行します。送信メッセージで脅威が検知された場合、メール脅威対策はそのメッセージの送信をブロックします。

メール脅威対策の設定

1. **コンポーネントのテスト導入用グループを定義する**

   メール脅威対策コンポーネントの設定をテストするために、少数のデバイスからなるグループを別に用意します。これにより、コンポーネントが正しく設定されていることを確認し、メールクライアントの安定した動作を確保して、発生する可能性のある障害を回避できます。

2. **添付ファイルフィルターを設定する**

   既定では、カスペルスキーが設定したメール脅威対策フィルターにより、推奨される保護レベルが提供されます。メールセキュリティに関して特別な要件がある場合は、添付ファイルフィルターの設定を変更できます。

3. **メッセージスキャンを設定する**

   必要に応じて、メールサーバーのパラメータに従ってメールメッセージのスキャンを設定します。たとえば、メールサーバーの負荷を軽減するために、スキャンするアーカイブのサイズを制限できます。

4. **メール脅威対策が正しく動作していることを確認する**

   悪意のある添付ファイルを含むテストメッセージを生成します。選択したデバイスグループにメッセージを送信し、メッセージ内の悪意のあるコンテンツがコンポーネントの設定に従って処理されたことを確認します。

   次のコマンドを実行して、本製品が対応する *脅威が検知されました* イベントを生成したことも確認できます：

```
kesl-control -E -q "TaskName == 'Mail_Monitoring'"
```

5. **組織内のすべてのデバイスにメール脅威対策の設定を適用する**

特別な考慮事項と制限事項

- 保護対象デバイス上のメールクライアントが信頼済み証明書のローカルストアを使用しない場合は、*カスペルスキー アンチウイルス パーソナルルート証明書*証明書をメールクライアントの信頼済み証明書ストアに手動で追加します。証明書の追加の詳細については、お使いのメールクライアントの公式ドキュメントを参照してください。

- メール脅威対策は、送信メール内の悪意のある添付ファイルの駆除を試行しません。悪意のある添付ファイルを含む送信メッセージは、完全にブロックされるか、通過が許可されます。

メール脅威が検知された場合の対処法

*送信メッセージ*の添付ファイルで感染したオブジェクトが検知されると、本製品はそのメッセージの送信を防止します。

*受信メッセージ*で感染したオブジェクトが検知されると、本製品はオブジェクトの駆除を試みてから、オブジェクトを削除するか、オブジェクトへのアクセスをブロックできます。Kaspersky Endpoint Security は、実行された処理に関する情報もメッセージの件名に追加します（例：*[メッセージは処理されました]* <*メッセージの件名*>）。

メール脅威対策を設定するとき、メールメッセージで脅威が検知された場合に Kaspersky Endpoint Security が実行する処理を選択できます。

Web コンソールで脅威検知時の処理を設定するには

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. ［**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**］に移動します。

5. 「**脅威の検知時の処理**」で、脅威が検知された場合に本製品が実行する処理を選択します：

- **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*>）。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。

- **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。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。

- **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。

6. 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。

メール脅威対策

コマンドラインで脅威検知時の処理を設定するには

1. メール脅威対策コンポーネントが有効になっていることを確認します：

```
kesl-control --get-task-state 35
```

コンポーネントのステータスは **開始済み** である必要があります。

2. コンポーネントが無効になっている場合は、次のコマンドを実行します：

```
kesl-control --start-task 35
```

3. 受信メッセージでメール脅威が検知された場合に実行する処理を選択します：

```
kesl-control --set-settings 35 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
```

4. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 35
```

記号

コマンドオプション

設定	説明
ActionOnThreat	脅威の検知時の処理： • DisinfectDeleteIfNotPossible（既定）。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>*）。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。 • DisinfectBlockIfNotPossible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。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。 • Block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。

メール添付ファイルのスキャンを最適化する方法

メール脅威対策コンポーネントを最適化するには、メール添付ファイルのスキャンを設定します。これにより、保護対象デバイスの CPU 使用率を低減できます。添付されたアーカイブのスキャンを制限したり、スキャン可能な添付ファイルの最大サイズを設定したり、オブジェクトの最大スキャン時間を設定したりできます。

Web コンソールで添付ファイルのスキャンを最適化する方法

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. ［**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**］に移動します。

5. ［**詳細設定**］で、［**スキャン設定**］を選択します。

6. 添付ファイルのスキャンを設定します：

- **添付のアーカイブのスキャン**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**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）**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）**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。

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。

コマンドラインで添付ファイルのスキャンを最適化する方法

1. メール脅威対策コンポーネントが有効になっていることを確認します：

```
kesl-control --get-task-state 35
```

2. コンポーネントのステータスは `Started` である必要があります。

3. コンポーネントが無効になっている場合は、次のコマンドを実行します：

```
kesl-control --start-task 35
```

4. 受信メッセージでメール脅威が検知された場合に実行する処理を選択します：

```
kesl-control --set-settings 35 [ScanFileArchive=<Yes|No>] [UseSizeLimit=<Yes|No>] [SizeLimit=<archive size
(MB)>] [UseTimeLimit=<Yes|No>] [TimeLimit=<scan time (sec)>] [ScanFileOffice=<Yes|No>]
```

5. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 35
```

記号

設定	説明
ScanFileArchive	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、本製品は添付されたアーカイブをスキャンします。
UseSizeLimit SizeLimit	スキャンできる添付されたアーカイブのサイズを制限します。メール脅威対策は、添付されたアーカイブのサイズが指定した値を超える場合、スキャン時にそのアーカイブをスキップします。既定では、本製品はサイズに関係なくアーカイブをスキャンします。
UseTimeLimit TimeLimit	添付されたアーカイブのスキャン時間の制限。既定では、添付されたアーカイブのスキャン時間は制限されません。
ScanFileOffice	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、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、本製品は添付された Office 形式のファイルをスキャンします。

メール添付ファイルフィルターの用途

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。

悪意のあるアプリケーションは、メールの添付ファイルという形式で配信されることがあります。メールの添付ファイル種別によるフィルタリングを設定し、特定の種類のファイルを自動的に名前変更したり削除したりできます。特定の種類の添付ファイルの名前を変更することにより、悪意のあるアプリケーションの自動実行を防ぐことができます。

たとえば、HTML ファイルに対する添付ファイルのフィルタリングを設定できます。HTML ファイルには悪意のあるスクリプトが含まれている可能性があります。本製品がそのようなファイルの名前を変更すると、ユーザーはメールメッセージ内の HTML ページをダブルクリックしても開くことができなくなります。HTML ファイルを開くには、ユーザーはファイルをダウンロードして名前を変更する必要があります。これにより、ユーザーは受信したメッセージを分析し、悪意のあるスクリプトの実行を防止する時間を確保できます。

既定では、本製品は CMD、COM、EXE、JS、JSE、MSI、SCR、VBE、VBS、SH の拡張子を持つファイルの名前を変更します。本製品は、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ます（例：attachment.doc_）。

Web コンソールで添付ファイルフィルターを設定するには

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. ［**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**］に移動します。
5. ［**詳細設定**］で、［**添付ファイルのフィルター**］を選択します。

6. 本製品がメール添付ファイルに対して実行する処理を選択します：

   - **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。

7. 前のステップで **選択した種別の添付ファイルの名前を変更する** または **選択した種別の添付ファイルを削除する** オプションを選択した場合は、該当するファイル種別のチェックボックスをオンにします。

8. 必要なファイル種別がリストにない場合は、新しい添付ファイル種別を追加します：

   a. ［**追加**］をクリックします。

      これにより、新しい添付ファイル種別を追加するためのフォームが開きます。

   b. **添付ファイル種別** フィールドで、拡張子マスクを `*.<extension>` 形式（例：`*.doc`）で指定します。

      複数のファイル種別を指定する場合は、ファイル種別ごとに新しい行に入力します。

9. 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。

コマンドラインで添付ファイルフィルターを設定するには

1. メール脅威対策コンポーネントが有効になっていることを確認します：

```
kesl-control --get-task-state 35
```

2. コンポーネントのステータスは `Started` である必要があります。

3. コンポーネントが無効になっている場合は、次のコマンドを実行します：

```
kesl-control --start-task 35
```

4. 本製品がメール添付ファイルに対して実行する処理を選択します：

```
kesl-control --set-settings 35 ExtensionFilter=<Disable|Rename|Delete>
ExtensionMasks.item_#.UseExtensionMask=Yes\
[ExtensionMasks=*.<extention>]
```

5. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 35
```

記号

設定	説明
ExtensionFilter	本製品がメール添付ファイルに対して実行する処理： Disable 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。 Rename（既定）。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。 Delete 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。
UseExtensionMask=Yes	添付ファイルフィルターにファイル種別を追加します。 添付ファイルフィルターからファイル種別を削除する代わりに、そのファイル種別を一時的に除外できます。これを行うには、 ExtensionMasks.item_#.UseExtensionMask=No を設定します
ExtensionMasks=*.<extention>	メールメッセージから名前を変更または削除する添付ファイル種別の拡張子。

ウェブ脅威対策

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への接続もブロックします。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。

ウェブ脅威対策の仕組み

Kaspersky Endpoint Security をインストールすると、本製品は自己署名証明書 *カスペルスキーアンチウイルス個人用ルート証明書* を追加します。アプリケーションは、この証明書をローカルの信頼済み証明書ストア（/etc/ssl/certs）とウェブブラウザーの証明書ストアに配置します。本製品は起動するたびに、証明書が存在するかどうかを確認します。証明書が削除されている場合、本製品は証明書を自動的に復元します。

1. **送信接続のインターセプト**

   サードパーティ製アプリケーション（ブラウザーなど）がサーバーへの接続を開始します。Kaspersky Endpoint Security は、サーバー証明書を、カスペルスキー アンチウイルス パーソナル ルート証明書で署名された独自の証明書に置き換えます。次に、アプリケーションは暗号化鍵をインターセプトし、通信セッションを復号します。Kaspersky Endpoint Security は、カスペルスキー アンチウイルス パーソナル ルート証明書が信頼済み証明書ストアにあるため、ユーザーにアラートを表示することなくこの処理を実行します。

2. **ネットワークトラフィックのスキャン**

   ウェブ脅威対策は、次の技術を使用してトラフィックをスキャンします：

   - 定義データベース。
   - Kaspersky Security Network のクラウドサービス。
   - ヒューリスティック分析技術により、カスペルスキーの定義データベースではまだ対応していない脅威を検知できます。

3. **スキャンの完了**

   ウェブサイトが悪意のあるサイトまたはフィッシングサイトとして分類された場合、Kaspersky Endpoint Security は、ウェブ脅威対策コンポーネントの設定で指定された処理を実行します。接続をブロックするか、警告を表示します。

ウェブ脅威対策の設定

1. **OS の Firewall のルールを設定します**

   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ように、ローカルデバイス（ループバック）からの着信接続を許可するルール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
   ```

2. **ネットワークトラフィックのインターセプトモードを選択する**

   ネットワークパケットを受信すると、ウェブ脅威対策は脅威をスキャンするためにデータを抽出します。ネットワークトラフィックのインターセプトでは、次のモードを使用できます：

   - eBPF
   - iptables（既定）

   ネットワークトラフィックのインターセプトモードの選択は、組織のインフラストラクチャによって異なります。閉じた境界内では、eBPF の使用を推奨します。その他のシナリオでは、iptables を使用します。

   > ネットワークトラフィックのインターセプトモードに応じて、デバイスを異なる管理グループにグループ化することを推奨します。

3. **証明書検証ポリシーを設定する**

   既定では、ウェブ脅威対策は、暗号化された接続を介して送信される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。デバイスがインターネットに直接アクセスできない場合は、ローカルの証明書検証方法を選択する（インターネットを使用しない）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。

   証明書検証ポリシーには、次の設定も含まれます：

   - 信頼されていない証明書を持つ Web サイトへのアクセス
   - 証明書の検証エラーがある Web サイトへのアクセス

   既定では、Kaspersky Endpoint Security は、信頼されていない証明書を使用する Web サイトへの移動を許可し、証明書検証エラーのあるドメインを除外リストに追加します。証明書検証エラーは、たとえば、バンキングアプリケーションやクラウドストレージを使用している場合に発生することがあります。これらのサービスが属するドメインが、Kaspersky Anti-Virus Personal Root Certificate を拒否する場合があります。独自の証明書検証ポリシーを設定することができます。

4. **信頼済み証明書を追加する**

   組織が内部サーバー用の証明書を発行するためにプライベート認証局を使用している場合、Kaspersky Endpoint Security が証明書検証エラーにより Web リソースへのアクセスをブロックする可能性があります。Web リソースを暗号化された接続のスキャンから除外するには、これらの証明書を信頼済みリストに追加します。

5. **ウェブ脅威対策の設定で、処理として「通知」を選択します。**

   既定では、ウェブ脅威対策タスクは無効です。ウェブ脅威対策を有効にし、脅威の検知時の処理として **通知** を選択して、すべての企業リソースへのアクセスを確認することを推奨します。Kaspersky Endpoint Security は、すべての Web サイトへのアクセスを許可し、検知された脅威に関する情報をログに記録します。

6. **ウェブ脅威対策が安全でないと判断した Web サイトに関する統計情報を収集する**

   ウェブ脅威対策が安全でないと判断した Web サイトの統計情報は、レポートを使用して取得できます。

7. **信頼する URL を追加する**

   ウェブ脅威対策のレポートを確認した後、信頼済みリストに信頼する URL を追加する必要があります。信頼する URL のリストだけでは、Kaspersky Endpoint Security とサードパーティ製アプリケーションと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 を使用することができます。*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。

8. **ウェブ脅威対策の設定で、処理として「ブロック」を選択します。**

   Web トラフィック内の感染オブジェクトのブロックを有効にします。

特別な考慮事項と制限事項

- アプリケーションは TCP ポートの受信トラフィックをスキャンし、localhost 上のポート 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。
- 本製品を有効または無効にした場合、および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有効または無効にした場合、インターセプトされたポート上の接続が切断されます。
- Kaspersky Endpoint Security は、HTTP および HTTPS トラフィックをスキャンします。URL、IP アドレスがスキャンされます。
- 本製品は、snap 形式を含む、次のブラウザーの実行ファイルをサポートしています：
  - chrome
  - chromium
  - chromium-browser
  - firefox
  - firefox-esr
  - google-chrome
  - opera
  - yandex-browser

- ユーザーが悪意のある Web サイトにアクセスしようとすると、本製品は次の処理を実行します：
  - **HTTP**。本製品はアクセスをブロックし、警告を表示します。
  - **HTTPS**。本製品はアクセスをブロックし、ブラウザーには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。

役立つ記事

「信頼されていない証明書を持つドメインにアクセスしています」という警告が表示された場合の対処方法

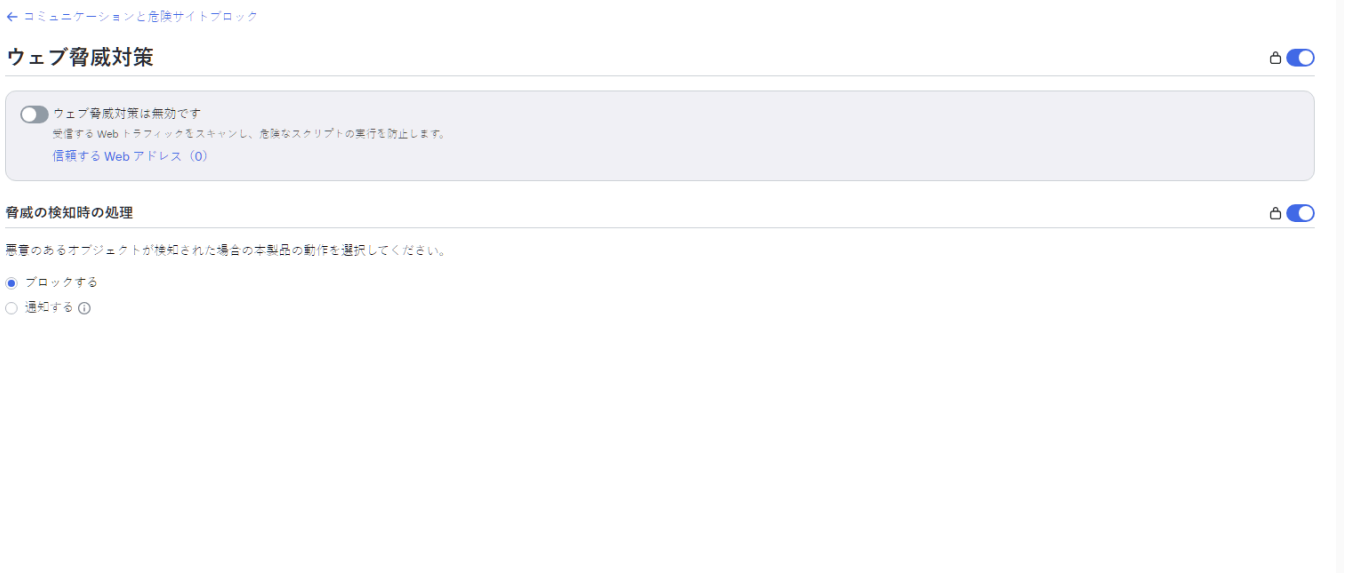
Web 脅威の検知時に実行する処理を選択する方法

Web 脅威が検知されると、Kaspersky Endpoint Security は危険なオブジェクトへのアクセスをブロックするか、危険なオブジェクトの検知について通知のみを行います。

Web コンソールで Web 脅威の検知時に実行する処理を設定する方法

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. ［**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**］に移動します。
5. 「**脅威の検知時の処理**」で、脅威が検知された場合に本製品が実行する処理を選択します：
   - **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。
   - **通知する**Kaspersky Endpoint Security は、Web トラフィック内の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。

6. 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。



ウェブ脅威対策

コマンドラインで脅威検知時の処理を設定するには

1. 次のコマンドを実行します：

```
kesl-control --set-settings 14 ActionOnDetect=<Block|Notify>
```

2. リンクのスキャンに使用する定義データベースを選択します：

```
kesl-control --set-settings 14 CheckMalicious=<Yes|No> CheckAdware=<Yes|No> CheckOther=<Yes|No>
```

3. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 14
```

記号

コマンドオプション

設定	説明
ActionOnDetect	脅威の検知時の処理： • Block（既定）。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。 • Notify このオプションを選択した場合、Web トラフィックで感染したオブジェクトが検知されると、Kaspersky Endpoint Security はこのオブジェクトのコンピューターへのダウンロードを許可しますが、感染したオブジェクトに関する情報をアクティブな脅威のリストに追加します。
CheckMalicious	Web アドレスをスキャンして悪意のあるリンクのデータベース内で確認し、Web サイトが拒否リストに登録されているかどうかを確認できます。カスペルスキーが維持する悪意のある URL のデータベースはアプリケーションインストールパッケージに含まれており、Kaspersky Endpoint Security の定義データベースアップデート時にアップデートされます。スキャンは既定で有効になっています（Yes）。
CheckAdware	広告 URL のデータベースとの照合によるリンクのチェック。スキャンは既定で無効になっています（No）。
CheckOther	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含む URL のデータベースとの照合によるリンクのチェック。スキャンは既定で無効になっています（No）。

フィッシング対策とは

ウェブ脅威対策では、リンクがフィッシングサイトへのリンクでないか確認します。これは*フィッシング攻撃*の防止になります。フィッシング攻撃は偽装して行われることがあります。たとえば、メールが銀行から来たもので、その銀行のオフィシャル Web サイトへのリンクが含まれているように見せかけます。リンクをクリックすると、その銀行の偽装サイトに移動します。偽装サイトにアクセスしているにもかかわらず、ブラウザーにはその銀行の実際の Web アドレスが表示されているように見えることがあります。それ以降、偽装サイトでの処理がすべて追跡され、現金が盗まれることがあります。

フィッシングサイトへのリンクは、メールからだけでなく、メッセンジャーなどの他のソースから受け取ることもあります。このため、ウェブ脅威対策は、Web トラフィックのレベルでフィッシングサイトへのアクセスを試行し、その Web サイトへのアクセスをブロックします。フィッシングサイトの URL のリストは、Kaspersky Endpoint Security の配信キットに含まれています。

フィッシング対策機能は、コマンドラインでのみ設定できます。Web コンソールではフィッシング対策を設定できません。既定では、フィッシング対策ではヒューリスティック分析が有効になっています。

コマンドラインでフィッシング対策を有効にする方法

1. ウェブ脅威対策コンポーネントが有効になっていることを確認します：

   ```
   kesl-control --get-task-state 14
   ```

   コンポーネントのステータスは **開始済み** である必要があります。

2. コンポーネントが無効になっている場合は、次のコマンドを実行します：

   ```
   kesl-control --start-task 14
   ```

3. フィッシング対策を有効にします：

   ```
   kesl-control --set-settings 14 CheckPhishing=Yes
   ```

4. フィッシングリンクがないかWebページをスキャンするためのヒューリスティック分析を設定します：

   ```
   kesl-control --set-settings 14 UseHeuristicForPhishing=<Yes|No>
   ```

   この設定は、Elbrus CPUを搭載したデバイスには適用されません。

5. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

   ```
   kesl-control --get-settings 14
   ```

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（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。

ネットワーク脅威対策の仕組み

1. **本製品は受信パケットを解析します**

   受信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。iptables トラフィックインターセプトモードでのネットワークスキャン処理中は、システム上のアプリケーションがそのポートをリッスンしていない場合でも、デバイス上でポートが開いているように見えることがあります。未使用のポートは Firewall で閉じておくことを推奨します。

2. **本製品は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、次の技術を使用して受信トラフィックをスキャンします：

   - 定義データベース。
   - Kaspersky Security Network のクラウドサービス。
   - ヒューリスティック分析技術により、カスペルスキーの定義データベースではまだ対応していない脅威を検知できます。

3. **スキャンの完了**

   ネットワーク脅威が検知されると、本製品は攻撃元デバイスからのすべてのネットワーク接続を指定された期間ブロックします。

ネットワーク脅威対策の設定

1. **OS の Firewall のルールを設定します**

   REDIRECT ルール（例：ポート 443 から 8443 へのリダイレクト）とネットワーク脅威対策のインターセプトルールとの互換性を確保するには、REDIRECT ルールを削除してインターセプトルールを追加する必要があります。

   REDIRECT ルールを削除するコマンドの例：

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

   インターセプトルールを追加するコマンドの例：

```
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
```

2. **監視対象ネットワークポートのリストの作成**

   既定では、本製品は既知の登録済みポートを監視します。たとえば、HTTPS 接続用のポート 443、IMAP メールプロトコル用のポート 143 などです。既定の設定により、推奨される保護レベルおよび最適なリソースを使用できます。必要に応じて、監視対象ポートのリストを変更するか、すべてのポートの監視を有効にすることができます。

3. **トラフィックインターセプトモードの選択**

   ネットワークパケットを受信すると、ネットワーク脅威対策は脅威をスキャンするためにデータを抽出します。受信トラフィックのインターセプトには、次のモードを使用できます：

   - eBPF
   - iptables（既定）

   トラフィックインターセプトモードの選択は、組織のインフラストラクチャによって異なります。閉じた境界内では、eBPF の使用を推奨します。その他のシナリオでは、iptables を使用します。

   > トラフィックインターセプトモードに応じて、デバイスを異なる管理グループにグループ化することを推奨します。

4. **通知モードでウェブ脅威対策を有効にする**

   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ブロックモードで有効にする前に、通知モードでコンポーネントを有効にすることを推奨します。これにより、Kaspersky Endpoint Security は、ネットワーク接続を中断することなく、不審なネットワークアクティビティを検知し、検知されたネットワーク攻撃に関する情報を記録できます。サードパーティ製の企業アプリケーションによるネットワークリソースへのアクセスを確認してください。ネットワークポート制御によってこれらのアプリケーションの動作が遅くならないことを確認してください。

5. **ネットワーク脅威対策が疑わしいネットワークアクティビティを検知した送信元 IP アドレスの統計情報を収集する**

   ネットワーク脅威対策が安全でないと判断した IP アドレスの統計情報を取得するには、レポートを確認できます。本製品は、*ネットワーク攻撃が検知されました*イベントを生成します。

6 **信頼する IP アドレスの追加**

ネットワーク脅威対策のレポートを確認した後、ネットワーク接続を信頼するデバイスの IP アドレスを信頼リストに追加する必要があります。個々のデバイスまたはサブネットのアドレスを除外リストに追加できます。ネットワーク脅威対策は、このようなデバイスから送信されるパケットをインターセプトまたはスキャンしません。

7 **ブロックモードでネットワーク脅威対策を有効にする**

信頼するデバイスの IP アドレスを除外リストに追加した後、コンポーネントをブロックモードで有効にします。信頼されていないデバイスのネットワークアクティビティはブロックされ、その旨の情報がレポートに表示されます。

特別な考慮事項と制限事項

- 本製品は、TCP ポートの受信トラフィックをスキャンします。本製品は、接続をインターセプトするために、localhost 上の固定ポート 9789 を使用します。
- 本製品を有効または無効にした場合、および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有効または無効にした場合、インターセプトされたポート上の接続が切断されます。
- CentOS 5.2 および 5.4 が実行されているコンピューターでは、TProxy がサポートされていないため、ネットワーク脅威対策は機能しません。

ネットワーク脅威の検知時に実行する処理を選択する方法

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元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、*ネットワーク攻撃が検知されました*イベントを作成します。

ネットワークトラフィックをブロックするため、Kaspersky Endpoint Security は動的 Firewall ルールを作成します。Firewall は、攻撃元デバイスのネットワークトラフィックを一時的にブロックします。アプリケーションは、侵害されたデバイスもブロックされたデバイスのリストに追加します。ブロックされたデバイスは、共有ネットワークディレクトリへのアクセスを拒否されます。

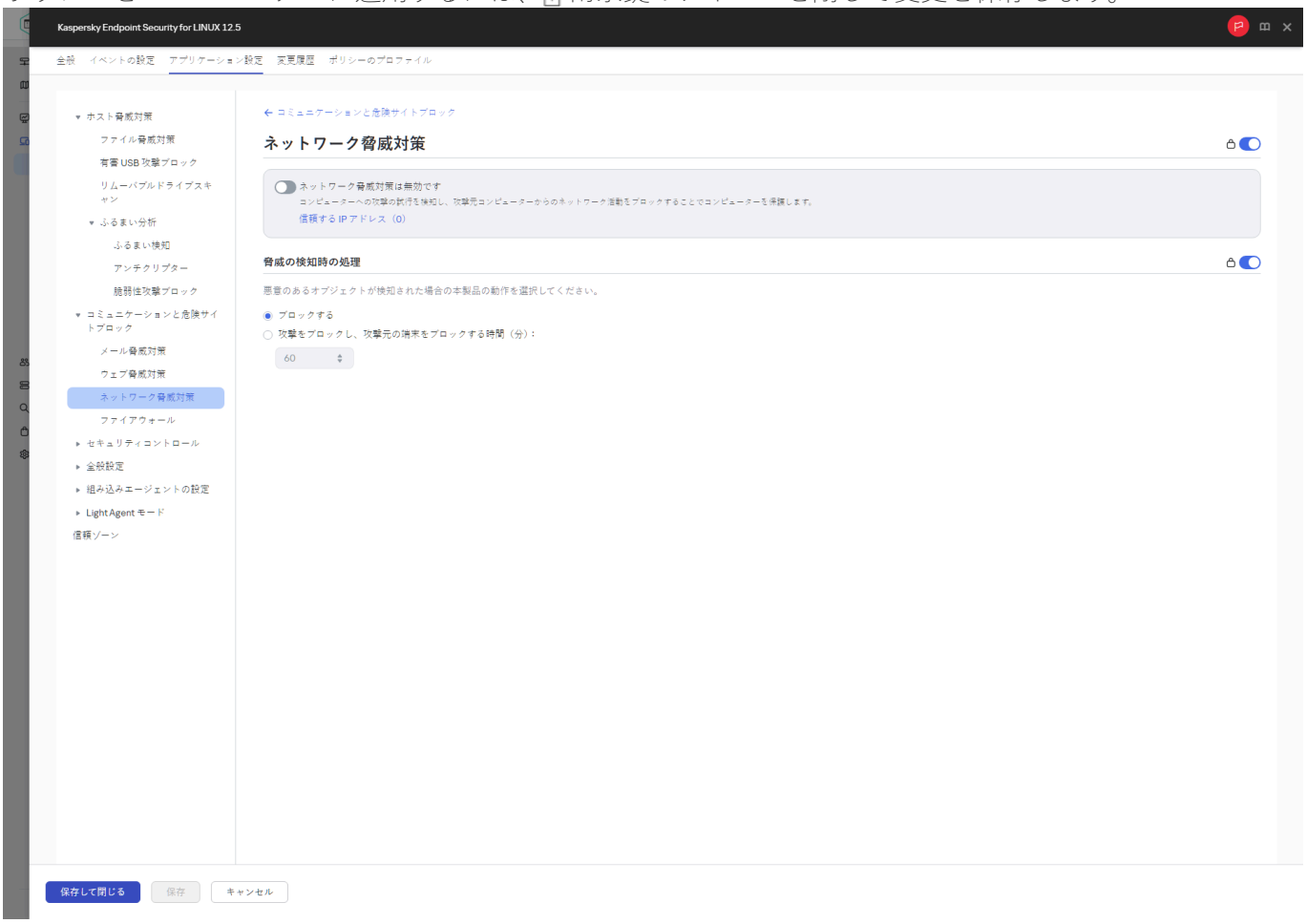
Web コンソールでネットワーク攻撃の検知時の処理を設定する方法

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. ［**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**］に移動します。
5. コンポーネントのトグルスイッチが **ネットワーク脅威対策は有効です** の位置にあることを確認します。
6. ［**Linux デバイスのネットワーク脅威対策を有効にする**］チェックボックスをオンにします。
7. **脅威の検知時の処理**で、脅威が検知されたときにアプリケーションが実行する処理（**ブロックする**または**攻撃をブロックし、攻撃元の端末をブロックする時間（分）**）を選択します。

8. **攻撃をブロックし、攻撃元の端末をブロックする時間（分）**を選択した場合、侵害されたデバイスのブロック期間を分単位で設定します。既定では、デバイスは60 分間ブロックされます。有効な値は1～999 です。

9. 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。



ネットワーク脅威対策

コマンドラインでネットワーク攻撃の検知時の処理を設定する方法

1. ネットワーク脅威対策コンポーネントが有効になっていることを確認します：

```
kesl-control --get-task-state 17
```

コンポーネントのステータスは **開始済み** である必要があります。

2. コンポーネントが無効になっている場合は、次のコマンドを実行します：

```
kesl-control --start-task 17
```

3. ネットワーク脅威の検知時の処理を選択します：

```
kesl-control --set-settings 17 ActionOnDetect=<Block|Notify>
```

4. 侵害されたデバイスのブロックを設定します：

```
kesl-control --set-settings 17 BlockAttackingHosts=<Yes|No>
```

5. `BlockAttackingHosts=Yes` 処理のブロック期間を選択します：

```
kesl-control --set-settings 17 BlockDurationMinutes=<Blocking period>
```

6. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 17
```

記号

コマンドオプション

設定	説明
`ActionOnDetect`	ネットワーク脅威の検知時の処理： • `Block`（既定）は、侵害されたデバイスのネットワークトラフィックをブロックし、*ネットワーク攻撃が検知されました*イベントを作成します。 • `Notify` は、ネットワークトラフィックをブロックせずに*ネットワーク攻撃が検知されました*イベントを作成します。
`BlockAttackingHosts`	攻撃元デバイスのネットワーク動作をブロックします。既定では、デバイスのブロックは 有効になっています。
`BlockDurationMinutes`	悪意のある動作または悪意のあるデータ暗号化に関与しているリモートデバイスのブロック期間を設定します。

ブロックされたデバイスを管理する方法

Kaspersky Endpoint Security は、ネットワークの脅威やリモートからの悪意のある暗号化からデバイスを保護する際、悪意のある動作をしていると判断されたリモートデバイスをブロックできます。これらの種類の脅威から、アンチクリプターおよびネットワーク脅威対策コンポーネントによってデバイスが保護されます。Kaspersky Endpoint Security は、一定時間ネットワークトラフィックをブロックします。ブロック期間が終了すると、Kaspersky Endpoint Security はネットワークトラフィックの再開を許可します。既定では、本製品は攻撃元デバイスのネットワークトラフィックを60 分間ブロックします。ブロック期間が終了すると、本製品はこのデバイスをブロックされたデバイスのリストから削除します。

Kaspersky Endpoint Security が信頼するデバイスをブロックした場合は、このデバイスの IP アドレスを除外リストに追加する必要があります。

ブロックされたデバイスのリストを表示する方法

```
kesl-control -H --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。

ブロックされたデバイスのリスト

```
Blocked devices: 1
Host                : 10.69.119.234
Block date          : 2026-04-29 15:44
Will be unblocked   : 2026-04-29 16:44
Task name           : Network_Threat_Protection
```

デバイスのブロックを解除する方法

```
kesl-control -H --allow-hosts <address>
```

ここで、`<address>` は、デバイスまたはサブネットの 1 つ以上の IP アドレス（IPv4 / IPv6、短縮形式のアドレスを含む）です。デバイスまたはサブネットの IP アドレスをスペースで区切って複数指定できます。

ファイアウォール管理

オペレーティングシステムの Firewall は、インターネットまたはローカルネットワークでのアクティビティを問わず、デバイスのすべてのネットワークアクティビティを制御します。Firewall は、デバイス上のデータを不正アクセスから保護し、ネットワークからデバイスへの攻撃など、ほとんどの脅威をブロックします。Firewall 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取得できます。

製品は、Firewall 管理コンポーネントを使用して、オペレーティングシステムの Firewall を管理します。このコンポーネントは、デバイスのネットワークアクティビティを監視するために、オペレーティングシステムの Firewall に ネットワークパケットルールを追加します。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。

Firewall 管理が有効になっている場合、Kaspersky Endpoint Security は 60 秒ごとにオペレーティングシステムの Firewall をチェックします。チェックの結果、サードパーティ製アプリケーションまたはユーティリティがネットワークパケットルールを追加または削除したことが判明した場合、Kaspersky Endpoint Security は製品を使用して作成された Firewall ルールのセットを復元します。

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。

Firewall 管理コンポーネントを有効にする前に、次の操作を実行してください：

- オペレーティングシステムの Firewall を管理する他のツールを無効にします。
- Firewall 管理コンポーネントを有効にする前に設定したカスタム Firewall ルールを保存し、バックアップを作成します。

ネットワークパケットルールを作成する方法

Firewallは、*ネットワークパケットルール*に従って、保護対象デバイス上のすべてのネットワーク動作をフィルタリングします。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または接続を制限します。ルールでは、次の条件に従ってネットワーク動作を許可または拒否できます。

- 接続プロトコルとポート
- トラフィックの方向
- ネットワークトラフィックを送受信するデバイスのIPアドレス

ネットワークパケットルールの優先順位

既定では、すべての送信パケットと接続。既定のルールの優先順位は最も低くなります。他のネットワークパケットルールが適用されていない場合、または他のネットワークパケットルールが指定されていない場合、ネットワーク動作は許可されます。

Firewallは、ネットワークパケットルールを優先順位に従って適用します。ルールの優先順位は、リスト内の位置（上から下）によって決まります。Firewallは、リスト内の最初のルールに基づいてネットワーク接続をフィルタリングし、ネットワーク動作を許可またはブロックします。ルールが一致しない場合、Firewallはリスト内の次のルールを適用し、以下同様に続けます。その後、コンポーネントはその接続に一致したルール以降のすべてのネットワークパケットルールを無視します。

ネットワークパケットルールを作成するための推奨事項

コマンドラインでネットワークパケットルールを作成するには、コマンドラインオプションまたは設定情報ファイルを使用できます。複数のルールを追加する場合は、設定情報ファイルを使用して追加します。

コマンドラインオプションを使用して多数のルールを1つずつ追加すると、CPUの負荷が急増する場合があります。

Web コンソールでのネットワークパケットルールの作成

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. ［**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**］の順に選択します。

5. コンポーネントのトグルスイッチが **ファイアウォールは有効です** の位置にあることを確認します。

6. ［**ネットワークパケットルール**］タブで［**追加**］をクリックします。

   新しいネットワークルールのフォームが開きます（下図を参照）。

7. ［**ルール名**］にルール名を入力します。

   ［**ルールのテンプレートを選択してください**］をクリックして定義済みのルールテンプレートを選択できます。ルールのテンプレートには、最もよく使用されるネットワーク接続の設定が含まれています。

   ネットワークルールのすべての設定（優先順位、およびFirewallが接続に適用する処理を除く）は自動的に入力されます。

8. ［**優先度**］に、ルールの優先順位を指定します。既定では、ルールは最も高い優先順位で作成されます。

9. ［**処理**］で、ルールが適用された場合にFirewallがネットワーク動作を処理する方法（［**許可する**］または［**ブロックする**］）を選択します。

10. ［**通信方向**］で、ルールを適用するネットワーク動作を選択します：

- **受信**ファイアウォールはすべての受信ネットワークパケットにネットワークルールを適用します。
- **受信（パケット）**リモートコンピューターにより開始されたネットワーク接続経由で送信されたパケットに、ネットワークルールが適用されます。
- **受信 / 送信**ネットワーク接続を開始したのがユーザーのコンピューターかリモートコンピューターか関係なく、送受信ネットワークパケットにネットワークルールが適用されます。
- **送信（パケット）**ファイアウォールはすべての送信ネットワークパケットにネットワークルールを適用します。
- **送信**ユーザーのコンピューターにより開始されたネットワーク接続経由で送信されたパケットに、ネットワークルールが適用されます。
- **受信 / 送信（パケット）**ファイアウォールはすべての送受信ネットワークパケットにネットワークルールを適用します。

11. ネットワークルールの処理をレポートに反映する場合は、［**イベントを記録**］をオンにします。ルールの処理に従って、製品は［*ネットワーク動作がブロックされました*］イベントまたは［*ネットワーク動作が許可されました*］イベントを作成します。

12. ［**プロトコルの設定**］タブで、ルールでネットワーク動作をフィルタリングするプロトコルを選択します。

13. ［**リモートネットワークアドレス**］タブに移動します。

14. ［**リモート**］に、ネットワークパケットを送受信できるリモートコンピューターのネットワークアドレスを指定します。Firewallは、指定されたアドレスにルールを適用します。

15. ［**ローカル**］に、Kaspersky Endpoint Security がインストールされ、ネットワークパケットを送受信できるコンピューターのネットワークアドレスを指定します。Firewallは、指定されたアドレスにルールを適用します。

16. 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。

ファイアウォール

コマンドラインでのネットワークパケットルールの作成

1. Firewall 管理が有効になっていることを確認します：

```
kesl-control --get-task-state 12
```

コンポーネントのステータスは **開始済み** である必要があります。

2. コンポーネントが無効になっている場合は、次のコマンドを実行します：

```
kesl-control --start-task 12
```

3. 新しいネットワークパケットルールを追加します：

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

複数のルールを追加する場合は、設定情報ファイルを使用して追加します：

a. コンポーネントの設定を設定情報ファイルに出力します：

```
kesl-control --get-settings 12 --file <path to file> [--json]
```

b. 設定情報ファイルを開き、次のセクションを使用してネットワークパケットルールを追加します：

```
[PacketRules.item_#]
Name=<rule name>
FirewallAction=<Allow|Block>
Protocol=<protocol>
Direction=<direction>
RemoteAddress=<remote address>
LocalAddress=<local address>
LogAttempts=<Yes|No>
```

c. 設定情報ファイルから設定をアプリケーションにインポートします：

```
kesl-control --set-settings 12 --file <path to file> [--json]
```

4. ネットワークパケット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 -F --query
```

本製品は、すべてのネットワークパケットルールの一覧を次の形式で表示します：`<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`。

記号

コマンドオプション

設定	説明
`--name <rule name>` `Name`	ネットワークパケットルールの名前。既定では、`Packet rule #<n>`。
`--action` `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）：接続を許可します。 • `Block`：接続をブロックします。
`--protocol` `Protocol`	監視対象のネットワーク活動のプロトコルの種類。 • `Any`（既定）は、Firewall がすべてのネットワーク活動を制御することを意味します • `TCP` • `UDP` • `ICMP` • `ICMPv6` • `IGMP` • `GRE`
`--direction` `Direction`	監視対象のネットワーク活動の通信方向： • `IncomingOutgoing` または `InOut`（既定）。ファイアウォールはすべての送受信ネットワークパケットにネットワークルールを適用します。 • `Incoming` または `In`。リモートコンピューターにより開始されたネットワーク接続経由で送信されたパケットに、ネットワークルールが適用されます。 • `Outgoing` または `Out`。ユーザーのコンピューターにより開始されたネットワーク接続経由で送信されたパケットに、ネットワークルールが適用されます。 • `IncomingPacket` または `InPacket`。ファイアウォールはすべての受信ネットワークパケットにネットワークルールを適用します。 • `OutgoingPacket` または `OutPacket`。ファイアウォールはすべての送信ネットワークパケットにネットワークルールを適用します。 • `IncomingOutgoingPacket` または `InOutPacket`。ネットワーク接続を開始したのがユーザーのコンピューターかリモートコンピューターか関係なく、送受信ネットワークパケットにネットワークルールが適用されます。

設定	説明
`--remote <remote address[:<port>]>` `RemoteAddress=<remote address>`	リモートデバイスの IP アドレス： • `Any`（既定）では、任意の IP アドレスを持つリモートデバイスが送信または受信するネットワークパケットの監視が有効になります。 • `Trusted` は、信頼済みネットワーク用に設定されたネットワークゾーンです。 • `Local` は、ローカルネットワーク用に設定されたネットワークゾーンです。 • `Public` は、パブリックネットワーク用に設定されたネットワークゾーンです。 • `d.d.d.d` は IPv4 アドレスです。d は 0 から 255 までの 10 進数です。 • `d.d.d.d - d.d.d.d` は IPv4 アドレスの範囲です。 • `d.d.d.d/p` は IPv4 アドレスのサブネットです。 p は 0 から 32 までの数値です。 • `x:x:x:x:x:x:x:x` は IPv6 アドレスです。x は 0 から ffff までの 16 進数です。 • `x:x:x:x:x:x:x:x - x:x:x:x:x:x:x:x` は IPv6 アドレスの範囲です。 • `x:x:x:x:x:x:x:x/p` は IPv6 アドレスのサブネットです。 p は 0 から 128 までの数値です。短縮表記として `::` を使用できます。 リモートポートを指定することもできます： • `Any`（既定）：すべてのリモートポートを監視します • `0 - 65535`
`--local <local address[:<port>]>` `LocalAddress=<local address>`	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： • `Any`（既定）：任意の IP アドレスを持つローカルデバイスが送信または受信するネットワークパケットを監視します。 • `Trusted` は、信頼済みネットワーク用に設定されたネットワークゾーンです。 • `Local` は、ローカルネットワーク用に設定されたネットワークゾーンです。 • `Public` は、パブリックネットワーク用に設定されたネットワークゾーンです。 • `d.d.d.d` は IPv4 アドレスです。d は 0 から 255 までの 10 進数です。 • `d.d.d.d - d.d.d.d` は IPv4 アドレスの範囲です。 • `d.d.d.d/p` は IPv4 アドレスのサブネットです。 p は 0 から 32 までの数値です。 • `x:x:x:x:x:x:x:x` は IPv6 アドレスです。x は 0 から ffff までの 16 進数です。 • `x:x:x:x:x:x:x:x - x:x:x:x:x:x:x:x` は IPv6 アドレスの範囲です。 • `x:x:x:x:x:x:x:x/p` は IPv6 アドレスのサブネットです。 p は 0 から 128 までの数値です。短縮表記として `::` を使用できます。 ローカルポートを指定することもできます： • `Any`（既定）：すべてのローカルポートを監視します • `0 - 65535`
`--at <index>`	ネットワークパケットルールのリストにおける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。
`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。

TCP ポート 23 へのすべての受信接続および確立済み接続をブロックするルールの例

```
kesl-control -F --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、TCP ポート 23 経由の受信接続および確立済み接続をブロックするルールの例

```
kesl-control -F --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の使用例

1. **ローカルネットワーク上の特定のコンピューター1台のみにインターネットアクセスを許可し、その他すべてのコンピューターのアクセスをブロックする**

   TCPプロトコル経由でインターネットへのアクセスが許可されるコンピューター（192.168.2.22）のルール：

```
kesl-control --add-rule --name InternetAccess --action Allow --protocol TCP --local 192.168.2.22
```

   インターネットアクセスをブロックするその他のコンピューターのルール：

```
kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.1.0/24
```

2. **ローカルネットワーク上の特定のコンピューター1台のみのインターネットアクセスをブロックする**

   インターネットアクセスをブロックするコンピューター（192.168.2.23）のルール：

```
kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.23
```

3. **ローカルネットワークから特定のWebサイトへのアクセスをブロックする**

   ローカルネットワーク上のコンピューターによる example.com（91.198.174.192）への HTTP アクセスを拒否するルール：

```
kesl-control --add-rule --name ExampleHTTP --action Block --protocol TCP --remote 91.198.174.192:80
```

   ローカルネットワーク上のコンピューターによる example.com（91.198.174.192）への HTTPS アクセスを拒否するルール：

```
kesl-control --add-rule --name ExampleHTTPS --action Block --protocol TCP --remote 91.198.174.192:443
```

4. **ローカルネットワーク上の特定のコンピューター1台に対して、指定したWebサイト1つのみへのアクセスを許可する**

   example.com（91.198.174.192）への HTTP アクセスが許可されるコンピューター（192.168.2.24）のルール：

```
kesl-control --add-rule --name ExampleHTTP --action Allow --protocol TCP --remote 91.198.174.192:80 --local
192.168.2.24
```

   example.com（91.198.174.192）への HTTPS アクセスが許可されるコンピューター（192.168.2.25）のルール：

```
kesl-control --add-rule --name ExampleHTTPS --action Allow --protocol TCP --remote 91.198.174.192:443 --local
192.168.2.25
```

   インターネットアクセスをブロックするコンピューター（192.168.2.26）のルール：

```
kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.26
```

ネットワークゾーン（パブリック、ローカル、信頼済み）に IP アドレスを追加する方法

Firewall では、*ネットワークゾーン*のネットワークアクティビティを監視できます。ネットワークゾーンは、1 つのネットワーク接続の種類にまとめられた IP アドレスまたはサブネットのグループです。定義済みのネットワークゾーンを使用すると、IP アドレスまたは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 アドレスまたはサブネットに同じルールを再利用できます。

Kaspersky Endpoint Security では、3 つのネットワークゾーンが区別されます：

- **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。

- **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。

Web コンソールでネットワークゾーンに IP アドレスを追加する方法

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. ［**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**］の順に選択します。

5. ［**使用可能なネットワーク**］タブに移動します。

6. ［**追加**］をクリックします。
   新しいネットワーク接続を追加するフォームが開きます。

7. ［**名前**］にネットワーク接続の名前を入力します。

8. ［**ネットワーク種別**］で、ネットワーク接続が属するネットワークゾーン（**パブリックネットワーク**、**プライベートネットワーク**、**信頼するネットワーク**）を選択します。

9. ［**IP アドレス**］に、ネットワーク接続に関連付ける IP アドレスまたはサブネットを指定します。

10. 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。

コマンドラインでネットワークゾーンに IP アドレスを追加する方法

1. Firewall 管理が有効になっていることを確認します：

```
kesl-control --get-task-state 12
```

コンポーネントのステータスは **開始済み** である必要があります。

2. コンポーネントが無効になっている場合は、次のコマンドを実行します：

```
kesl-control --start-task 12
```

3. ネットワークゾーンにアドレスを追加します：

```
kesl-control -F --add-zone <Public|Local|Trusted> --address <IP address>
```

ネットワークパケット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 -F --query
```

記号

コマンドオプション

設定	説明
`--add-zone`	定義済みのネットワークゾーン： • `Public` パブリックネットワーク。 • `Local` プライベートネットワーク。 • `Trusted` 信頼するネットワーク。
`--address`	ネットワークアドレスまたはサブネット。

例

```
kesl-control -F --add-zone Local --address 10.28.0.0/24
```

動的ルールとは

Kaspersky Endpoint Security では、アプリケーションが正しく動作するために必要な Firewall の*動的ルール*を追加または削除できます。例：

- ネットワークエージェントは、Kaspersky Security Center への接続を許可する動的ルールを追加します。
- アンチクリプターコンポーネントは、NFS および SMB ファイル転送 / ストレージプロトコルを介して送信されるトラフィックをインターセプトするための動的ルールを追加します。これにより、アプリケーションが悪意のある暗号化と判断した動作を行うデバイスのネットワークトラフィックを、このコンポーネントがブロックできるようになります。
- 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、アプリケーションコンポーネントがネットワークリソースにアクセスできるようにする動的ルールを自動的に作成します。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。動的ルールのセット内のいずれかのルールが、たとえば iptables ユーティリティを使用して削除された場合、アプリケーションはその動的ルールのセットを復元します。kesl プロセスが Watchdog サーバーによって強制終了された場合、アプリケーションの動作中にアプリケーションによって作成されたルールチェーンへのすべてのリンク（kesl-bypass を除く）は iptables から削除されます。

次のコマンドを使用して、動的ルールのセットを表示できます：

```
kesl-control -F --query
```

本製品は、すべてのネットワークパケットルールの一覧を次の形式で表示します：`<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`。動的ルールは、`kesl_input`、`kesl_output`、`kesl_prerouting`、`kesl_postrouting`、`kesl_forward` の個別のチェーンに分離されます。

動的ルールの設定は管理できません。

例

```
ipv4 mangle kesl_output -p tcp -m tcp --dport 80 -m mark ! --mark 0x400/0x400 -m conntrack --ctdir ORIGINAL -m
addrtype ! --dst-type LOCAL -j MARK --set-xmark 0x100/0x100 tag WebAv
```

Kaspersky Security Center に接続するためのルールを作成する方法

ネットワークエージェントは Kaspersky Security Center との連携に使用されます。ネットワークエージェントと Kaspersky Security Center の間で常時接続を確立するには、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追加する必要があります。この場合、Firewall を正しく設定せず、誤ってすべての接続をブロックしてしまった場合でも、Kaspersky Security Center コンソールでリモートから Firewall を設定できます。

ポートの組み合わせは、コンピューターの役割（ディストリビューションポイントなど）によって異なります。コンピューターで開かれるポートについて詳しくは、Kaspersky Security Center ヘルプを参照してください。

Web コンソールでネットワークエージェントの許可ルールを追加する方法

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. ［**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**］の順に選択します。
5. コンポーネントのトグルスイッチが **ファイアウォールは有効です** の位置にあることを確認します。
6. ［**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**］チェックボックスをオンにします。
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。

コマンドラインでネットワークエージェントの許可ルールを追加する方法

1. Firewall 管理が有効になっていることを確認します：

```
kesl-control --get-task-state 12
```

コンポーネントのステータスは **開始済み** である必要があります。

2. コンポーネントが無効になっている場合は、次のコマンドを実行します：

```
kesl-control --start-task 12
```

3. 次のコマンドを実行します：

```
kesl-control --set-settings 12 OpenNagentPorts=Yes
```

4. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 12
```

セキュリティコントロール

デバイスコントロール

*デバイスコントロール*は、クライアントデバイスに内蔵または接続されているデバイス（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。

デバイスコントロールの仕組み

既定では、デバイスコントロールコンポーネントは既定の設定で有効になっています。

1. **ユーザーがデバイスへのアクセスを試行する**
2. **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）。各デバイス種別には、次の*アクセスモード*のいずれかを適用できます：
     - *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。

- *カスタム*：デバイスアクセスルールに従って、デバイスへのアクセスを許可またはブロックします。
- *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。

- **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。

3 スキャンの完了

ユーザーがアクセスしようとしているデバイスがこのユーザーの信頼するデバイスでない場合、またはアクセスモードに従ってデバイスにアクセスする権限がユーザーにない場合、アプリケーションはこのユーザーによるデバイスへのアクセスをブロックします。

誤ってブロックされたと考えられる場合、ユーザーはその旨を申し立てるリクエストを組織の管理者に送信できます。また、デバイスへの一時的なアクセスをリクエストすることもできます。

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の設定

1 信頼するデバイスの設定

「*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。個々のユーザー、ユーザーグループ、または組織のすべてのユーザーに、信頼するデバイスへのアクセスを許可できます。たとえば、指定した USB デバイスへのアクセスを制限するか、USB ドライブのみに制限できます。他の USB デバイスへのアクセスはできません。

2 アクセスモードの設定

デバイス種別および接続バスに対してアクセスモードを設定できます。既定では、すべてのデバイス種別に対して「*バスに依存*」アクセスモード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。

3 アクセスルールの設定

ストレージデバイス（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、CD/DVD ドライブ）には、*アクセスルール*を設定できます。

4 メッセージテンプレートの設定

必要に応じて、デバイスへのアクセスがブロックされたこと、またはデバイスでの操作が禁止されていることをユーザーに通知するメッセージのテンプレートテキストをカスタマイズできます。

5 デバイスへの一時的なアクセスの設定

必要に応じて、ブロックされたデバイスへの一時的なアクセスをユーザーに許可します。

特別な考慮事項と制限事項

- 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。

- 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。

コマンドラインで信頼するデバイスのリストを管理する方法

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用）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。

信頼するデバイスのリストを表示する

```
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

```
kesl-control --trusted-devices --add <device id or mask>
```

ここで、`<device id or mask>` 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

```
kesl-control --trusted-devices --delete <device id or mask>
```

ここで、`<device id or mask>` 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

```
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 <file>` 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。

デバイスのアクセスモードを設定する方法

デバイスの種別ごとに（デバイスコントロールコンポーネントの分類に従います。たとえば、プリンター、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。

- *カスタム*：デバイスアクセスルールに従って、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。

- *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。

Web コンソールでデバイス種別のアクセスモードを設定する方法

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**］→［**デバイスコントロール**］に移動します。

5. コンポーネントのトグルスイッチが **デバイスコントロールは有効です** の位置にあることを確認します。

6. ［**デバイスアクセスルール**］で、表の［**デバイスと Wi-Fi ネットワーク**］タブを選択します。

7. ［**名前**］列で、アクセスモードを設定するデバイスの種別を選択します。

8. ［**アクセス**］ドロップダウンリストで、次のいずれかのアクセスモードを選択します：

   - **許可** – 選択した種別のデバイスに対するアクセスが許可されます。

   - **ブロック**– 選択した種別のデバイスに対するアクセスがブロックされます。

   - **バスに依存**（既定値）– 接続バスのアクセスモードに応じて、デバイスへのアクセスを許可またはブロックします。

   - **カスタム**：アクセスルールとスケジュールに従って、デバイスへのアクセスを許可またはブロックします。このオプションは、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。このオプションは、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。

9. 下の表で、［**追加**］をクリックします。

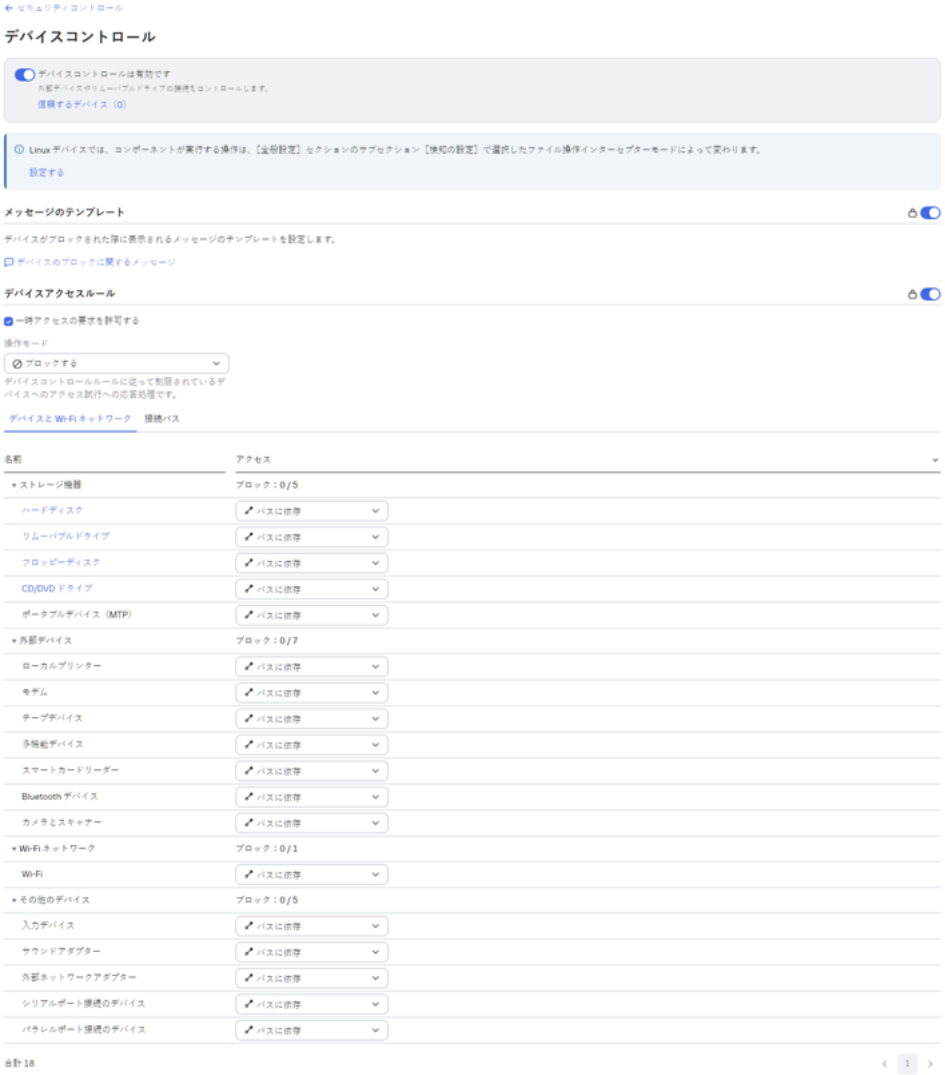
   新しいアクセスルールを追加するウィンドウが開きます。

10. ［**優先度**］フィールドで、アクセスルールの優先度を設定します。

11. 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選択します。既定では、ルールはすべてのユーザーに適用されます。

12. 必要に応じて、アクセススケジュールを設定します。既定では、ルールは常に適用されます。

13. 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。



デバイスコントロール

コマンドラインでデバイス種別のアクセスモードを設定する方法

1. デバイスコントロールコンポーネントが実行されていることを確認します：

```
kesl-control --get-task-list
```

コンポーネントのステータスは **開始済み** である必要があります。

2. コンポーネントが無効になっている場合は、次のコマンドを実行します：

```
kesl-control --start-task 15
```

3. 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が試行された場合の動作モードを選択します：

```
kesl-control --set-settings 15 OperationMode=<Notify|Block>
```

4. 次のいずれかのデバイスタイプについて、アクセスモードを指定します：`HardDrive`、`RemovableDrive`、`FloppyDrive`、`OpticalDrive`、`SerialPortDevice`、`ParallelPortDevice`、`Printer`、`Modem`、`TapeDrive`、`MultifuncDevice`、`SmartCardReader`、`WiFiAdapter`、`NetworkAdapter`、`PortableDevice`、`PortableDevice`、`BluetoothDevice`、`ImagingDevice`、`SoundAdapter`、`InputDevice`

```
kesl-control --set-settings 15 DeviceClass.<device type>=<Allow|Block>
```

5. デバイス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 15
```

Web コンソールで接続バスのアクセスモードを設定する方法

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**］→［**デバイスコントロール**］に移動します。
5. コンポーネントのトグルスイッチが **デバイスコントロールは有効です** の位置にあることを確認します。
6. ［**デバイスアクセスルール**］で、表の［**接続バス**］タブを選択します。
7. ［**名前**］列で、アクセスモードを設定するバスを選択します。
8. ［**アクセス**］ドロップダウンリストで、次のいずれかのアクセスモードを選択します：
   - **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。
9. 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。

コマンドラインで接続バスのアクセスモードを設定する方法

1. デバイスコントロールコンポーネントが実行されていることを確認します：

```
kesl-control --get-task-list
```

   コンポーネントのステータスは **開始済み** である必要があります。

2. コンポーネントが無効になっている場合は、次のコマンドを実行します：

```
kesl-control --start-task 15
```

3. 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が試行された場合の動作モードを選択します：

```
kesl-control --set-settings 15 OperationMode=<Notify|Block>
```

4. 接続バスのアクセスモードを指定します：

```
kesl-control --set-settings 15 DeviceBus.USB=<Allow|Block>
kesl-control --set-settings 15 DeviceBus.FireWire=<Allow|Block>
```

5. デバイス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 15
```

デバイスアクセスルールを設定する方法

ストレージデバイス（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、CD/DVD ドライブ）には、アクセスルールを設定できます。*デバイスアクセスルール*は、クライアントデバイスにインストールされている、または接続されているデバイスにアクセスできるユーザーと、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。

Web コンソールでデバイスアクセスルールを設定する方法

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**］→［**デバイスコントロール**］に移動します。
5. コンポーネントのトグルスイッチが **デバイスコントロールは有効です** の位置にあることを確認します。
6. ［**デバイスアクセスルール**］で、表の［**デバイスと Wi-Fi ネットワーク**］タブを選択します。
7. ［**名前**］列で、アクセスルールを追加するストレージデバイスの種類（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）を選択します。
8. 表示されるウィンドウで、［**デバイスアクセスルール**］の下にある［**カスタム**］を選択します。
9. 下の表で、［**追加**］をクリックします。
   新しいアクセスルールを追加するウィンドウが開きます。
10. ［**優先度**］フィールドで、アクセスルールの優先度を設定します。

11. 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選択します。既定では、ルールはすべてのユーザーに適用されます。

12. 必要に応じて、アクセススケジュールを設定します。既定では、ルールは常に適用されます。

13. 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。

コマンドラインでデバイスアクセスルールを設定する方法

1. デバイスコントロールコンポーネントが実行されていることを確認します：

```
kesl-control --get-task-list
```

コンポーネントのステータスは **開始済み** である必要があります。

2. コンポーネントが無効になっている場合は、次のコマンドを実行します：

```
kesl-control --start-task 15
```

3. デバイス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 15
```

4. 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が試行された場合の動作モードを選択します：

```
kesl-control --set-settings 15 OperationMode=<Notify|Block>
```

5. デバイス種別（`HardDrivePrincipals.item_#.AccessRules.item_#`、`RemovableDrivePrincipals.item_#.AccessRules.item_#`、`FloppyDrivePrincipals.item_#.AccessRules.item_#`、`OpticalDrivePrincipals.item_#.AccessRules.item_#`）のいずれかに新しいアクセスルールを追加します。

- ルールを有効にして、既定のスケジュールを指定します：

```
kesl-control --set-settings 15
<Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.UseRule=Yes
<Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.ScheduleName=Default
```

例

```
kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
```

- ルールがトリガーされたときのデバイスコントロールの処理を設定します：

```
kesl-control --set-settings 15
<Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.Access=Allow|Block
```

例

```
kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
RemovableDrivePrincipals.item_0001.AccessRules.item_0001.Access=Allow
RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
```

- 必要に応じて、ルールを適用するユーザーを指定します：

```
kesl-control --set-settings 15 <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.Principal=<Name>=
<\Everyone|user name|@group name>
```

例

```
kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.Principal=\Everyone
```

- 必要に応じて、ルールのスケジュールを編集します：

```
kesl-control --set-settings 15 Schedules.item_#.ScheduleName=<Name> Schedules.item_#.DaysHours=<All|day of
the week|hour>
```

例

```
kesl-control --set-settings 15 Schedules.item_0001.ScheduleName=Default Schedules.item_0001.DaysHours=All
```

デバイスコントロールメッセージテンプレートを設定する方法

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. 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**］→［**デバイスコントロール**］に移動します。

5. ［**メッセージのテンプレート**］で、［**デバイスのブロックに関するメッセージ**］リンクをクリックします。

   メッセージテンプレートの設定ウィンドウが開きます。

6. ［**ユーザーへのメッセージ**］タブで、デバイスコントロールメッセージテンプレートを設定します。

7. ［**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。

   メッセージテンプレートのテキストを復元するには、［**既定値に戻す**］ボタンをクリックします。

8. ［OK］をクリックします。

9. ［**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する方法

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。

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 コンソールまたは管理コンソールのポリシーのプロパティ、またはデバイスコントロールタスクの設定で、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 コンソールでブロックされたデバイス向けのアクセスキーを作成する方法

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）**］→［**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。

コマンドラインで一時アクセスを要求して取得する方法

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：

ブロックされたデバイスへの一時アクセスを要求する

```
kesl-control --request-temporary-device-access --device-id <device identifier>  --access-duration <access
duration> --path <path to the access request file>
```

説明：

`--device-id <device identifier>` は、アクセスする対象のブロックされたデバイスの ID です。

`--access-duration <access duration>` は、デバイスへのアクセスを取得する期間（時間単位）です。可能な値：1 ～ 100

`--path <path to the access request file>` 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です。

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受け取ったら、デバイスへの一時アクセスを取得するためにアクセスキーを入力する必要があります。

ブロックされたデバイスのアクセスキーをアップロードする

```
kesl-control --upload-temporary-device-access-key --path <path to the file with the access key>
```

説明：

`--path <path to the file with the access key>` は、デバイス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。

グラフィカルインターフェイスで一時アクセスを要求して取得する方法

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. アプリケーションの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. アプリケーションの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。

ウェブコントロール

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。

ウェブコントロールでは、コンテンツカテゴリやデータタイプに基づいて Web リソースへのアクセスを制限したり、個別の Web サイトへのアクセスをブロックしたりできます。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。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。

ウェブコントロールの仕組み

1. **アプリケーションによる Web リソースへのリクエストのチェック**

   ウェブコントロールは、次の技術を使用して Web サイトのコンテンツカテゴリとデータタイプを判定します：

   - 定義データベース。
   - Kaspersky Security Network のクラウドサービス。
   - ヒューリスティック分析技術により、カスペルスキーの定義データベースではまだ対応していない脅威を検知できます。

2. **アプリケーションによるルールの適用**

   アプリケーションは、ウェブコントロールルールを優先順位に従って適用します。優先順位の数値が小さいほど、そのルールの優先順位は高くなります。Web サイトに複数のルールが適用できる場合、ウェブコントロールは最も優先順位の高いルールを適用します。

   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。ソーシャルネットワークカテゴリのサイトへのアクセスは制限しつつ企業ポータルへのアクセスを可能にするには、「*SNS*」カテゴリ用のブロックルールと企業ポータル用の許可ルールの計 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。

3. **スキャンの完了**

   ルールによって Web リソースへのアクセスがブロックされた場合、アプリケーションはブラウザーにブロックメッセージを表示します。リソースは使用できなくなります。

   ユーザーは、Web ページが誤ってブロックされたと思われる場合、誤ったブロックについて組織の管理者にリクエストを送信できます。

ウェブコントロールの設定

1. **ウェブコントロールルールの設定**

   ウェブコントロールは、*アクセスルール*を使用して、ユーザーによる Web サイトへのアクセスを管理します。これらのルールを使用すると、個別のユーザーに対して Web サイトへのアクセスを制限したり、アクセススケジュールを設定したりできます。

   たとえば、IT 部門を除く組織内のすべてのユーザーに対して、*インターネットコミュニケーション*カテゴリの Web サイトへのアクセスを制限できます。

2. **メッセージテンプレートの設定**

   アクセスルールの処理に応じて、ウェブコントロールは、望ましくない Web サイトへのアクセスに関するメッセージまたはブロックメッセージをユーザーに表示します。Web サイトがブロックされた場合、ユーザーは、誤ったブロックについてローカルネットワークの管理者にメッセージを送信できます。

   このようなメッセージには、テンプレートが用意されています。

   > テンプレートはコマンドラインでは編集できません。

3. **ウェブコントロールを有効にする**

   既定では、ウェブコントロールは無効になっています。トグルスイッチを使用して Web コンソールまたは管理コンソールでコンポーネントを有効にするか、コマンドラインで次のコマンドを使用して有効にします：

   ```
   kesl-control --start-task 26
   ```

特別な考慮事項と制限事項

- 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。
- Kaspersky Endpoint Security は、HTTP および HTTPS トラフィックのみを監視します。
- ウェブ脅威対策とウェブコントロールが同時に実行されている場合、ウェブ脅威対策の設定が Web リソースに適用されます。これは、ウェブコントロールルールでアクセスが許可されている場合でも、悪意のある Web サイトやフィッシング Web サイトはブロックされることを意味します。

Web リソースへのアクセスルールを作成する方法

*Web リソースアクセスルール*は、一連のフィルターと、Web リソースにユーザーがアクセスした時に、Kaspersky Endpoint Security によって適用される一連の処理で構成されています。アクセスルールには、ルールのスケジュールを含めることができます。

ルールでは、次のフィルターによって Web リソースへのアクセスを制限します：

- **コンテンツカテゴリ** ウェブコントロールでは、Web リソースがコンテンツ別およびデータ種別で分類されます。これにより、特定のコンテンツカテゴリ（例：*決済システム*）および / または特定のデータ種別（例：*実行ファイル*）に該当する Web サイトへのユーザーのアクセスを制限できます。

- **個別の Web サイト** ウェブコントロールでは、Web リソースの個別の URL または URL のグループへのユーザーのアクセスを制限できます。

  URL のドメインでは、大文字と小文字は区別されません。ルールに `examPLE.com` のような URL が含まれる場合、ウェブコントロールは `example.com` へのアクセスを制限します。

  アクセスルールでコンテンツカテゴリによるフィルターと個別の Web サイトによるフィルターが同時に設定されている場合、ウェブコントロールは、指定されたコンテンツカテゴリのすべての Web サイトへのアクセスを制限するのではなく、指定された URL へのアクセスのみを制限します。

- **ユーザー名とユーザーグループ名で絞り込む**。ウェブコントロールでは、個別のユーザーまたはユーザーグループに対して Web リソースへのアクセスを制限できます。たとえば、IT 部門を除く組織内のすべてのユーザーに対して、ソーシャルメディアの Web サイトへのアクセスを制限できます。

- **ルールのスケジュール**：ルールスケジュールは、ルールで指定された Web リソースへのアクセスを本製品が制御する時間を決定します。たとえば、勤務時間中にのみ、不要な Web サイトへのアクセスを制限できます。

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 コンソールでのアクセスルールの作成

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**］→［**ウェブコントロール**］に移動します。

5. コンポーネントのトグルスイッチが **ウェブコントロールは有効です** の位置にあることを確認します。

6. ［**ルールリスト**］で、ウェブコントロールの既定の処理を選択します：

   - **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**

7. ［**追加**］をクリックします。

   新しいアクセスルールを追加するためのフォームが開きます。

8. ［**ルール名**］にルール名を入力します。ルール名は一意である必要があります。

9. ［**優先度**］フィールドで、アクセスルールの優先度を設定します。

10. ルールがトリガーされたときにウェブコントロールが Web リソースに適用する処理を選択します：

- **許可する**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。
- **ブロックする**ウェブコントロールは、ユーザーの Web リソースへのアクセスをブロックし、アクセスがブロックされていることを示すメッセージを表示します。ブロックメッセージ内のリンクをクリックすると、ユーザーはローカルネットワーク管理者にメッセージを送信して、ブロックの誤りを報告できます。
- **通知する**ウェブコントロールは、不要な Web リソースへのアクセスに関する警告を表示します。ユーザーが警告が誤りであると考える場合、警告内のリンクを使用して、Web ページに移動するか、組織のローカルネットワーク管理者にリクエストを送信できます。

11. アクセスルールのフィルターを選択します：

- **コンテンツカテゴリ**アクセスルールで制御するコンテンツカテゴリを指定します。複数のカテゴリを選択できます。
- **個別の Web サイト**Web サイトの URL または Web サイトのグループを指定します。

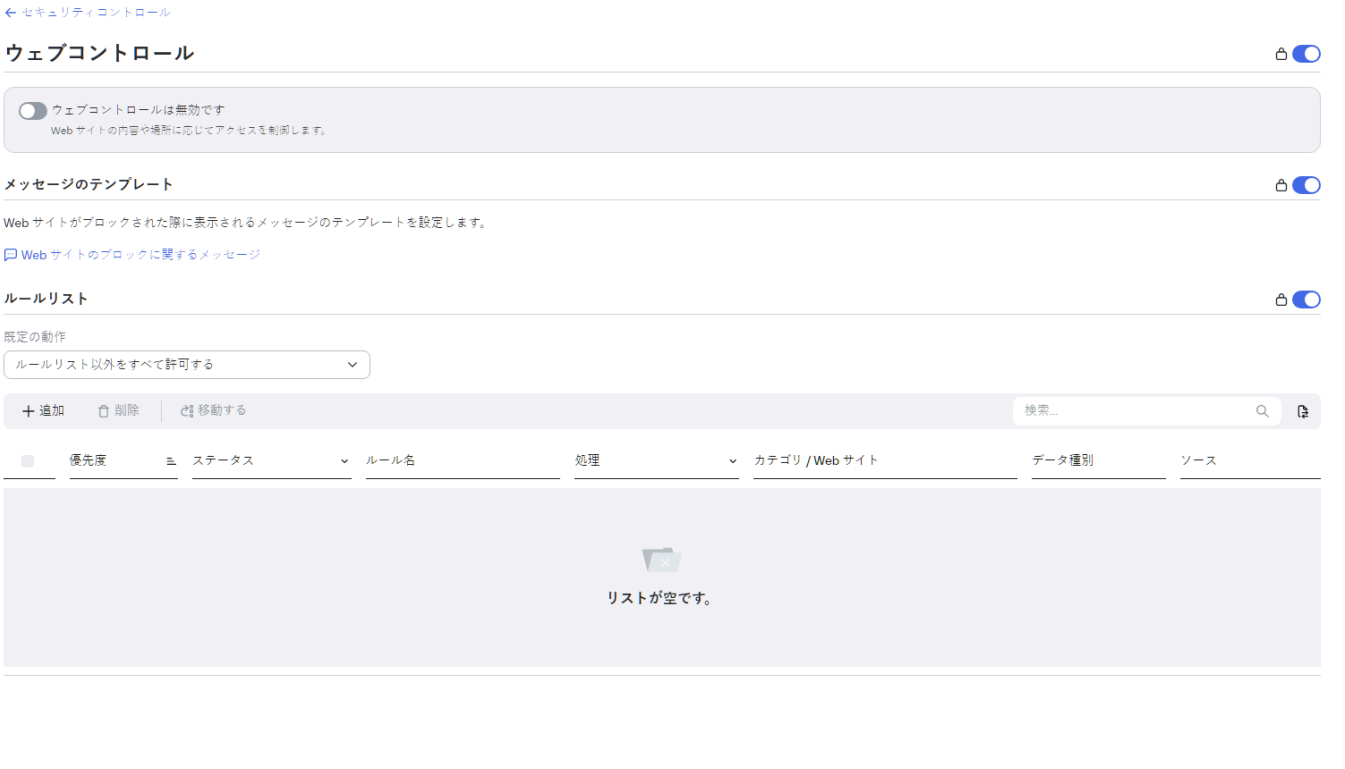
> Web コンソールでは、コンテンツカテゴリによるフィルターと個別の Web サイトによるフィルターを同時に設定することはできません。

12. 必要に応じて、製品によってフィルタリングするデータ種別を指定します。

13. 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選択します。既定では、ルールはすべてのユーザーに適用されます。

14. 必要に応じて、アクセススケジュールを設定します。既定では、ルールは常に適用されます。

15. 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クセスルールを作成する方法

1. ウェブコントロールコンポーネントが有効になっていることを確認します：

```
kesl-control --get-settings 26
```

コンポーネントのステータスは **開始済み** である必要があります。

2. コンポーネントが無効になっている場合は、次のコマンドを実行します：

```
kesl-control --start-task 26
```

3. 既定のウェブコントロール処理を選択します：

```
kesl-control --set-settings 26 WebControlDefaultAction=<Allow|Block>
```

4. ID `#` の新しいアクセスルールを追加します：

   a. ルールを有効にします：

   ```
   kesl-control --set-settings 26 Rules.item_#.Enabled=Yes
   ```

   b. ルール名を入力します：

   ```
   kesl-control --set-settings 26 Rules.item_#.Name=<rule name>
   ```

   c. ルールがトリガーされたときにウェブコントロールが Web リソースに適用する処理を指定します：

   ```
   kesl-control --set-settings 26 Rules.item_#.WebControlAction=<Allow|Block|Notify>
   ```

   d. コンテンツカテゴリで Web リソースをフィルタリングする必要がある場合：

   ```
   kesl-control --set-settings 26 Rules.item_#.UseCategories=<ContentOnly|FormatOnly|ContentAndFormat>
   kesl-control --set-settings 26 Rules.item_#.ContentCategories.item_#.ContentCategory=<category>
   [Rules.item_#.FormatCategories.item_#.FormatCategory=<format>]
   ```

   e. 個々の Web リソースをフィルタリングする必要がある場合：

   ```
   kesl-control --set-settings 26 Rules.item_#.UseUrls=Yes
   kesl-control --set-settings 26 Rules.item_#.Urls.item_#=<web address>
   ```

   f. 必要に応じて、ルールを適用するユーザーを指定します：

   ```
   kesl-control --set-settings 26 Rules.item_#.UsePrincipals=Yes
   kesl-control --set-settings 26 Rules.item_#.Principals.item_#.Name=<user name|@group name>
   ```

g. 必要に応じて、ルールのスケジュールを指定します：

```
kesl-control --set-settings 26 Rules.item_#.Schedules.item_#.Id=<ID> Rules.item_#.Schedules.item_#.Name=
<schedule name> Rules.item_#.Schedules.item_#.DaysHours=<day of the week|hour>
```

5. ウェブコントロール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 --get-settings 26
```

記号

コマンドオプション

設定	説明
WebControlDefaultAction	どのアクセスルールにも指定されていない Web リソースにウェブコントロールが適用する処理。
Enabled=Yes	ID # のアクセスルールを有効にします。
Name	ルールの名前。ルール名は一意である必要があります。
WebControlAction	ルールがトリガーされたときに、ウェブコントロールが Web リソースに適用する処理： 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 – 望ましくない Web リソースへのアクセスに関する警告を表示します。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。
UseCategories	ルールでの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。
ContentCategories.item_#.ContentCategory	コンテンツカテゴリ。
FormatCategories.item_#.FormatCategory	データ種別カテゴリ： Video – 動画ファイル Audio – 音声ファイル 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
UseUrls=Yes	フィルタールールでの個別の Web サイトの使用。
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。
UsePrincipals=Yes	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。
Principals.item_#.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： <user name> は、ルールを適用するユーザーの名前です。 @<group name> は、ルールを適用するユーザーグループの名前です。
Schedules.item_#.Id	スケジュール ID。
Schedules.item_#.Name	スケジュールの名前を指定します。

設定	説明
`Schedules.item_#.DaysHours`	スケジュールの時間間隔を指定します： `<day of week>` 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。 `<hour>` – 時間 [0:24]。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のメッセージテンプレートを変更する方法

アクセスルール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、ウェブコントロールはユーザーに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。**望ましくないリソースにアクセスしようとしたときにユーザーに表示されるメッセージ。ルールに対して**通知する**処理が選択されている場合、本製品はこのメッセージを表示します。

  ユーザーが警告が誤りであると考える場合、警告内のリンクを使用して、Web ページに移動するか、組織のローカルネットワーク管理者にリクエストを送信できます。

- **ブロックされた Web リソースに関するメッセージ** 望ましくない Web リソースがブロックされたときにユーザーに表示されるメッセージ。ルールに対して**ブロックする**処理が選択されている場合、本製品はこのメッセージを表示します。

  ユーザーが Web リソースが誤ってブロックされたと考える場合、Web リソースのブロックメッセージ内のリンクを使用して、組織のローカルネットワーク管理者にリクエストを送信できます。

警告メッセージ、Web リソースのブロックに関するメッセージ、および組織のローカルネットワーク管理者へのリクエスト用のテンプレートが用意されています。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。Kaspersky Endpoint Security は、メッセージを生成する際に、オペレーティングシステムの設定から変数の値を取得し、特定のコンピューター、ユーザー、およびイベントに一致するメッセージに挿入します。

テンプレートはコマンドラインでは編集できません。

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、［**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**］→［**ウェブコントロール**］に移動します。

5. ［**メッセージのテンプレート**］で、［**Web サイトのブロックに関するメッセージ**］リンクをクリックします。

   メッセージテンプレートのウィンドウが開きます。

6. ウェブコントロールのメッセージのテンプレートを設定します。

- **警告**望ましくないリソースにアクセスしようとしたときにユーザーに表示される警告のテンプレート。
- **ブロックに関するメッセージ**望ましくない Web ページまたは Web サイトがブロックされたときに表示されるメッセージのテンプレート。
- **管理者へのメッセージ**管理者へのメッセージのテンプレート。Web ページが誤ってブロックされたとユーザーが考える場合に使用します。ユーザーがアクセスをリクエストすると、本製品は *Web ページへのアクセスブロックに関するメッセージが管理者に送信されました* イベントを Kaspersky Security Center 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。

メッセージテンプレートのテキストを復元するには、［**既定のテキストにリセット**］ボタンをクリックします。

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。

管理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. 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、**プロパティ: <ポリシー名>**ウィンドウを開きます。

   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。

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
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。

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は、ユーザーデバイスでのサードパーティ製アプリケーションの起動を管理します。これにより、保護対象デバイスがマルウェアに感染するリスクを低減できます。

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。

アプリケーションコントロールの仕組み

1. **ユーザーがサードパーティ製アプリケーションを実行しようとする**

2. **アプリケーションコントロールがルールを適用する**

   アプリケーションコントロールは、起動されるアプリケーションにルールを順次適用します。選択したルールモードに応じて、このコンポーネントは起動されるアプリケーションを*制御*するか、ルールを*テスト*します。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。

3. **スキャンの完了**

   ルールによりアプリケーションの実行が阻止される場合、このコンポーネントはアプリケーションの起動をブロックし、*アプリケーションの起動が禁止されました*イベントを生成します。テストモードでは、このコンポーネントはアプリケーションの起動をブロックせず、*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*イベントを生成します。

アプリケーションコントロールの設定

1. **アプリケーションのインベントリを作成する**

   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のリストを取得します。この情報に基づいて、実行を阻止するアプリケーションのリストを作成します。

2. **アプリケーションコントロールの動作モードを選択する**

   アプリケーションコントロールコンポーネントは、2 つのモードのいずかれかで動作できます：

   - *ルールリスト以外をすべて許可する*アプリケーションコントロールを使用すると、ルールで禁止されているものを除き、ユーザーは任意のサードパーティ製アプリケーションを実行できます。

   - *ルールリスト以外をすべて禁止する*アプリケーションコントロールを使用すると、ルールで許可されており禁止されていないものを除き、ユーザーは任意のサードパーティ製アプリケーションを実行できます。

   アプリケーションコントロールの動作モードの選択は、組織のセキュリティポリシーと、制御するアプリケーションの数によって異なります。

3. **アプリケーションカテゴリの作成**

許可または禁止するアプリケーションのカテゴリを定義します。アプリケーションカテゴリは、管理グループに関係なく、企業ネットワーク内のすべてのデバイスを対象としています。アプリケーションカテゴリを使用すると、包含条件や除外条件に基づくのではなく、アプリケーションのグループに対してルールを設定できます。

会社で使用されている標準セットのアプリケーションを網羅する「作業アプリケーション」カテゴリを作成すると有用です。さまざまなユーザーグループが仕事で異なるアプリケーションセットを使用している場合は、ユーザーグループごとに別個のアプリケーションカテゴリを作成できます。

Kaspersky Security Center でアプリケーションカテゴリを設定することを推奨します。

4. **アプリケーションコントロールルールの設定**

このコンポーネントは、*アプリケーションコントロールルール*に基づいてアプリケーションの起動を制御します。このルールでは、選択したユーザーグループに対してサードパーティ製アプリケーションの起動を許可または拒否する際の条件を定義します。

5. **アプリケーションコントロールルールをテストする**

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テストモードで有効にし、作成したアプリケーションコントロールルールをテストすることを推奨します。本製品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しませんが、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。

6. **アプリケーションコントロールルールの仕組みを確認する**

テストモードでのアプリケーションコントロールの動作に関するレポートを確認します。情報を確認した後、必要に応じてアプリケーションコントロールルールを調整します。

7. **アプリケーションコントロールルールの使用を有効にする**

このモードでは、ルールでこれらのアプリケーションの実行が許可されていない場合、Kaspersky Endpoint Security はサードパーティ製アプリケーションの実行を防止します。

Web コンソールでアプリケーションコントロールルールの使用を有効にする方法

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 **ルールを適用** 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ルールの使用を有効にする方法

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=ApplyRules
```

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。

特別な考慮事項と制限事項

- 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。
- ルールでインタープリターの実行が許可されている場合、アプリケーションコントロールはそのインタープリターから起動されたスクリプトをブロックしません。インタープリターのコマンドラインで指定されたスクリプトのうち少なくとも 1 つの起動がルールによって禁止されている場合、Kaspersky Endpoint Security は、インタープリターのコマンドラインで指定されたすべてのスクリプトをブロックします。除外：cat script.py | Python

アプリケーションインベントリ

最適なアプリケーションコントロールルールを作成するには、まず、企業 LAN 上の保護対象デバイスで使用されているアプリケーションを把握することを推奨します。インベントリタスクを使用すると、次の情報を取得できます：

- サードパーティ製アプリケーションの名前とバージョン
- 簡単な説明

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。

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。上限に達すると、新しいファイルは処理されません。インベントリを再開するには、前回のインベントリ中に Kaspersky Security Center データベースに追加されたファイルを保護対象デバイスから削除する必要があります。

インベントリタスクの設定と実行

1. **インベントリタスクを作成する**

   Web コンソールでのインベントリタスクの作成

   1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
      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**］から［**Kaspersky Endpoint Security for Linux 12.5**］を選択します。

   b. ［**タスク種別**］から［**インベントリ**］を選択します。

   c. **タスク名** フィールドにタスク名を入力します。

   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

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。

5. ウィザードを終了します。

コマンドラインでのインベントリタスクの作成

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 <task name> --type InventoryScan
```

ここで、`<task name>` は新しいタスクの名前です。

このコマンドは、作成されたタスクの ID を返します。

コマンド実行結果の例：

タスクが作成されました（タスク ID：100）

2 インベントリ範囲を設定する

タスクを開始するには、少なくとも 1 つのインベントリ範囲を指定する必要があります。既定では、*実行可能なコマンド* – `/usr/bin` の範囲が設定されています。

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。

Web コンソールでのインベントリ範囲の設定

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
   タスクのリストが表示されます。

2. 作成したインベントリ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。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**インベントリ範囲**］に移動します。

5. ［**追加**］をクリックします。
   インベントリ範囲を追加するウィンドウが開きます。

6. **範囲名** フィールドに、インベントリ範囲の名前（例：*デスクトップ上のファイル*）を入力します。

7. **パス** フィールドで、個々のファイルまたはディレクトリへのパス（例：`/path/to/folder`）を指定します。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。

8. 必要に応じて、コマンドシェル形式でオブジェクト名のマスクを指定します（例：`*.txt`、`file?.*`）。マスクは一度に1つずつ追加します。

9. 変更内容を保存します。

コマンドラインでのインベントリ範囲の設定

1. 次のコマンドを実行します：

```
kesl-control --set-settings <task name | task ID> ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. 現在の設定を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings <task name | task ID>
```

記号

インベントリタスクの設定

設定	説明
`UseScanArea=Yes`	ID が `#` のインベントリ範囲を有効にします。 範囲を削除する代わりに、インベントリ範囲のスキャンを一時的に無効にできます。これを行うには、`ScanScope.item_#.UseScanArea=No` を設定します。
`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。
`AreaMask.item_#`	インベントリスキャン範囲の制限。インベントリ範囲で、シェル形式のマスクを使用して指定したオブジェクトのみをスキャンします。 複数の `ScanScope.item_#.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。 例：「`ScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`」。
`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。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。 既定値：`/usr/bin`

3. **必要に応じて、タスク設定を編集します**

Web コンソールでインベントリタスクを設定するには

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
   タスクのリストが表示されます。

2. 作成したインベントリ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。

3. ［**アプリケーション設定**］タブを選択します。

4. ［**インベントリ設定**］に移動します。

5. アプリケーションの「ゴールデンイメージ」カテゴリに対する処理を選択します：

- **変更なし** – インベントリの完了後、「ゴールデンイメージ」カテゴリを変更しません。これは既定で選択されています。このオプションは、デバイスで使用されているサードパーティ製アプリケーションのリストを取得するが、それらのアプリケーションを「ゴールデンイメージ」カテゴリに追加しない場合に使用します。

- **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によってデバイス上で検知されたアプリケーションを「ゴールデンイメージ」カテゴリに追加します。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。

- **削除** – 「ゴールデンイメージ」アプリケーションカテゴリをクリアします。タスクが開始されるとすぐにカテゴリがクリアされ、デバイス上のファイルのインベントリは実行されません。

6. 必要に応じて、次のチェックボックスをオンにします：

- **スクリプトファイルのインベントリ**インベントリ範囲内のスクリプトをチェックします。アプリケーションはこの情報を Kaspersky Security Center に送信します。

- **実行ファイルをすべてスキャン**

- **バイナリをスキャン**バイナリファイル（拡張子が .elf、.java、および .pyc のファイル）をスキャンします。

7. 変更内容を保存します。

コマンドラインでインベントリタスクを設定するには

次のコマンドを実行します：

```
kesl-control --set-settings <task name | task ID> ScanScripts=<Yes|No> ScanBinaries=<Yes|No>
ScanAllExecutable=<Yes|No> GoldenImageAction=<DoNothing|Create|Remove>
```

記号

インベントリタスクの設定

設定	説明
ScanScripts	インベントリ領域内のスクリプトのチェック： 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（拡張子が .elf、.java、および .pyc のファイル）のスキャン： 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	実行ファイルのスキャン： 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。
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に対して実行する処理： DoNothing（既定） –「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 –「ゴールデンイメージ」アプリケーションカテゴリをクリアします。タスクが開始されるとすぐにカテゴリがクリアされ、デバイス上のファイルのインベントリは実行されません。

4 監視の除外範囲を設定する

除外はインベントリ範囲よりも優先度が高くなります。除外されたオブジェクトは、インベントリ範囲内にある場合でもスキャンされません。インベントリ範囲が除外されたディレクトリよりも下位のレベルで定義されている場合、タスクの実行時に本製品はこのインベントリ範囲をスキップします。

Web コンソールで除外範囲を設定するには

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
2. タスクのリストが表示されます。
3. 作成したインベントリ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。
4. ［**アプリケーション設定**］タブを選択します。
5. ［**除外範囲**］に移動します。
6. ［**追加**］をクリックします。
   除外範囲を追加するためのウィンドウが開きます。
7. **範囲名** フィールドで、除外範囲の名前（例：*システムファイル*）を指定します。
8. **パス** フィールドで、個々のファイルまたはディレクトリへのパス（例：`/path/to/folder`）を指定します。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。
9. コマンドシェル形式でオブジェクト名のマスク（例：`*.txt` または `file?.*`）を指定します。マスクは一度に 1 つずつ追加します。
10. 変更内容を保存します。

コマンドラインで除外範囲を設定する方法

1. 次のコマンドを実行します：

```
kesl-control --set-settings <task name | task ID>       ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. 現在の設定を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings <task name | task ID>
```

記号

インベントリタスクの設定

設定	説明
`UseScanArea`	指定された範囲のインベントリを除外します。 除外範囲を削除する代わりに、一時的に無効にすることができます。これを行うには、`ExcludedFromScanScope.item_#.UseScanArea=No` を設定します。
`AreaDesc`	インベントリの除外範囲の説明。

設定	説明
AreaMask.item_#	除外範囲の制限。除外範囲では、本製品は、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スキャンから除外します。 複数の ExcludedFromScanScope.item_#.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。 例：「ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt」。
Path	インベントリから除外するディレクトリへのパス。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。

/tmp ディレクトリをインベントリから除外する例：

```
kesl-control --set-settings 100 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

5 **タスクの実行**

Web コンソールでインベントリタスクを実行する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
   タスクのリストが表示されます。
2. 作成したタスクの横にあるチェックボックスをオンにします。
3. ［**開始**］をクリックします。

コマンドラインでインベントリタスクを実行する方法

タスクを実行するには、次のコマンドを実行します：

```
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。

検知されたアプリケーションのリストの表示

Web コンソールで、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：

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
   タスクのリストが表示されます。

2. 作成したインベントリ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。

3. ［**履歴**］タブを選択します。

クライアントデバイスで検出されたアプリケーションの一覧を表示します

```
kesl-control --get-app-list [--json]
```

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
- 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：
  - アプリケーションへのパス。
  - アプリケーションのハッシュ値。
  - アプリケーションタイプ。例えば、`Script`、`Executable`。
  - 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を表示するには、次のコマンドを使用します：

    ```
    kesl-control --get-categories
    ```

> 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。アプリケーションのリストをアップデートするには、インベントリタスクを再度実行する必要があります。

アプリケーションコントロールの動作モードを設定する方法

アプリケーションコントロールコンポーネントは、2 つのモードのいずかれかで動作できます：

- *ルールリスト以外をすべて許可する*アプリケーションコントロールを使用すると、ルールで禁止されているものを除き、ユーザーは任意のサードパーティ製アプリケーションを実行できます。
- *ルールリスト以外をすべて禁止する*アプリケーションコントロールを使用すると、ルールで許可されており禁止されていないものを除き、ユーザーは任意のサードパーティ製アプリケーションを実行できます。

アプリケーションコントロールの動作モードの選択は、組織のセキュリティポリシーと、制御するアプリケーションの数によって異なります。

Web コンソールでアプリケーションコントロールの動作モードを設定する方法

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。

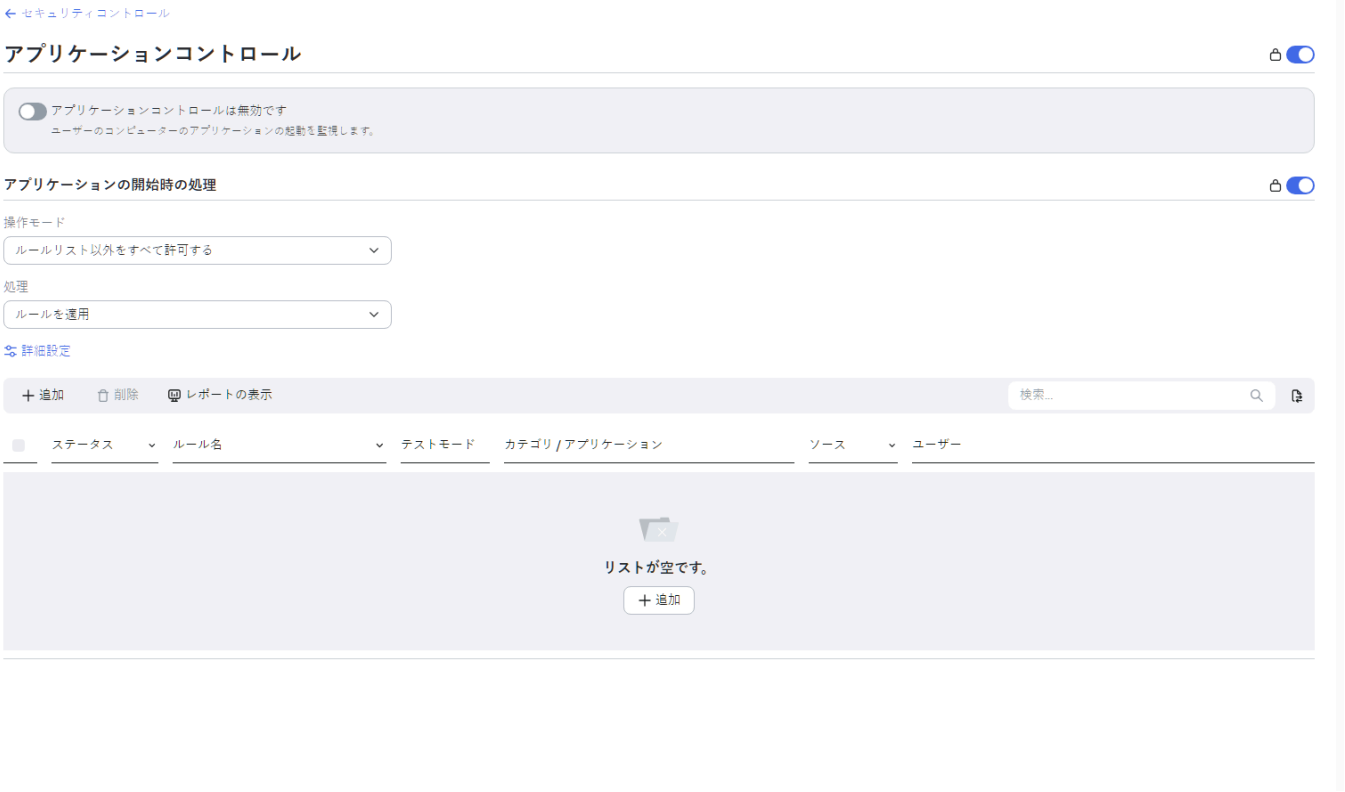
4. ［**セキュリティコントロール**］→［**アプリ管理**］に移動します。

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の動作モードを選択します：

   - **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**

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。



アプリケーションコントロール

コマンドラインでアプリケーションコントロールの動作モードを設定する方法

次のコマンドを実行します：

```
kesl-control --set-settings 21 AppControlMode=<AllowList|DenyList>
```

記号

コマンドオプション

設定	説明
AppControlMode	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。

アプリケーションカテゴリの作成

アプリケーションコントロールルールの作成を容易にするため、*アプリケーションカテゴリ*を作成できます。

Kaspersky Endpoint Security は、次の技術を使用してアプリケーションのカテゴリを判定します：

- 定義データベース。
- Kaspersky Security Network のクラウドサービス。
- ヒューリスティック分析技術により、カスペルスキーの定義データベースではまだ対応していない脅威を検知できます。

Kaspersky Endpoint Security for Linux では、次のパラメータに基づいてカテゴリを作成できます：

- 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。

  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。

  マスクの指定ルール

  * 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。

会社で使用されている標準セットのアプリケーションを網羅する「作業アプリケーション」カテゴリを作成すると有用です。さまざまなユーザーグループが仕事で異なるアプリケーションセットを使用している場合は、ユーザーグループごとに別個のアプリケーションカテゴリを作成できます。

Kaspersky Endpoint Security for Linux は KL カテゴリをサポートしていません。

Kaspersky Security Center でアプリケーションカテゴリを作成するには：

1. Web コンソールのメインウィンドウで、［**資産管理**］→［**サードパーティ製品**］→［**アプリケーションカテゴリ**］をクリックします。
2. ［**追加**］をクリックします。

   ユーザーカテゴリの作成ウィザードが表示されます。
3. ユーザーカテゴリの作成ウィザードの指示に従います。

ステップ 1：

このステップでは、アプリケーションカテゴリの名前を指定し、次のいずれかのアプリケーションカテゴリの種別を選択します。

- *手動でコンテンツを追加するカテゴリ：実行ファイルのデータを手動でカテゴリに追加します*このカテゴリ種別を選択した場合、「*条件*」と「*除外リスト*」ステップで、実行ファイルをカテゴリに追加する条件を定義できます。

- *特定のフォルダーの実行ファイルを含むカテゴリ：指定されたフォルダーにコピーされたアプリケーションの実行ファイルが自動的に処理され、メトリックがカテゴリに追加されます*このカテゴリ種別を選択した場合、次のステップで、カテゴリに自動的に追加する実行ファイルが格納されているフォルダーを指定できます。

- *選択したデバイスの実行ファイルを含むカテゴリ：デバイスの実行ファイルが自動的に処理され、メトリックがカテゴリに追加されます*このカテゴリ種別を選択した場合、次のステップで、カテゴリに自動で追加する実行ファイルのコンピューターを指定できます。

ステップ 2：

このステップは、カテゴリ種別［**手動でコンテンツを追加するカテゴリ：実行ファイルのデータを手動でカテゴリに追加します**］を選択した場合に利用できます。

このステップでは、カテゴリにアプリケーションを含める基準を選択します。

- **KL カテゴリから選択**

  このオプションをオンにすると、カスタムカテゴリにアプリケーションを追加するための条件として、カスペルスキー製品のカテゴリを指定できます。*KL カテゴリ*とは、テーマ属性が共有されているアプリケーションのリストです。このリストは、カスペルスキーのスペシャリストによって管理されています。たとえば、「Office アプリケーション」KL カテゴリには、Microsoft Office スイートのアプリケーション、Adobe Acrobat などが含まれます。

  すべての KL カテゴリを選択することで、広範な信頼するアプリケーションのリストを生成できます。

- **リポジトリから証明書を選択**

  このオプションをオンにすると、ストアから証明書を指定できます。カテゴリの条件は、指定された証明書で署名された実行ファイルのみに一致します。

  ルールを適用する条件として証明書を選択した場合、その証明書がコンピューター上の信頼するシステムの保管領域に追加されていることを確認し、本製品で信頼するシステム保管領域の使用設定を確認してください。

- **アプリケーションのパスを指定（マスクをサポート）**

  このオプションをオンにすると、クライアントデバイス上のファイルまたはフォルダーを指定して、そこから実行ファイルをカスタムアプリケーションカテゴリに追加できます。`C:\path_to_exe\*` のような正規表現を使用できます。例：`C:\Program Files\Internet Explorer\*`

- **リムーバブルドライブ**

  このオプションをオンにすると、アプリケーションを起動するメディアの種類（任意またはリムーバブルドライブ）を指定できます。選択した種別のメディアから起動されたアプリケーションがカスタムアプリケーションカテゴリに追加されます。

- **ハッシュ、メタデータ、証明書のいずれか**：

  - **実行ファイルのリストから選択する**

    このオプションをオンにすると、クライアントデバイス上の実行ファイルのリストからカテゴリに追加するアプリケーションを選択できます。

  - **アプリケーションのレジストリから選択する**

    このオプションをオンにすると、アプリケーションのレジストリが表示されます。レジストリからアプリケーションを選択すると、選択したアプリケーションのメタデータが事前に入力された設定を含むウィンドウが開きます。

    - ファイル名
    - ファイルバージョン 正確なバージョンを指定するか、条件（例：「5.0 より大きい」）を入力できます。
    - 製品名。
    - 本ソフトウェアのバージョン。正確なバージョンを指定することも、条件（例：「5.0 より大きい」など）を入力することもできます。
    - 製造元。

    指定されたパラメータに一致する実行ファイルのみがブロックされ、選択したアプリケーションの起動自体はブロックされないことにご注意ください。選択したメタデータが、アプリケーションの起動時に開始される実行ファイルのメタデータと一致する場合は、次のステップに進めます。それ以外の場合は、実行可能ファイルのメタデータと一致するように値を手動で編集する必要があります。

  - **手動設定**

    このオプションをオンにすると、カスタムカテゴリにアプリケーションを追加するための条件として、ファイルハッシュ、メタデータ、または証明書を指定する必要があります。

    ファイルのハッシュ

    ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、Kaspersky Endpoint Security がカテゴリ内のファイルに適用するハッシュアルゴリズムを選択する必要があります。ハッシュ関数によって計算されたハッシュ値に関する情報は、管理サーバーのデータベースに保存されます。

    SHA256 は、アルゴリズムに既知の弱点がない暗号ハッシュ関数であり、現在最も安全なハッシュ関数であると考えられています。Kaspersky Endpoint Security 10 以降では SHA256 がサポートされています。MD5 ハッシュ関数は、Kaspersky Endpoint Security の 10 以前のバージョンでサポートされています。

Kaspersky Endpoint Security がカテゴリ内のファイルに適用するハッシュ関数を 1 つ選択します。

- ネットワークにインストールされているセキュリティ製品のすべてのインスタンスが Kaspersky Endpoint Security のバージョン 10 以降である場合は、［**SHA256**］をオンにします。Kaspersky Endpoint Security のバージョン 10 以前の実行ファイルの SHA256 ハッシュに基づくカテゴリの作成は推奨されません。これにより、セキュリティ 製品が誤動作する可能性があります。この場合は、カテゴリのファイルに対して MD5 暗号化ハッシュ関数を使用できます。

- ネットワークに Kaspersky Endpoint Security 10 以前のバージョンがインストールされている場合は、［**MD5 ハッシュ**］をオンにします。Kaspersky Endpoint Security のバージョン 10 以降の実行ファイルの MD5 ハッシュに基づいてカテゴリを作成することはできません。この場合は、カテゴリのファイルに対して SHA256 暗号化ハッシュ関数を使用できます。

- ネットワークに Kaspersky Endpoint Security のバージョン 10 以前とそれ以降の両方を使用しているデバイスが含まれている場合は、［**SHA256**］と［**MD5 ハッシュ**］をオンにします。

メタデータ

このオプションをオンにすると、ファイル名、ファイルのバージョン、製造元などのファイルのメタデータを指定できます。カテゴリの条件は、同一のメタデータを持つ実行可能ファイルのみに一致します。

証明書

このオプションをオンにすると、ストアから証明書を指定できます。カテゴリの条件は、指定された証明書で署名された実行ファイルのみに一致します。

- **MSI パッケージ、アーカイブフォルダーから選択**

  このオプションをオンにすると、カスタムカテゴリにアプリケーションを追加するための条件として、MSI インストーラーファイルを指定できます。アプリケーションのインストーラーのメタデータは管理サーバーに送信されます。インストーラーのメタデータが指定された MSI インストーラーと一致するアプリケーションが、カスタムアプリケーションカテゴリに追加されます。

ステップ 3：

このステップは、カテゴリ種別［**手動でコンテンツを追加するカテゴリ：実行ファイルのデータを手動でカテゴリに追加します**］を選択した場合に利用できます。

この手順で指定したアプリケーションは、「アプリケーションをカテゴリに含める条件の設定」ステップで指定されていても、カテゴリから除外されます。

このステップでは、カテゴリからアプリケーションを除外するための基準を選択します。

- **KL カテゴリから選択**

  このオプションをオンにすると、カスタムカテゴリにアプリケーションを追加するための条件として、カスペルスキー製品のカテゴリを指定できます。*KL カテゴリ*とは、テーマ属性が共有されているアプリケーションのリストです。このリストは、カスペルスキーのスペシャリストによって管理されています。たとえば、「Office アプリケーション」KL カテゴリには、Microsoft Office スイートのアプリケーション、Adobe Acrobat などが含まれます。

すべての KL カテゴリを選択することで、広範な信頼するアプリケーションのリストを生成できます。

- **リポジトリから証明書を選択**

  このオプションをオンにすると、ストアから証明書を指定できます。カテゴリの条件は、指定された証明書で署名された実行ファイルのみに一致します。

  ルールを適用する条件として証明書を選択した場合、その証明書がコンピューター上の信頼するシステムの保管領域に追加されていることを確認し、本製品で信頼するシステム保管領域の使用設定を確認してください。

- **アプリケーションのパスを指定（マスクをサポート）**

  このオプションをオンにすると、クライアントデバイス上のファイルまたはフォルダーを指定して、そこから実行ファイルをカスタムアプリケーションカテゴリに追加できます。`C:\path_to_exe\*` のような正規表現を使用できます。例：`C:\Program Files\Internet Explorer\*`

- **リムーバブルドライブ**

  このオプションをオンにすると、アプリケーションを起動するメディアの種類（任意またはリムーバブルドライブ）を指定できます。選択した種別のメディアから起動されたアプリケーションがカスタムアプリケーションカテゴリに追加されます。

- **ハッシュ、メタデータ、証明書のいずれか**：

  - **実行ファイルのリストから選択する**

    このオプションをオンにすると、クライアントデバイス上の実行ファイルのリストからカテゴリに追加するアプリケーションを選択できます。

  - **アプリケーションのレジストリから選択する**

    このオプションをオンにすると、アプリケーションのレジストリが表示されます。レジストリからアプリケーションを選択すると、選択したアプリケーションのメタデータが事前に入力された設定を含むウィンドウが開きます。

    - ファイル名
    - ファイルバージョン 正確なバージョンを指定するか、条件（例：「5.0 より大きい」）を入力できます。
    - 製品名。
    - 本ソフトウェアのバージョン。正確なバージョンを指定することも、条件（例：「5.0 より大きい」など）を入力することもできます。
    - 製造元。

    指定されたパラメータに一致する実行ファイルのみがブロックされ、選択したアプリケーションの起動自体はブロックされないことにご注意ください。選択したメタデータが、アプリケーションの起動時に開始される実行ファイルのメタデータと一致する場合は、次のステップに進めます。それ以外の場合は、実行可能ファイルのメタデータと一致するように値を手動で編集する必要があります。

- **手動設定**

  このオプションをオンにすると、カスタムカテゴリにアプリケーションを追加するための条件として、ファイルハッシュ、メタデータ、または証明書を指定する必要があります。

  ファイルのハッシュ

  ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、Kaspersky Endpoint Security がカテゴリ内のファイルに適用するハッシュアルゴリズムを選択する必要があります。ハッシュ関数によって計算されたハッシュ値に関する情報は、管理サーバーのデータベースに保存されます。

  SHA256 は、アルゴリズムに既知の弱点がない暗号ハッシュ関数であり、現在最も安全なハッシュ関数であると考えられています。Kaspersky Endpoint Security 10 以降では SHA256 がサポートされています。MD5 ハッシュ関数は、Kaspersky Endpoint Security の 10 以前のバージョンでサポートされています。

  Kaspersky Endpoint Security がカテゴリ内のファイルに適用するハッシュ関数を 1 つ選択します。

  - ネットワークにインストールされているセキュリティ製品のすべてのインスタンスが Kaspersky Endpoint Security のバージョン 10 以降である場合は、［**SHA256**］をオンにします。Kaspersky Endpoint Security のバージョン 10 以前の実行ファイルの SHA256 ハッシュに基づくカテゴリの作成は推奨されません。これにより、セキュリティ 製品が誤動作する可能性があります。この場合は、カテゴリのファイルに対して MD5 暗号化ハッシュ関数を使用できます。

  - ネットワークに Kaspersky Endpoint Security 10 以前のバージョンがインストールされている場合は、［**MD5 ハッシュ**］をオンにします。Kaspersky Endpoint Security のバージョン 10 以降の実行ファイルの MD5 ハッシュに基づいてカテゴリを作成することはできません。この場合は、カテゴリのファイルに対して SHA256 暗号化ハッシュ関数を使用できます。

  - ネットワークに Kaspersky Endpoint Security のバージョン 10 以前とそれ以降の両方を使用しているデバイスが含まれている場合は、［**SHA256**］と［**MD5 ハッシュ**］をオンにします。

  メタデータ

  このオプションをオンにすると、ファイル名、ファイルのバージョン、製造元などのファイルのメタデータを指定できます。カテゴリの条件は、同一のメタデータを持つ実行可能ファイルのみに一致します。

  証明書

  このオプションをオンにすると、ストアから証明書を指定できます。カテゴリの条件は、指定された証明書で署名された実行ファイルのみに一致します。

- **MSI パッケージ、アーカイブフォルダーから選択**

  このオプションをオンにすると、カスタムカテゴリにアプリケーションを追加するための条件として、MSI インストーラーファイルを指定できます。アプリケーションのインストーラーのメタデータは管理サーバーに送信されます。インストーラーのメタデータが指定された MSI インストーラーと一致するアプリケーションが、カスタムアプリケーションカテゴリに追加されます。

ステップ 4：設定

このステップは、カテゴリ種別［**選択したデバイスの実行ファイルを含むカテゴリ：デバイスの実行ファイルが自動的に処理され、メトリックがカテゴリに追加されます**］を選択した場合に利用できます。

この手順では、［**追加**］をクリックしてコンピューターを指定します。そのコンピューターにある実行ファイルが、Kaspersky Security Center によってアプリケーションカテゴリに追加されます。

この手順では、次の設定を構成できます：

- **ハッシュ関数の計算アルゴリズム**

  ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、Kaspersky Security Center がカテゴリ内のファイルに適用するハッシュアルゴリズムを選択する必要があります。ハッシュ関数によって計算されたハッシュ値に関する情報は、管理サーバーのデータベースに保存されます。

  *SHA256 は、アルゴリズムに既知の弱点がない暗号ハッシュ関数であり、現在最も安全なハッシュ関数であると考えられています。*Kaspersky Endpoint Security for Linux では SHA256 がサポートされています。

  カテゴリ内のファイルに適用するハッシュアルゴリズムを 1 つ選択します：

  - 保護対象デバイスで Kaspersky Endpoint Security for Linux を使用している場合は、**このカテゴリのファイルの SHA256 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以降のバージョンでサポート）** チェックボックスをオンにします。

  - 保護対象デバイスで Kaspersky Endpoint Security for Windows を使用している場合は、**このカテゴリのファイルの MD5 の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows より前のバージョンでサポート）** チェックボックスをオンにします。

  ネットワーク内で Windows 用と Linux 用の両方の製品を使用している場合は、両方のチェックボックスをオンにします。

- **管理サーバーの保管領域とデータを同期する**

  管理サーバーが指定されたフォルダ（複数可）の変更を定期的に確認するように設定する場合は、このオプションを有効にします。

  既定で、この設定は有効です。

  このパラメータを有効にすると、指定したフォルダ（複数可）の変更をチェックする期間を時間単位で指定します。既定では、期間は 24 時間 に設定されています。

- **ファイル種別**

  このセクションでは、アプリケーションカテゴリを作成するために使用するファイル種別を指定できます。

  すべてのファイルこのカテゴリはすべてのファイルに一致します。このオプションは既定では有効になっています。

  アプリケーションカテゴリ以外のファイルのみこのカテゴリは、アプリケーションカテゴリ以外のファイルのみに一致します。

- **<フォルダー>**

  このセクションでは、アプリケーションカテゴリの作成に使用するファイルが含まれる、選択したコンピューターのフォルダーを指定できます。

  すべてのフォルダーこのカテゴリはすべてのフォルダーに一致します。このオプションは既定では有効になっています。

  指定フォルダーこのカテゴリは指定されたフォルダーのみに一致します。このオプションを選択した場合は、フォルダーパスを指定する必要があります。

ステップ 5：

このステップは、カテゴリ種別［**特定のフォルダーの実行ファイルを含むカテゴリ：指定されたフォルダーにコピーされたアプリケーションの実行ファイルが自動的に処理され、メトリックがカテゴリに追加されます**］を選択した場合に利用できます。

このステップでは、カテゴリの作成に使用する実行ファイルが格納されているフォルダーを指定します。

次の設定を管理します：

- **ダイナミックリンクライブラリ（DLL）をこのカテゴリに含める**

  アプリケーションカテゴリにはダイナミックリンクライブラリ（DLL 形式のファイル）が含まれ、アプリケーションコントロールコンポーネントはシステム内で実行されているそのようなライブラリの処理を記録します。DLL ファイルをアプリケーションカテゴリに含めると、Kaspersky Security Center のパフォーマンスが低下する場合があります。

  既定では、このチェックボックスはオフです。

- **このカテゴリ内のスクリプトデータを含める**

  アプリケーションカテゴリにはスクリプトに関するデータが含まれ、スクリプトはウェブ脅威対策によってブロックされません。スクリプトのデータをカテゴリに含めると、Kaspersky Security Center のパフォーマンスが低下する場合があります。

  既定では、このチェックボックスはオフです。

- **ハッシュ関数の計算アルゴリズム**

  ネットワーク内のデバイスにインストールされているセキュリティ製品のバージョンに応じて、Kaspersky Security Center がカテゴリ内のファイルに適用するハッシュアルゴリズムを選択する必要があります。ハッシュ関数によって計算されたハッシュ値に関する情報は、管理サーバーのデータベースに保存されます。

  *SHA256 は、アルゴリズムに既知の弱点がない暗号ハッシュ関数であり、現在最も安全なハッシュ関数であると考えられています。*Kaspersky Endpoint Security for Linux では SHA256 がサポートされています。

カテゴリ内のファイルに適用するハッシュアルゴリズムを1つ選択します：

- 保護対象デバイスでKaspersky Endpoint Security for Linuxを使用している場合は、**このカテゴリのファイルのSHA256の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windows以降のバージョンでサポート）** チェックボックスをオンにします。

- 保護対象デバイスでKaspersky Endpoint Security for Windowsを使用している場合は、**このカテゴリのファイルのMD5の値を計算する（Kaspersky Endpoint Security 10 Service Pack 2 for Windowsより前のバージョンでサポート）** チェックボックスをオンにします。

ネットワーク内でWindows用とLinux用の両方の製品を使用している場合は、両方のチェックボックスをオンにします。

- **変更のあったフォルダーを強制スキャンする**

  このオプションをオンにすると、本製品はカテゴリコンテンツの追加用フォルダーに変更がないか定期的に確認します。チェックボックスの横にある入力フィールドで、確認の頻度（時間単位）を指定できます。既定では、強制的な確認の間隔は24時間です。

  このオプションがオフの場合、本製品はフォルダーの確認を強制的に実行しません。サーバーは、ファイルが変更、追加、または削除された場合に、そのファイルへのアクセスを試行します。

  既定では、このチェックボックスはオフです。

ステップ6：

ウィザードを終了します。ウィザードが終了すると、新しいアプリケーションカテゴリが作成されます。カテゴリ内のアプリケーションは、アプリケーションコントロールルールを使用して管理できます。

ゴールデンイメージ

インベントリを使用して、Golden Imageアプリケーションカテゴリを追加できます。既定では、このカテゴリは空です。「ゴールデンイメージ」カテゴリには、オペレーティングシステムとともにデバイスに提供されるアプリケーションが含まれます。このカテゴリのアプリケーションは信頼されているとみなされます。必要に応じて、サードパーティ製アプリケーションをこのカテゴリに追加できます。

インベントリタスクが完了すると、本製品は「ゴールデンイメージ」カテゴリを次のように変更できます：

- **変更なし** – インベントリの完了後、「ゴールデンイメージ」カテゴリを変更しません。これは既定で選択されています。このオプションは、デバイスで使用されているサードパーティ製アプリケーションのリストを取得するが、それらのアプリケーションを「ゴールデンイメージ」カテゴリに追加しない場合に使用します。

- **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によってデバイス上で検知されたアプリケーションを「ゴールデンイメージ」カテゴリに追加します。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。

- **削除** – 「ゴールデンイメージ」アプリケーションカテゴリをクリアします。タスクが開始されるとすぐにカテゴリがクリアされ、デバイス上のファイルのインベントリは実行されません。

これは、次のシナリオで役立ちます：

- デバイス上で「ゴールデンイメージ」カテゴリのアプリケーションが起動されないようにする必要があるが、アプリケーションコントロールルールを無効にできない場合。
- 現在のポリシーとは異なるアプリケーションコントロールルールを含む新しいポリシーをデバイスに適用する場合、またはデバイスを子ポリシーに移動する場合。この場合、許可されたアプリケーションを誤ってブロックしないようにするため、「ゴールデンイメージ」カテゴリをクリアすることを推奨します。

ベースラインコンピューターに基づくゴールデンイメージカテゴリの設定

ベースラインコンピューターを使用して、必要な一連のアプリケーションを含むゴールデンイメージカテゴリを作成できます。その後、このカテゴリを使用して、アプリケーションコントロールの許可ルールを作成できます。

ベースラインコンピューターに基づくゴールデンイメージカテゴリを設定するには、次の手順を実行します：

1. **参照用コンピューターを設定する**

   デバイスが社内ネットワークで動作するために必要なすべてのソフトウェア（Kaspersky Endpoint Security for Linux およびネットワークエージェントを含む）をインストールして設定します。

2. **インベントリタスクを作成する**

   Web コンソールまたはコマンドラインでタスクを作成し、次の設定を管理します：

   - アプリケーションの「ゴールデンイメージ」カテゴリに対する処理： **アップデートまたは作成（存在しない場合）**；

     ```
     GoldenImageAction=Create
     ```

   - インベントリの対象範囲は参照用コンピューターです。

3. **インベントリタスクを実行し、完了するまで待機します。**

   タスクにより、アプリケーションの「ゴールデンイメージ」カテゴリが生成されます。

4. **カテゴリのリストをファイルにエクスポートします。**

   > Web コンソールではカテゴリのリストをエクスポートできません。

   次のコマンドを実行します：

   ```
   kesl-control [-A] --get-categories --file <path to file> --json
   ```

   ここで、`<path to file>` は、タスク設定の出力先となる設定情報ファイルへのパスです。

5. **必要に応じて「ゴールデンイメージ」カテゴリを調整する**

   アプリケーションカテゴリのリストを含む設定情報ファイルを確認します。必要に応じて、「ゴールデンイメージ」カテゴリのアプリケーションのリストを調整します。

6 **設定情報ファイルから設定をインポートします。**

アプリケーションカテゴリのリストを含む設定情報ファイルを変更した場合は、そのファイルをアプリケーションにインポートします：

```
kesl-control [-A] --set-categories --names GoldenImage [<category name 1> <category name 2> ... <name of category N>] --file <path to file>
```

ここで、`<category name 1> <category name 2> ... <category name N>` は、「ゴールデンイメージ」カテゴリ以外の、情報を変更するカテゴリの名前です。

`<path to file>` は、タスク設定の出力先となる設定情報ファイルへのパスです。

その結果、「ゴールデンイメージ」カテゴリを使用してアプリケーションコントロールルールを作成できます。

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*は、選択したユーザーグループに対してアプリケーションコントロールがサードパーティ製アプリケーションの起動を許可するか拒否するかを決定する一連の条件です。

ルールは、次の条件に従ってサードパーティ製アプリケーションの起動を制限します：

- **アプリケーションカテゴリ**。アプリケーションカテゴリに属するアプリケーション。

  各カテゴリは、1つのルールでのみ使用できます。

- **ユーザーとユーザーグループ**。アプリケーションコントロールを使用すると、個々のユーザーまたはユーザーグループによるサードパーティ製アプリケーションへのアクセスを制限できます。たとえば、組織内のユーザーのうち、IT 部門に所属するユーザーを除くすべてのユーザーに対して、リモート管理アプリケーションへのアクセスを制限できます。

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：

- **有効にします**。アプリケーションコントロールはルールを適用します。
- **無効**。アプリケーションコントロールはこのルールを適用しません。
- **テスト**。アプリケーションコントロール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しませんが、起動に関する通知を管理サーバーに送信します。

Web コンソールでアプリケーションコントロールルールを追加する方法

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**］ブロックの［**追加**］をクリックします。
   これにより、アプリケーションコントロールルールを追加するためのフォームが開きます。

7. ［**ステータス**］でルールのステータスを設定します。

8. ルールをテストする場合は、このトグルスイッチを **有効** に設定し、［**テストモード**］チェックボックスをオンにします。

9. ［**ルール名**］にルール名を入力します。ルール名は一意である必要があります。

10. ルールを適用するアプリケーションカテゴリを選択します。カテゴリを指定しないとルールを保存できません。

11. アプリケーションを実行するユーザーまたはユーザーグループと、その権限を選択します。

12. 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ルールを追加する方法

1. アプリケーションコントロールルールのリストをファイルに出力します：

```
kesl-control --get-settings 21 --file <path to file> [--json]
```

2. 設定情報ファイルを開き、アプリケーションコントロールモードに応じて、ID `#` のルールのセクションを追加します：

   a. `AppControlMode=AllowList`:

   ```
   [AllowListRules.item_#]
   Description=<rule name>
   AppControlRuleStatus=<On|Off|Test>
   Category=<category name>
   [AllowListRules.item_#.ACL.item_#]
   Access=<Allow|Block>
   Principal=<user>
   ```

   モードが選択されている場合

   b. `AppControlMode=DenyList`:

   ```
   [DenyListRules.item_#]
   Description=<rule name>
   AppControlRuleStatus=<On|Off|Test>
   Category=<category name>
   [DenyListRules.item_#.ACL.item_#]
   Access=<Allow|Block>
   Principal=<user>
   ```

   モードが選択されている場合

3. 設定情報ファイルから設定をアプリケーションにインポートします：

```
kesl-control --set-settings 21 --file <path to file> [--json]
```

記号

設定	説明
[AllowListRules.item_#] [DenyListRules.item_#]	ID # のアプリケーションコントロールルール。
[AllowListRules.item_#.ACL.item_#] [DenyListRules.item_#.ACL.item_#]	ID # の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のリスト。
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。 Golden Image を指定できます。
Access	ユーザーまたはユーザーグループに割り当てられるアクセスの種別： Allow（既定値）– アプリケーションの実行を許可します。 Block – 実行中のアプリケーションを拒否します。
Principal	アプリケーションコントロールルールが適用されるユーザーまたはユーザーグループ： \Everyone（既定値）– すべてのユーザーにルールが適用されます。 <user> は、ルールを適用するユーザーの名前です。 @<group name> は、ルールを適用するユーザーグループの名前です。

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が動作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をテストすることを推奨します。テストモードでは、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し、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。

システム変更監視

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。

システム変更監視の仕組み

システム変更監視は、リアルタイムおよびオンデマンドで動作できます：

- *システム変更監視* コンポーネントでは、監視範囲に含めたファイルとディレクトリの変更の監視を*リアルタイムで*実行できます。
- *システム変更チェック*機能では、監視範囲に含まれるオブジェクトについて、記録されたステータスとの現在のステータスの比較を*スケジュールに基づいて、またはオンデマンドで*実行できます。

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。

特別な考慮事項と制限事項

- 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。
- 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。

リアルタイムのシステム整合性監視

システム変更監視では、監視範囲に含まれるオブジェクトの変更をリアルタイムで検知できます。

システム変更監視の仕組み

1. **アプリケーションがファイル操作イベントをインターセプトする**

   アプリケーションは、スキャン対象のファイルに対して読み取り専用アクセス権を持つ特殊なインターセプトメカニズムを使用します。

2. **アプリケーションは、ファイルが変更されているかどうかを確認します。**

   システム変更監視は、次のファイルプロパティの変更を追跡します：

   - 内容（`write ()`、`truncate ()`、その他の変更）
   - メタデータ（`chmod` コマンドまたは `chown` コマンドによるアクセス権限の変更）
   - タイムスタンプ（`utimensat`）
   - 拡張属性（`setxattr`）など

3. **スキャンの完了**

   アプリケーションは、ファイルが変更されている場合、*システム変更チェックに失敗しました*イベントを生成します。

システム変更監視の設定

1. **システム変更監視を有効にする**

   既定では、システム変更監視は無効になっています。ファイルの変更をリアルタイムで監視するデバイスを選択し、それらのデバイスでシステム変更監視コンポーネントを有効にします。

2. **監視範囲の設定**

   コンポーネントが動作するには、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/`）の監視範囲が設定されています。

   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。

   Web コンソールで監視範囲を設定する方法

   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**］→［**システム変更監視**］に移動します。

5. ［**監視範囲**］リンクをクリックします。
   スキャン範囲のテーブルが表示されたウィンドウが開きます。

6. ［**追加**］をクリックします。
   スキャン範囲を追加するウィンドウが開きます

7. **名前** フィールドで、監視範囲の名前（例：*重要なオブジェクト*）を指定します。

8. **パス** フィールドで、個々のファイルまたはディレクトリへのパス（例：`/path/to/folder`）を指定します。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。

9. 必要に応じて、コマンドシェル形式でオブジェクト名のマスク（例：`*.txt` または `file?.*`）を指定します。マスクは一度に 1 つずつ追加します。

10. 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。

システム変更監視

コマンドラインで監視範囲を設定する方法

1. 次のコマンドを実行します：

```
kesl-control --set-settings 11  ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 11
```

記号

コマンドオプション

設定	説明
`UseScanArea=Yes`	ID が `#` の監視範囲を有効にします。 監視範囲を削除せずに、監視範囲のスキャンを一時的に無効にできます。これを行うには、`ScanScope.item_#.UseScanArea=No` を設定します。
`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。

設定	説明
`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。 例：「`ScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`」。
`Path`	監視対象のディレクトリのパス。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。

例

`/etc` ディレクトリのみを含む監視範囲：

```
kesl-control --set-settings 11 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

3 監視の除外範囲を設定する

除外は監視範囲よりも優先度が高くなります。除外されたオブジェクトは、監視範囲内にある場合でもスキャンされません。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。

Web コンソールで除外範囲を設定するには

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**］→［**システム変更監視**］に移動します。

除外は、パスまたはファイル名マスクで指定できます。本製品では、ディレクトリ全体（または個別のファイル）をスキャンから除外したり、監視範囲内でファイル名マスクが一致するファイルを除外したりできます。

パスで除外を追加するには：

1. ［**除外リストの範囲**］リンクをクリックします。
   除外範囲のテーブルを含むウィンドウが開きます。
2. ［**追加**］をクリックします。
   除外範囲を追加するためのウィンドウが開きます。
3. **名前** フィールドで、除外範囲の名前（例：*システムファイル*）を指定します。
4. **パス** フィールドで、個々のファイルまたはディレクトリへのパス（例：`/path/to/folder`）を指定します。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。

5. コマンドシェル形式でオブジェクト名のマスク（例：`*.txt` または `file?.*`）を指定します。マスクは一度に1つずつ追加します。

6. 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。

ファイル名マスクで除外を追加するには：

1. ［**マスクによる除外リストを追加**］チェックボックスをオンにします。

2. ［**マスクによる除外**］リンクをクリックします。
   マスクによる除外範囲のテーブルが開きます。

3. ［**追加**］をクリックします。
   マスクによる除外範囲を追加するためのウィンドウが開きます。

4. ファイル名マスクをコマンドシェル形式で指定します（例：`*.txt` または `file?.*`）。マスクは一度に1つずつ追加します。

5. 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。

コマンドラインで除外範囲を設定する方法

1. 次のコマンドを実行します：

```
kesl-control --set-settings 11  ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 11
```

記号

コマンドオプション

設定	説明
`UseScanArea=Yes`	ID `#` の指定した範囲を監視対象から除外します。 除外範囲を削除する代わりに、一時的に無効にすることができます。これを行うには、`ExcludedFromScanScope.item_#.UseScanArea=No` を設定します。
`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。
`AreaMask.item_#`	除外範囲の制限。除外範囲では、本製品は、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スキャンから除外します。 例：「`ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`」。
`Path`	スキャンから除外するディレクトリへのパス。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。

例

`/tmp` ディレクトリのみを含む除外範囲：

```
kesl-control --set-settings 11 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

システム整合性チェック

*システム変更チェック*タスクの実行中、本製品は各オブジェクトの現在の状態を元の状態（ベースライン）と比較します。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。これにより、監視範囲に含まれるファイルとディレクトリの変更を追跡できます。

> 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。

システム変更監視コンポーネントとは異なり、*システム変更チェック*タスクでは、イベント数を制限し、オペレーティングシステムでの変更に関する要約レポートを生成できます。

システム変更チェックの仕組み

1. **本製品はシステムのスナップショットを取得します**

   システムのベースラインは、タスクの初回実行時に作成されます。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。Linux デバイスでは、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）や、**タスクを開始するたびにベースラインを再構築する**設定を有効にしてタスクが開始された場合に、ベースラインが再構築されます。

   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。ベースラインは、関連するシステム変更チェックタスクと一緒に削除されます。

2. **本製品はシステムの状態の変更を検出します**

   本製品は、監視範囲に含まれるオブジェクトに関する情報を比較するために、次の基準を適用します：

   - ファイルの SHA256 ハッシュ（完全チェックの場合）
   - ファイル変更時間
   - ファイルサイズ

3. **スキャンの完了**

   システムの現在の状態がベースラインと異なる場合、Kaspersky Endpoint Security はシステム変更違反イベントを生成します：*システム変更チェックに失敗しました。*

システム変更チェックタスクの設定と実行

1. **システム変更チェックタスクの作成**

   Web コンソールでシステム変更チェックタスクを作成する方法

   1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
      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**］から［**Kaspersky Endpoint Security for Linux 12.5**］を選択します。
      b. ［**タスク種別**］から［**システム変更チェック**］を選択します。
      c. ［**タスク名**］に「*週次のシステム変更チェック*」などの短く分かりやすい名前を付けます。
      d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。
   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。
   5. ウィザードを終了します。

   コマンドラインでシステム変更チェックタスクを作成する方法

   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 <task name> --type ODFIM
   ```

   ここで、`<task name>` は新しいタスクの名前です。

   このコマンドは、作成されたタスクの ID を返します。

   コマンド実行結果の例：

   タスクが作成されました（タスク ID：115）

2. **必要に応じて、タスク設定を編集します**

   Web コンソールでシステム変更チェックタスクを設定する方法

   1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
      タスクのリストが表示されます。
   2. 新しく作成したシステム変更チェック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。
   3. ［**アプリケーション設定**］タブを選択します。

4. スキャン種別を選択します：

- **完全スキャン**本製品は、ファイルの現在の状態の SHA256 ハッシュと、システムスナップショットのハッシュを比較します。
- **簡易スキャン**本製品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、変更時刻は重要なパラメータとはみなされません。

5. ［**システム変更チェック設定**］セクションで、次のチェックボックスをオンにします：

- **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をオンにすると、本製品はタスクが開始されるたびにベースラインを再構築します。
- **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をオンにすると、本製品はユーザーが指定したディレクトリをチェックします。チェックボックスをオフにすると、本製品は既定のスキャン範囲（*カスペルスキーの内部オブジェクト*（`/opt/kaspersky/kesl/`））のみをスキャンします。
- **各タスクの開始時にファイルの最終アクセス時刻を追跡する**このチェックボックスをオンにすると、本製品はタスクが実行されるたびにファイルの最終アクセス時刻（`noatime` パラメータ）をチェックします。

6. 変更内容を保存します。

コマンドラインでシステム変更チェックタスクを設定する方法

次のコマンドを実行します：

```
kesl-control --set-settings <task ID|name> RebuildBaseline=<Yes|No> [CheckFileHash=<Yes|No>]
[TrackDirectoryChanges=<Yes|No>] [TrackLastAccessTime=<Yes|No>] [UseExcludeMasks=<Yes|No>]
[ExcludeMasks.item_#=<object mask>]
```

記号

［*システム変更チェック*］タスクの設定

設定	説明
`RebuildBaseline`	タスクを開始するたびにベースラインを再構築する。
`CheckFileHash`	ファイルの SHA256 ハッシュのスキャン。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`	ユーザーが指定したディレクトリのスキャン。設定を無効にすると、本製品は既定の範囲（`/opt/kaspersky/kesl/`）のみをスキャンします。
`TrackLastAccessTime`	ファイルの最終アクセス時刻のチェック（`noatime` オプション）。
`UseExcludeMasks`	監視からの除外。新しい `[ExcludeMasks.item_#]` セクションが設定情報ファイルに追加されます。本製品は、このセクションで指定されたオブジェクトをスキャンしません。 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。
`ExcludeMasks.item_#=<object mask>`	監視範囲からのオブジェクトの除外。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、コマンド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。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。 この設定は、`UseExcludeMasks` パラメータが有効になっている場合にのみ管理できます。 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。 例：`ExcludeMasks.item_0000=<eicar1.*>`

3 監視範囲の設定

タスクを開始するには、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/`）の監視範囲が設定されています。

タスクは、ベースラインにタスクの監視範囲に属するオブジェクトに関する情報が含まれている場合にのみ実行されます。

指定された範囲にあるオブジェクトは、範囲の表の並び順でスキャンされます。必要に応じて、サブディレクトリを親ディレクトリよりもリストの上に配置し、親ディレクトリとは異なるセキュリティ設定をサブディレクトリに設定します。

Web コンソールで監視範囲を設定する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
   タスクのリストが表示されます。
2. 新しく作成したシステム変更チェック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。
3. ［**アプリケーション設定**］タブを選択します。
4. ［**監視範囲にあるディレクトリを監視する**］がオンになっていることを確認してください。
5. ［**監視と除外範囲**］セクションで、［**監視範囲**］をクリックします。
   スキャン範囲のテーブルが表示されたウィンドウが開きます。
6. ［**追加**］をクリックします。
   スキャン範囲を追加するウィンドウが開きます
7. ［**名前**］フィールドに、監視範囲の名前（例：*デスクトップ上のファイル*）を入力します。
8. **パス** フィールドで、個々のファイルまたはディレクトリへのパス（例：`/path/to/folder`）を指定します。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。
9. 必要に応じて、コマンドシェル形式でオブジェクト名のマスクを指定します（例：`*.txt`、`file?.*`）。マスクは一度に1つずつ追加します。
10. 変更内容を保存します。

コマンドラインで監視範囲を設定する方法

1. 次のコマンドを実行します：

```
kesl-control --set-settings <task ID|name> TrackDirectoryChanges=Yes ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. 現在の設定を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings <task ID|name>
```

記号

［システム変更チェック］タスクの設定

設定	説明
UseScanArea=Yes	ID が # の監視範囲を有効にします。 監視範囲を削除せずに、監視範囲のスキャンを一時的に無効にできます。これを行うには、ScanScope.item_#.UseScanArea=No を設定します。
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。
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 ScanScope.item_#.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。 例：「ScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt」。
Path	監視対象のディレクトリのパス。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。

例

/etc ディレクトリのみを含む監視範囲：

```
kesl-control --set-settings 115 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

4 監視の除外範囲を設定する

除外は監視範囲よりも優先度が高くなります。除外されたオブジェクトは、監視範囲内にある場合でもスキャンされません。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。

Web コンソールで除外範囲を設定するには

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
2. タスクのリストが表示されます。
3. 新しく作成したシステム変更チェック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。
4. ［**アプリケーション設定**］タブを選択します。

除外は、パスまたはファイル名マスクで指定できます。本製品では、ディレクトリ全体（または個別のファイル）をスキャンから除外したり、監視範囲内でファイル名マスクが一致するファイルを除外したりできます。

パスで除外を追加するには：

1. ［**監視と除外範囲**］セクションで、［**除外リストの範囲**］をクリックします。
   除外範囲のテーブルを含むウィンドウが開きます。
2. ［**追加**］をクリックします。
   除外範囲を追加するためのウィンドウが開きます。
3. **名前** フィールドで、除外範囲の名前（例：システムファイル）を指定します。
4. **パス** フィールドで、個々のファイルまたはディレクトリへのパス（例：/path/to/folder）を指定します。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。

5. コマンドシェル形式でオブジェクト名のマスク（例：`*.txt` または `file?.*`）を指定します。マスクは一度に1つずつ追加します。

6. 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。

ファイル名マスクで除外を追加するには：

1. ［**監視と除外範囲**］セクションで、［**マスクによる除外**］をクリックします。
   マスクによる除外範囲のテーブルが開きます。

2. ［**追加**］をクリックします。
   マスクによる除外範囲を追加するためのウィンドウが開きます。

3. ファイル名マスクをコマンドシェル形式で指定します（例：`*.txt` または `file?.*`）。マスクは一度に1つずつ追加します。

4. 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。

コマンドラインで除外範囲を設定する方法

1. 次のコマンドを実行します：

```
kesl-control --set-settings <task ID|name>      ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. 現在の設定を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings <task ID|name>
```

記号

［*システム変更チェック*］タスクの設定

設定	説明
`UseScanArea=Yes`	ID `#` の指定した範囲を監視対象から除外します。 除外範囲を削除する代わりに、一時的に無効にすることができます。これを行うには、`ExcludedFromScanScope.item_#.UseScanArea=No` を設定します。
`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。
`AreaMask.item_#`	除外範囲の制限。除外範囲では、本製品は、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スキャンから除外します。 複数の `ExcludedFromScanScope.item_#.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。 例：「`ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`」。
`Path`	スキャンから除外するディレクトリへのパス。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。

例

`/tmp` ディレクトリのみを含む除外範囲：

```
kesl-control --set-settings 115 ExcludedFromScanScope.item_0001.UseScanArea=Yes
```

```
ScanScope.item_0001.Path=/tmp
```

5 **タスクの実行**

Web コンソールでシステム変更チェックタスクを実行する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
   タスクのリストが表示されます。
2. 作成したタスクの横にあるチェックボックスをオンにします。
3. ［**開始**］をクリックします。

コマンドラインでシステム変更チェックタスクを実行する方法

タスクを実行するには、次のコマンドを実行します：

```
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。

信頼ゾーン

*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。

信頼ゾーンの設定

設定	説明
Web アドレス	ウェブ脅威対策コンポーネントが信頼すると判断する URL。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 URL のリストは、既知の Web サイトからファイルをダウンロードする際にコンポーネントによって妨げられる場合などに使用できます。 詳しくは、信頼する URL を追加する方法の記事を参照してください
IP アドレス	信頼するデバイスの IP アドレス。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。 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。 詳しくは、コンピューターの信頼する IP アドレスを追加する方法の記事を参照してください
ネットワークポート	ネットワーク脅威対策コンポーネントがスキャン対象から除外するネットワークポートのリストです。 詳しくは、監視対象のネットワークポートを選択する方法の記事を参照してください

設定	説明
ルート証明書	Kaspersky Endpoint Security が信頼すると判断するルート証明書。信頼するルート証明書のリストは、ウェブ脅威対策、メール脅威対策、ウェブコントロールの各コンポーネントが暗号化された接続（HTTPS 接続）をスキャンする際に使用されます。 詳しくは、信頼するルート証明書のリストに証明書を追加する方法の記事を参照してください
ドメイン	信頼するドメインのリストウェブ脅威対策およびウェブコントロールの各コンポーネントは、これらのドメインとの暗号化された接続を制御しません。 詳しくは、信頼するドメインを追加する方法の記事を参照してください
マウントポイント	信頼するマウントポイントのリスト。ファイル脅威対策、アンチクリプター、コンテナスキャンの各コンポーネントは、指定されたマウントポイントをスキャン対象から除外します。 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。 詳しくは、「マウントポイントを除外する方法」の記事を参照してください
アプリケーション	ファイルおよびネットワークの動作やシステムレジストリへのアクセスを Kaspersky Endpoint Security が制御しないアプリケーション。ファイル脅威対策やふるまい検知などの保護コンポーネントは、指定されたアプリケーションの動作を制御しません。 詳しくは、信頼するアプリケーションを追加する方法の記事を参照してください
マルウェアスキャンの除外リスト	本製品コンポーネントのすべてまたは一部によるスキャンから除外されるファイルまたはフォルダー、および（ウイルス百科事典に基づく）オブジェクト種別。 詳しくは、保護の除外を追加する方法の記事を参照してください
デバイス	デバイスコントロールコンポーネントが、選択されたユーザーまたはグループに対して常にフルアクセスを許可するデバイス。 詳しくは、信頼するデバイスを追加する方法の記事を参照してください

保護の除外を追加する方法

*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。

次の方法を使用して、スキャンからオブジェクトを除外できます：

- **除外**。ディレクトリパス。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。例：`/.snapshots/*/snapshot/`

  コンテナまたはイメージ内のパスを指定するには、タグを使用します。

  タグの使用方法

  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。

- **マスクによる除外**。マスクで指定されたファイル名。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。例：`*.txt` マスクは、すべてのテキストファイルに一致します。

  マスクを使用する

  - 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはディレクトリのパスにおけるファイル名またはディレクトリ名の区切り文字）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「`/dir/*/*.txt`」には、dir ディレクトリ内のディレクトリにある拡張子が TXT のすべてのファイルへのパスが含まれますが、サブディレクトリにあるファイルへのパスは含まれません。
  - 連続する2つの「`*`」文字。ファイル名またはディレクトリ名内の、「`\`」および「`/`」（ファイルまたはディレクトリのパスにおけるファイル名またはディレクトリ名の区切り文字）を含む任意の文字列（空の文字列を含む）に置き換えられます。たとえば、マスク「`/dir/**/*.txt`」には、dir ディレクトリ内にネストされたディレクトリにある拡張子が TXT のすべてのファイルへのパスが含まれますが、dir ディレクトリ自体にあるファイルへのパスは含まれません。
  - 「`?`」（クエスチョンマーク）文字。「`\`」および「`/`」（ファイルまたはディレクトリのパスにおけるファイル名またはディレクトリ名の区切り文字）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「`/dir/???.txt`」には、dir ディレクトリにある、拡張子が TXT でファイル名が3文字のすべてのファイルへのパスが含まれます。

- **脅威名による除外** カスペルスキー百科事典の分類に従ったオブジェクト種別の名前（例：`Email-Worm`、`Rootkit`、`RemoteAdmin`）。任意の1文字を置き換える「`?`」と複数の文字を置き換える「`*`」を使用してマスクを使用することができます。たとえば、マスク「`Client*`」を使用すると、「`Client-IRC`」、「`Client-P2P`」および「`Client-SMTP`」がスキャンから除外されます。

- **プロセスによる除外** プロセスパス。

Kaspersky Endpoint Security では、特定の形式のファイルを除外することもできます：アーカイブ、メールデータベース、テキストファイル、データベースログファイル。

Web コンソールで保護の除外を追加する方法

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. ［**ホスト脅威対策**］→［**ファイル脅威対策**］に移動します。
5. ［**信頼するオブジェクト**］リンクをクリックします。
6. 表示されたウィンドウで、［**追加**］をクリックします。
7. 保護の除外に使用する条件のチェックボックスをオンにします：
   - **ファイルまたはフォルダーのパス**ファイルまたはディレクトリのパス、またはファイル名のマスクを指定します。コンテナまたはイメージ内のパスを指定するには、タグを使用します。
     ローカルファイルシステムの場合は、ディレクトリパスを指定します（例：`/path/to/folder/`）。マウントされたファイルシステム、またはすべてのリモートマウントファイルシステムの場合は、ファイル名のマスクを入力します。マウントされたファイルシステムの場合は、アクセスプロトコル（NFS、Samba、またはカスタム）も指定します。
   - **オブジェクト種別**脅威名を指定します。
   - **オブジェクトハッシュ**オブジェクトの SHA256 ハッシュを入力します。除外の SHA256 ハッシュの取得元として、ファイルを追加したりイベントを指定したりすることもできます。
8. 除外を適用する保護コンポーネントを選択します：
   - **すべての保護機能**この除外は、**マルウェアスキャンの除外リスト** の影響を受けるすべての保護コンポーネントに適用されます。
   - **選択した保護機能**除外を適用するコンポーネントを選択します：ファイル脅威対策、アンチクリプター、脆弱性攻撃ブロック。
9. 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。

コマンドラインで保護の除外を追加する方法

1. パスによる除外を追加するには、次のコマンドを実行します：

```
kesl-control --set-settings 1 --add-exclusion <path>
```

2. マスクによる除外を追加するには、次の手順を実行します：
   a. マスクによるファイルの除外を有効にします：

```
kesl-control --set-settings 1 UseExcludeMasks=Yes
```

b. ファイルマスクを追加します：

```
kesl-control --set-settings 1 ExcludeMasks.item_#=<file mask>
```

3. 脅威名による除外を追加するには、次の手順を実行します：

a. 脅威名によるファイルの除外を有効にします：

```
kesl-control --set-settings 1 UseExcludeThreats=Yes
```

b. 脅威名を追加します：

```
kesl-control --set-settings 1 ExcludeThreats.item_#=<threat name>
```

4. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 1
```

記号

コマンドオプション

設定	説明
`--add-exclusion`	ディレクトリをスキャン対象から除外します。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。
`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。シェル形式のマスクを使用してファイル名を入力します。例： `ExcludeMasks.item_0000=*_my_file_??.html`
`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。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。例： `ExcludeThreats.item_0000=EICAR-Test-*`

信頼する URL を追加する方法

悪意のある Web サイトやフィッシング Web サイトのほかにも Web サイトをブロックすることができます。例えば、ウェブ脅威対策は RFC 標準に適合しない HTTP トラフィックをブロックします。コンテンツが信頼できる Web サイトのリストを作成できます。ウェブ脅威対策は、信頼する URL からの情報にウイルスおよびその他の脅威が含まれるかどうかを分析しません。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、このオプションを使用してください。

Web コンソールで信頼する URL を追加する方法

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**］タブを選択します。

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. ［**信頼ゾーン**］に移動します。

5. 表示されたウィンドウで、［**Web アドレス**］をクリックします。
   信頼する URL のリストを含むウィンドウが開きます。

6. 信頼するコンテンツを含む URL / Web サイトのリストを作成します。
   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 URL のリストを JSON ファイルからインポートすることもできます。

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。

コマンドラインで信頼する URL を追加する方法

1. 信頼する URL のリストを有効にするには、次のコマンドを実行します：

```
kesl-control --set-settings 14 UseTrustedAddresses=Yes
```

2. 信頼する URL を追加するには、次のコマンドを実行します：

```
kesl-control --set-settings 14 TrustedAddresses.item_#=<trusted web address>
```

3. コンポーネント設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 14
```

例

```
kesl-control --set-settings 14 TrustedAddresses.item_001=https://example.com/
```

コンピューターの信頼する IP アドレスを追加する方法

Kaspersky Endpoint Security はネットワーク攻撃を認識し、パケット数の大きな保護されていないネットワーク接続（監視カメラなど）をブロックすることができます。信頼するデバイスについては、除外リストにデバイスの IP アドレスを追加できます。信頼する URL は、ネットワーク脅威対策コンポーネントに影響します。

Web コンソールでブロックから除外するアドレスを設定するには

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**］タブを選択します。

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. ［**信頼ゾーン**］に移動します。

5. 表示されたウィンドウで、［**IP アドレス**］をクリックします。
   信頼する IP アドレスのリストを含むウィンドウが開きます。

6. 表示されたウィンドウで、［**追加**］をクリックします。

7. ネットワーク攻撃防御の対象にしないコンピューターの IP アドレスを入力します。
   必要に応じて、サブネットを指定します。

8. 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。

コマンドラインでブロックから除外するアドレスを設定するには

1. 信頼する IP アドレスを適用するには、次のコマンドを実行します：

```
kesl-control --set-settings 17 UseExcludeIPs=Yes
```

2. 信頼する IP アドレスを追加するには、次のコマンドを実行します：

```
kesl-control --set-settings 17 ExcludeIPs.item_#=<IP address>
```

3. 信頼する IP アドレスのリストをスキャンするには、次のコマンドを実行します：

```
kesl-control --get-settings 17 TrustedIPAddresses
```

例

```
kesl-control --set-settings 17 ExcludeIPs.item_0000="192.168.2.0/24"
```

監視するネットワークポートを選択する方法

Kaspersky Endpoint Security は、特定のプロトコルを介して送信され、ユーザーのコンピューター上の特定の開いている TCP ポートを通過するデータストリームを監視します。既定では、本製品は既知の登録済みポートを監視します。たとえば、HTTPS 接続用のポート 443、IMAP メールプロトコル用のポート 143 などです。

*信頼するネットワークポート*は、ネットワーク脅威対策コンポーネントによるスキャンの対象から除外されるネットワークポートです。これは、Kaspersky Endpoint Security を信頼するサードパーティのサービスやアプリケーションと互換性があるように設定し、パフォーマンスを最適化するために必要です。たとえば、内部バックアップサービス用のネットワークポートを指定して、バックアップコピーのダウンロードまたはアップロードが本製品によって妨げられないようにすることができます。

ネットワークポートをスキャン対象から除外すると、デバイスの保護レベルが低下することに留意してください。除外は最小限に抑えるようにしてください。

Web コンソールでネットワークポートをスキャン対象から除外する方法

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. ［**信頼ゾーン**］→［**ネットワークポート**］に移動します。
   監視対象のネットワークポートのリストを含むウィンドウが開きます。

5. スキャン対象から除外するポートのトグルスイッチを無効にします。
   必要なポートがリストにない場合、本製品はそのポートをスキャンしていません。

6. 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。

コマンドラインでネットワークポートをスキャン対象から除外する方法

1. 次のコマンドを実行して、監視対象のポートのリストを取得します：

```
kesl-control --get-net-setting
```

2. すべてのポートの監視が有効になっている場合（`MonitorNetworkPorts=All`）、次のコマンドを実行します：

```
kesl-control --set-net-settings MonitorNetworkPorts=Selected
```

   これにより、監視対象のネットワークポートを含む `[NetworkPorts.item_#]` セクションが追加されます。

3. セクションにスキャン対象から除外するポートが含まれている場合は、次の手順に従います：

   a. 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-setting --file <path to file>
```

   b. このファイルで、監視対象から除外するネットワークポートを含む `[NetworkPorts.item_#]` セクションを削除します。

   c. 設定を適用するには、次のコマンドを実行します：

```
kesl-control --set-net-settings --file <path to file>
```

   変更した設定が本製品にインポートされます。

信頼するルート証明書のリストに証明書を追加する方法

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。

信頼するルート証明書は、次のコンポーネントで使用されます：

- ウェブ脅威対策
- メール脅威対策
- ウェブコントロール

CER、CRT、PEM、DER 形式の信頼する証明書がサポートされています。信頼する証明書の最大ファイルサイズは 2 MB です。

Web コンソールで信頼するルート証明書をインストールする方法

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. ［**信頼ゾーン**］→［**ルート証明書**］に移動します。
   信頼するルート証明書のリストを含むウィンドウが開きます。
5. ［**追加**］をクリックします。
   証明書を追加するためのフォームが開きます。
6. 証明書をアップロードします。
7. 必要に応じて、**コメント** フィールドに証明書の説明を入力します。
8. 変更内容を保存します。

信頼済み証明書のリストでは、シリアル番号が証明書名として使用されます。

コマンドラインで信頼するルート証明書をインストールする方法

1. 証明書を追加するには、次のコマンドを実行します：

   ```
   kesl-control --add-certificate <path to certificate>
   ```

2. 信頼するルート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

3. リストから証明書を削除するには、次のコマンドを実行します：

```
kesl-control --remove-certificate <certificate subject>
```

信頼するドメインを追加する方法

Kaspersky Endpoint Security には、暗号化された接続をスキャンしない信頼するドメインのリストがあります。信頼するドメインは、ウェブ脅威対策およびウェブコントロールに影響します。ドメインをスキャン対象から除外すると、既知のソースからのトラフィックがブロックされるのを防ぐことができます。

ドメイン名を指定します。`example.com/*` や `https://example.com` などの URL は無視されます。

Web コンソールで信頼するドメインを指定する方法

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. ［**信頼ゾーン**］→［**信頼するドメイン**］に移動します。
   信頼するドメインのリストを含むウィンドウが開きます。
5. ［**追加**］をクリックします。
   ドメインを追加するためのフォームが開きます。
6. ドメイン名またはドメインマスクを指定します。例：「`*example.com`」。
7. 変更内容を保存します。

コマンドラインで信頼するドメインを指定する方法

1. ドメインを追加するには、次のコマンドを実行します。

```
kesl-control --set-net-settings ManageExclusions=Yes Exclusions.item_#.DomainName=<domain name>
```

2. 設定をテストするには、次のコマンドを実行します。

```
kesl-control --get-net-settings
```

   信頼するドメインは、`[Exclusions.item_#]` セクションに列挙する必要があります。

例

```
kesl-control --set-net-settings Exclusions.item_0000.DomainName=example.com
```

マウントポイントを除外する方法

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。このような除外は*グローバル除外*と呼ばれます。アプリケーションは、デバイスにマウントされている信頼するローカルまたはリモートディレクトリを、スキャンおよびファイル操作のインターセプトの対象から除外します。たとえば、一時ファイルを含むマウントポイントを除外して、システムの負荷を軽減し、スキャンを早く完了させることができます。

マウントポイントの除外は、次のコンポーネントに影響します：

- ファイル脅威対策
- アンチクリプター
- コンテナスキャン

信頼するマウントポイントは、次のタスクによるスキャンからも除外されます：

- マルウェアのスキャン
- 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

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。

Web コンソールで信頼するマウントポイントを指定する方法

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. ［**信頼ゾーン**］→［**マウントポイント**］に移動します。
   信頼するマウントポイントのリストを含むウィンドウが開きます。
5. ［**追加**］をクリックします。
   マウントポイントを追加するためのフォームが開きます。
6. ファイルシステムのドロップダウンリストで、除外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します：**ローカル**、**マウント済み**、**リモートでマウント済みのすべての場所**。

Kaspersky Endpoint Security は、リモートディレクトリに対して Samba および NFS プロトコルをサポートしています。

> 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。

7. 除外するディレクトリが含まれているファイルシステムの名前を入力します。
8. 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。

コマンドラインで信頼するマウントポイントを指定する方法

1. ディレクトリがマウントポイントでない場合は、次のコマンドを実行して、そのディレクトリからマウントポイントを作成します：

```
mount --bind <path to dir> <path to dir>
```

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：

```
<path to dir> <path to dir> none defaults,bind 0 0
```

3. Kaspersky Endpoint Security を再起動します：

```
systemctl restart kesl
```

4. 信頼するマウントポイントを追加するには、次のコマンドを実行します：

```
kesl-control --set-app-settings ExcludedMountPoint.item_#=<path to mount point>
```

5. グローバル除外を適用するには、アプリケーションを再起動します：

```
systemctl restart kesl
```

例

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/tmp"
```

信頼するアプリケーションを追加する方法

*信頼するアプリケーションのリスト*は、Kaspersky Endpoint Security がファイルとプロセスのアクティビティ（悪意のあるアクティビティを含む）またはプロセスのメモリを監視しないアプリケーションのリストです。既定では、Kaspersky Endpoint Security は、任意のアプリケーションプロセスによって開かれる、実行される、または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のアクティビティを制御します。

信頼するアプリケーションは、次のコンポーネントに影響します：

- ファイル脅威対策
- ふるまい検知

また、プロセスメモリのスキャンの除外にも影響します。

Web コンソールで信頼するアプリケーションを指定する方法

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. ［**信頼ゾーン**］→［**信頼するアプリケーション**］に移動します。
   信頼するアプリケーションのリストを含むウィンドウが開きます。
5. 組織内のすべてのコンピューターの信頼するアプリケーションのリストを作成する場合は［**継承時に値を統合する**］をオンにします。親ポリシーおよび子ポリシー内の信頼するアプリケーションのリストが結合されます。親ポリシーのアプリケーションは、子ポリシーでは表示のみ可能で、変更または削除はできません。

   リストをマージするには、親ポリシー設定の継承を有効にする必要があります。

6. ［**追加**］をクリックします。
   アプリケーションを追加するためのフォームが開きます。
7. アプリケーションのパスまたはパスマスクを指定します。
8. 信頼するアプリケーションの設定を指定します：
   - **アプリケーションがファイルを開く前にスキャンしない**アプリケーションが開いたファイルはすべて Kaspersky Endpoint Security のスキャンの対象外になります。
   - **アプリケーションの動作を監視しない**Kaspersky Endpoint Security は、オペレーティングシステム内の信頼するアプリケーションのファイルアクティビティとネットワークアクティビティを監視しません。
     ［**Managed Detection and Response および Endpoint Detection and Response を監視しない**］チェックボックスをオンにして、MDR および EDR (KATA) コンポーネントのアプリケーションアクティビティの監視を個別に設定することもできます。
   - **子アプリケーションの動作を監視しない**Kaspersky Endpoint Security は、信頼するアプリケーションによって起動されたアプリケーションのファイルアクティビティとネットワークアクティビティを監視しません。
   - **指定したアプリケーションのメモリをスキャンしない**Kaspersky Endpoint Security は、信頼するアプリケーションによって生成されたプロセスのメモリをスキャンしません。

Web コンソールでは、Kaspersky Endpoint Security for Linux に対して［**コメント**］設定は使用できません。

9. 変更内容を保存します。

コマンドラインで信頼するアプリケーションを指定する方法

1. 信頼するアプリケーションのファイルアクティビティをスキャン対象から除外するには、次のコマンドを実行します：

```
kesl-control --set-settings 1 ExcludedForProgram.item_#.UseExcludedForProgram=Yes
ExcludedForProgram.item_#.ProgramPath=<path to app> ExcludedForProgram.item_#.AreaDesc=<trusted app name>
[ExcludedForProgram.item_#.ApplyToDescendants=Yes]
```

2. 信頼するアプリケーションのプロセスアクティビティをスキャン対象から除外するには、次のコマンドを実行します：

```
kesl-control --set-set 20 UseTrustedPrograms=Yes TrustedPrograms.item_#.UseTrustedProgram=Yes
TrustedPrograms.item_#.ProgramPath=<path to app> TrustedPrograms.item_#.ProgramDesc=<trusted app name>
[TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes] [TrustedPrograms.item_#.ApplyToDescendants=Yes]
```

3. 信頼するアプリケーションのプロセスのメモリをスキャン対象から除外するには、次のコマンドを実行します：

```
kesl-control --set-app-settings MemScanExcludedProgramPath.item_#=<path to app>
```

記号

コマンドオプション

設定	説明
`ExcludedForProgram.item_#.UseExcludedForProgram=Yes`	信頼するアプリケーションのファイルアクティビティを、ファイル脅威対策コンポーネントによるスキャンから除外します。
`ExcludedForProgram.item_#.ProgramPath`	ID `#` の信頼するアプリケーションへのパス。ファイル脅威対策コンポーネントは、指定されたアプリケーションのプロセスをスキャンしません。 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。
`ExcludedForProgram.item_#.AreaDesc`	ID `#` の信頼するアプリケーション名。
`ExcludedForProgram.item_#.ApplyToDescendants=Yes`	信頼するアプリケーションの子プロセスを、ファイル脅威対策コンポーネントによるスキャンから除外します。
`UseTrustedPrograms=Yes`	信頼するアプリケーションのプロセスのアクティビティを、ふるまい検知コンポーネントによるスキャンから除外します。
`TrustedPrograms.item_#.UseTrustedProgram=Yes`	ID `#` の信頼するアプリケーションのアクティビティをスキャンから除外します。
`TrustedPrograms.item_#.ProgramPath`	ID `#` の信頼するアプリケーションへのパス。ふるまい検知コンポーネントは、指定されたアプリケーションのプロセスをスキャンしません。 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。
`TrustedPrograms.item_#.ProgramDesc`	ID `#` の信頼するアプリケーション名。

設定	説明
`TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes`	Managed Detection and Response および Endpoint Detection and Response Expert（オンプレミス）コンポーネントによるテレメトリ収集から、信頼するアプリケーションのアクティビティを除外します。
`TrustedPrograms.item_#.ApplyToDescendants=Yes`	信頼するアプリケーションの子プロセスを、ふるまい検知コンポーネントによるスキャンから除外します。
`MemScanExcludedProgramPath.item_#`	ID `#` の信頼するアプリケーションへのパス。本製品は、信頼するアプリケーションのプロセスのメモリをチェックしません。

信頼するデバイスを追加する方法

「*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。たとえば、組織でリムーバブルドライブの使用を許可していないが、管理者が仕事でリムーバブルドライブを使用している場合、管理者グループのみにリムーバブルドライブを許可できます。これを行うには、信頼するリストにリムーバブルドライブを追加し、ユーザーのアクセス許可を設定します。

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。

- **ID**各デバイスには固有の識別子（Hardware ID、または HWID）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。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。

- **ID マスクによる指定**。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*`」。

Kaspersky Security Center Web コンソールで信頼するデバイスを追加する方法

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. ［**デバイスコントロール**］→［**信頼するデバイス**］に移動します。

   信頼するデバイスのリストを含むウィンドウが開きます。

5. ［**追加**］をクリックします。

   デバイスを追加するためのフォームが開きます。

6. ［**ユーザーまたはグループ**］で、このデバイスを信頼するデバイスとみなす対象となるユーザーまたはユーザーグループを指定します。

   Kaspersky Security Center のアカウントのリストでユーザーを選択するか、ローカルユーザー名を手入力して選択できます。ローカルユーザーアカウントを使用するのは、ドメインユーザーアカウントを使用できない特別な状況のみにすることを推奨します。

既定では、信頼するデバイスへのアクセスは Everyone グループに対して許可されます。

7. ［**デバイス種別**］で、ドロップダウンリストからデバイス種別を選択します（たとえば、［**リムーバブルドライブ**］）。

8. ID マスクに基づいてデバイスを追加する場合は、［**マスクを使用**］チェックボックスをオンにします。

9. ［**信頼するデバイスの検索**］フィールドに、デバイス ID または ID マスクを入力します。
   テーブルには、定義された基準を満たすデバイスのリストが表示されます。

10. 信頼するデバイスのリストに追加する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。

11. 必要に応じて、［**コメント**］タブで、デバイスが信頼リストに追加された理由を説明します。

12. 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。

コマンドラインで信頼するデバイスを追加する方法

1. 信頼する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 <device ID>
```

2. コンポーネントの信頼するデバイスのリストをスキャンするには、次のコマンドを実行します：

```
kesl-control --trusted-devices --list
```

例

```
kesl-control --trusted-devices --add WDC_C*
```

全般設定

検知の設定

他の種類のオブジェクトの検知

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。

コンピューターまたはユーザー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の検知を追加で有効にできます。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の検知を Web コンソールで設定する方法

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. ［**全般設定**］→［**検知の設定**］に移動します。
5. ［**その他の種別のオブジェクトの検知**］ブロックで、［**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ソフトウェア**］をオンにします。
6. 変更内容を保存します。

検知の設定

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の検知をコマンドラインで設定する方法

1. デバイスやデータに損害を与える目的で攻撃者が悪用する可能性があるアプリケーションの検知を設定するには、本製品の保護コンポーネントに対して次のコマンドを実行します：

```
kesl-control --set-app-settings DetectOtherObjects=<Yes|No>
```

2. 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含む URL のデータベースとリンクを照合するには、ウェブ脅威対策コンポーネントで次のコマンドを実行します：

```
kesl-control --set-settings 14 CheckOther=<Yes|No>
```

3. 現在のアプリケーション設定を確認するには、次のコマンドを実行します：

```
kesl-control --get-app-settings
```

4. ウェブ脅威対策の現在の設定を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 14
```

イベントログの設定

既定では、Kaspersky Endpoint Security は、パックされたオブジェクトおよび感染していないオブジェクトの処理に関するイベントや、ファイル脅威対策コンポーネントで処理されなかったオブジェクトに関するイベントをログに記録しません。

このようなイベントのログ記録を有効にすると、アプリケーションで *圧縮されたオブジェクトが検知されました*、*オブジェクトが処理されていません*、*処理済みオブジェクト* の各イベントが生成されるようになります。このようなイベントは、コンポーネントの設定時だけでなく、本製品のデバッグやトラブルシューティングにも役立ちます。これにより、このようなオブジェクトが本製品によってスキャンされており、エラーによってスキップされていないことを確認できます。

Web コンソールでオブジェクトの処理に関するイベントの記録を有効にする方法

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. ［**全般設定**］→［**検知の設定**］に移動します。
5. **オブジェクトの記録設定**で、該当するイベント種別の横にあるチェックボックスをオンにします。
   - **感染していないオブジェクトを記録する**
   - **処理されていないオブジェクトを記録する**
   - **圧縮されたオブジェクトを記録する**
6. 変更内容を保存します。

コマンドラインでオブジェクトの処理に関するイベントの記録を有効にする方法

1. 感染していないオブジェクトに関するイベントを記録するには、次のコマンドを実行します：

```
kesl-control --set-settings 1 ReportCleanObjects=Yes
```

2. 未処理のオブジェクトに関するイベントを記録するには、次のコマンドを実行します：

```
kesl-control --set-settings 1 ReportUnprocessedObjects=Yes
```

3. 圧縮されたオブジェクトに関するイベントを記録するには、次のコマンドを実行します：

```
kesl-control --set-settings 1 ReportPackedObjects=Yes
```

4. ファイル脅威対策の設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-settings 1
```

Kaspersky Security Network

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を含む ksn_license.<language ID> ファイルは、アプリケーションの配布パッケージに含まれており、/opt/kaspersky/kesl/doc ディレクトリにあります。

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

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 Private Security Network

Kaspersky Private Security Network は、オブジェクト（ファイルまたは Web アドレス）の評価をチェックするためのローカルの評価データベースです。ローカルの評価データベースに追加されたオブジェクトの評価は KSN または KPSN に追加されたものより優先度は高くなります。たとえば、Kaspersky Endpoint Security がコンピューターをスキャン中に KSN または KPSN に評価を要求したとします。あるファイルに対して、ローカルの評価データベースに「*ブロック*」という評価があり、KSN または KPSN に「*信頼済み*」という評価があった場合、Kaspersky Endpoint Security はファイルを「*ブロック*」と判断して検出し、検知された脅威に対して定義された操作を実行します。

しかし、Kaspersky Endpoint Security が KSN または KPSN にオブジェクトの評価を要求しないこともあります。この場合、Kaspersky Endpoint Security KPSN のローカル評価データベースからデータを受け取りません。Kaspersky Endpoint Security は次の理由で KSN または KPSN にオブジェクトの評価を要求しないことがあります：

- カスペルスキー製品がオフラインの評価データベースを使用している。オフラインの評価データベースは、カスペルスキー製品の動作中にリソースの最適化をするため、またコンピューター上の特に重要なオブジェクトを保護するために設計されています。オフライン評価データベースは、Kaspersky Security Network のデータに基づいてカスペルスキーによって作成されています。カスペルスキー製品は特定のアプリケーションの定義データベースがアップデートされる際にあわせてオフラインの評価データベースをアップデートします。オフラインの評価データベースにスキャンされるオブジェクトに関する情報が存在する場合、製品は KSN または KPSN にこのオブジェクトの評価を要求しません。

- スキャンの除外リスト（信頼ゾーン）は製品の設定で指定されます。該当する場合、製品はローカルの評価データベースのオブジェクトの評価を判断に使用しません。

- アプリケーションは、iChecker や KSN / KPSN への評価要求のキャッシュなどのスキャン最適化技術を使用します。この場合は製品が以前にスキャンしたオブジェクトの評価を要求しません。

- 負荷を最適化するため、本製品は特定の形式またはサイズのファイルのみスキャンします。対応する形式およびサイズの制限はカスペルスキーによって定義されています。リストは本製品のウイルス定義データベースとあわせてアップデートされます。たとえば、ファイル脅威対策機能など、スキャンの最適化の設定を製品インターフェイスから設定することも可能です。

- Kaspersky Endpoint Security は、Light Agent モードで、KSN プロキシサーバーを介して KSN サーバーと通信します。KSN との直接通信には対応していません。

Kaspersky Security Network を有効または無効にする方法

既定では、拡張 KSN モードが使用されます。*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。

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。

Web コンソールで KSN を有効または無効にする方法

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. ［**全般設定**］→［**Kaspersky Security Network**］に移動します。

5. ［**Kaspersky Security Network（KSN）の使用**］トグルスイッチを使用して、コンポーネントを有効または無効にします。

6. KSN の使用を有効にすると、［**Kaspersky Security Network に関する声明**］ウィンドウが開きます。
   Kaspersky Security Network（KSN）に関する声明の条項に同意する場合は、内容を確認した上で同意してください。

7. 必要に応じて、［**拡張 KSN モードを使用する**］チェックボックスをオンまたはオフにします。

8. 変更内容を保存します。

Kaspersky Security Network

コマンドラインで KSN を有効または無効にする方法

1. Kaspersky Security Network のステータスを確認します：

```
kesl-control --app-info
```

本製品では、**Kaspersky Security Network の使用** 行に KSN のステータスが表示されます：

- **無効**
- **基本 KSN モード**
- **拡張 KSN モード**

2. Kaspersky Security Network の標準モードを有効にするには、次のコマンドを実行します：

```
kesl-control --set-app-settings UseKSN=Basic --accept-ksn
```

3. Kaspersky Security Network の拡張モードを有効にするには、次のコマンドを実行します：

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

4. Kaspersky Security Network 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
```

製品インターフェイスで KSN の使用を有効または無効にする方法

1. メインウィンドウを開きます。
2. メインウィンドウの下部にある［**設定**］をクリックします。
3. 表示されたウィンドウで、次のいずれかのオプションを選択します：
   - ［**拡張 KSN モード**］：Kaspersky Security Network を使用し、ナレッジベースから情報を取得して、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場合。
   - ［**基本 KSN モード**］：Kaspersky Security Network を使用し、ナレッジベースから情報を取得するが、脅威の種別や発生源に関する統計や情報を匿名で送信しない場合。
4. ［**有効にする**］をクリックします。
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、次のいずれかのオプションを選択します：
   - **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**
   - **Kaspersky Security Network に関する声明の条項に同意しない**
6. ［**OK**］をクリックします。

KSN の使用を有効にすると、Kaspersky Endpoint Security は Kaspersky Security Network から受け取ったファイル、Web リソース、アプリケーションの評価に関する情報を使用します。

Kaspersky Endpoint Security は、外部サービスとの通信に次のネットワーク設定を使用します：

アドレス	プロトコル	ポート
ds.kaspersky.com	HTTPS	443
ksn-a-stat-geo.kaspersky-labs.com	KSN	443, 1443
ksn-file-geo.kaspersky-labs.com	KSN	443, 1443
ksn-verdict-geo.kaspersky-labs.com	KSN	443, 1443
ksn-url-geo.kaspersky-labs.com	KSN	443, 1443
ksn-a-p2p-geo.kaspersky-labs.com	KSN	443, 1443
ksn-cinfo-geo.kaspersky-labs.com	KSN	443, 1443

アプリケーションのクラウドモードとは

*クラウドモード*では、Kaspersky Endpoint Security は軽量版の定義データベースを使用するため、コンピューターの RAM への負荷が約半分になります。

クラウドモードは、Kaspersky Security Network が有効な場合にのみ使用できます。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。クラウドモードは既定で有効になっています。

本製品が Light Agent モードで動作している場合、クラウドモードは使用できません。

Web コンソールでクラウドモードを有効または無効にする方法

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. ［**全般設定**］→［**Kaspersky Security Network**］に移動します。
5. ［**クラウドモードを使用**］トグルスイッチを使用して機能を有効または無効にします。
6. 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。

コマンドラインでクラウドモードを有効または無効にする方法

1. 本製品の現在の状態を確認するには、本製品の全般設定を表示するコマンドを実行します：

   ```
   kesl-control --get-app-settings
   ```

   本製品の状態は、`CloudMode` 行に表示されます。

2. クラウドモード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 CloudMode=<Yes|No>
   ```

次のアップデートから、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。

軽量なバージョンの定義データベースが使用できない場合、通常のバージョンの定義データベースに自動的に切り替えられます。

KSN プロキシの目的とは

Kaspersky Security Center 管理サーバーによって管理されるクライアントコンピューターは、直接、または KSN Proxyサービス経由で KSN と連携できます。

> 本製品が Light Agent モードで実行されている場合、KSN との直接通信はサポートされません。Kaspersky Endpoint Security は、KSN プロキシサーバーを使用して KSN サーバーと連携します。

KSN Proxy サービスは次の機能を提供します：

- ユーザーのコンピューター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 Proxy は処理データをキャッシュすることにより、外部ネットワークとの通信チャネルの負荷を軽減し、クライアントコンピューターによって要求される情報の受信を高速化します。

既定では、KSN を有効にして KSN 声明に同意すると、本製品はプロキシサーバーを使用して Kaspersky Security Network. に接続します。本製品が使用するプロキシサーバーは TCP ポート 13111 を介した Kaspersky Security Center 管理サーバーです。

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。

コマンドラインを使用して KSN プロキシサーバーへの接続設定を構成することはできません。

Web コンソールでプロキシサーバー経由の KSN 接続を設定する方法

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. ［**全般設定**］→［**Kaspersky Security Network**］に移動します。
5. ［**管理サーバーを KSN プロキシサーバーとして使用する**］チェックボックスを使用して、KSN プロキシの使用を有効または無効にします。
6. 必要に応じて、［**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**］チェックボックスをオンまたはオフにします。既定では、このチェックボックスはオンです。
   このオプションを有効にすると、Kaspersky Endpoint Security は KSN プロキシサービスを使用できない場合に、KSN サーバーを直接使用します。KSN サーバーは、カスペルスキー側に配置されている場合と、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。
7. 変更内容を保存します。

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で隔離されたファイルを表示する方法

クライアントデバイス上のカスペルスキー製品によって隔離されたファイルの一覧は、Kaspersky Security Center に保存されます。

1. Web コンソールのメインウィンドウで、［**操作**］→［**リポジトリ**］の順に選択します。
2. ［**隔離**］フォルダーに移動します。
3. 隔離されたオブジェクトに関する情報が、コンソールの右側のペインに表示されます。

クライアントデバイスでバックアップ内のファイルを表示する方法

クライアントデバイス上のカスペルスキー製品によってバックアップに配置されたファイルの一覧は、Kaspersky Security Center に保存されます。

1. Web コンソールのメインウィンドウで、［**操作**］→［**リポジトリ**］の順に選択します。
2. ［**ファイルのバックアップ**］フォルダーに移動します。
3. バックアップに配置されたオブジェクトに関する情報が、コンソールの右側のペインに表示されます。

アクティブな脅威のリスト内の未処理ファイルに関する情報を表示する方法

1. Web コンソールのメインウィンドウで、［**操作**］→［**リポジトリ**］の順に選択します。
2. ［**アクティブな脅威**］フォルダーに移動します。
3. アクティブな脅威のリスト内の未処理ファイルに関する情報が、コンソールの右側のペインに表示されます。

クライアントデバイスに接続されているハードウェアに関する情報を表示する方法

1. Web コンソールのメインウィンドウで、［**操作**］→［**リポジトリ**］の順に選択します。
2. ［**ハードウェア**］フォルダーに移動します。
3. デバイスに関する情報が、コンソールの右側のペインに表示されます。

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のアプリケーションに関する情報を表示する方法

1. Web コンソールのメインウィンドウで、［**操作**］→［**サードパーティ製アプリケーション**］の順に選択します。
2. ［**アプリケーションレジストリ**］フォルダーに移動します。
3. アプリケーションに関する情報が、コンソールの右側のペインに表示されます。

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。

管理サーバーとの連携を設定する方法

ポリシーのプロパティで管理サーバーとの連携を設定するには：

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. ［**全般設定**］→［**KSC 連携**］に移動します。
5. ［**詳細設定**］リンクをクリックします。

6. 管理サーバーに情報を転送する必要がある、クライアントコンピューター上のイベントのカテゴリを選択します：

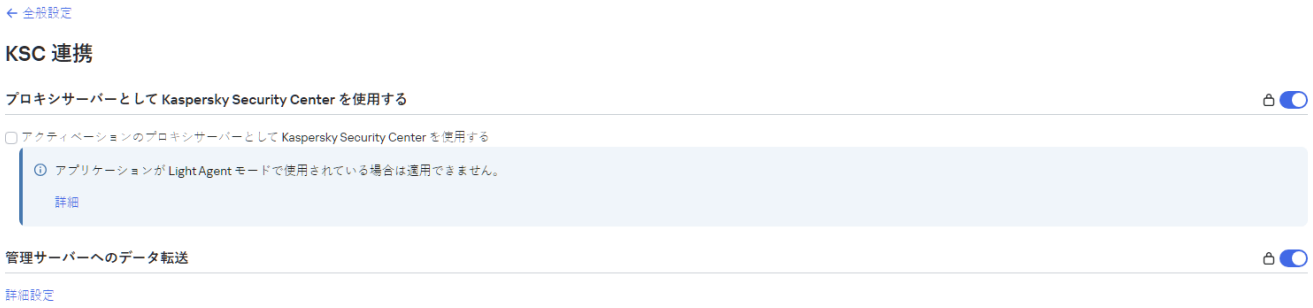
- **隔離内のファイルについて** このチェックボックスでは、隔離されたファイルに関するデータを管理サーバーに送信するかどうかを選択します。
- **バックアップにあるファイルについて**。このチェックボックスでは、バックアップされているファイルについてのデータを管理サーバーに送信するかどうかを選択します。
- **処理されていないファイルについて**。このチェックボックスでは、スキャン中に処理されなかったファイルに関する通知を管理サーバーに送信するかどうかを選択します。
- **インストールされているデバイスについて**。このチェックボックスは、クライアントデバイスにインストールされている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。
- **起動され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。

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。

管理対象デバイスのプロパティで管理サーバーとの連携を設定するには：

1. Web コンソールのメインウィンドウで、［**アセット管理**］ →［**アセット（デバイス）**］→［**管理対象デバイス**］の順に選択します。
2. ［**<device name>**］リンクをクリックします。
3. ［**アプリケーション**］タブを選択し、［**Kaspersky Endpoint Security**］リンクをクリックします。
4. ［**アプリケーション設定**］タブで、［**ストレージ設定**］セクションに移動します。
5. ［**管理サーバーへのデータ転送設定**］で、［**設定**］をクリックします。
6. ［**データ転送設定**］ウィンドウで、管理サーバーへの情報の送信を有効または無効にできます：
   - **バックアップ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、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。
   - **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。
   - **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。
   - **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。
   - **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。

7. 変更内容を保存します。



アプリケーション起動の設定方法

本製品の起動の設定

Kaspersky Endpoint Security では、起動に失敗する最大回数と起動タイムアウトを設定できます。これにより、本製品を長時間起動できない場合にシステムへの負荷を軽減できます。既定では、本製品の起動に連続して失敗する最大回数は 5 回、最大タイムアウトは 3 分です。

Web コンソールで本製品の起動を設定する方法

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. ［**全般設定**］→［**ユーザーインターフェイス**］に移動します。
5. ［**アプリケーションの起動設定**］で、次のフィールドに値を入力します：
   - **アプリケーションの起動失敗の最大試行回数**既定値：5
   - **アプリケーションの起動を待つ時間（分）**既定値：3
6. 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。

コマンドラインで本製品の起動を設定する方法

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

重要なアップデートの適用

製品のインストール後、最初の24時間が経過した後に重要なアップデートを受信した場合に、製品が自動的に再起動するように設定できます。インストール後最初の 24 時間は、重要なアップデートを受信すると、追加の設定なしで本製品が自動的に再起動します。

Web コンソールで製品の自動再起動を設定するには

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. ［**全般設定**］→［**ユーザーインターフェイス**］に移動します。
5. ［**緊急アップデートの適用**］ブロックで、［**緊急アップデートを受信した時に本製品を自動的に再起動する**］をオンにします。
   Kaspersky Endpoint Security は、インストールから1日後に重要なアップデートを受信すると再起動します。
6. 変更内容を保存します。

コマンドラインで本製品の自動再起動を設定する方法

全般設定の `UrgentUpdateRestartEnabled` 設定を使用して、コマンドラインで製品の自動再起動を設定できます。

重要なアップデートをインストールするときに製品を自動的に再起動するには、次のコマンドを実行します：

```
kesl-control --set-app-settings UrgentUpdateRestartEnabled=Yes
```

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、編集、作成、削除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）の各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 コンソールでタスク管理権限を設定するには：

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. ［**全般設定**］→［**ユーザーインターフェイス**］に移動します。
5. ［**許可された操作**］で、ユーザーにデバイスでの実行を許可する操作を選択します：
   - **ローカルタスクへのアクセス**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。これが他のポリシー制限によって禁止されていない場合、ユーザー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、利用可能なローカルタスクを設定、実行、作成、削除できます。
   - **グループタスクを管理する**このチェックボックスをオンにすると、ユーザーは Kaspersky Security Center で設定されたグループタスクをクライアントデバイスで管理できます。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から実行できます。
6. 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。

パスワードによる保護

パスワードによる保護を使用すると、付与された権限（たとえば、アプリケーションレポートの表示権限）に従って、ユーザーによる Kaspersky Endpoint Security の変更を制限できます。アプリケーション設定へのアクセスを制限することで、アプリケーションに対する不正な変更や意図しない変更のリスクを軽減できます。

パスワードによる保護の仕組み

1. **ユーザーがコンポーネントによって制御される操作を実行しようとします**

   たとえば、保護コンポーネントを無効にしたり、Kaspersky Endpoint Security のレポートを表示したりする操作です。

2. **Kaspersky Endpoint Security がユーザー権限を確認します**

   ユーザーに対応する権限がある場合、操作は正常に実行されます。ユーザーに対応する権限がない場合、アプリケーションは操作をブロックし、エラーを表示します。

   Kaspersky Endpoint Security のグラフィカルインターフェイスでは、禁止された操作は表示も編集もできません。

パスワードによる保護を設定する

1. **パスワードによる保護を有効にする**

   既定では、パスワードによる保護は無効になっています。Web コンソールまたは管理コンソールで、またはコマンドラインで次のコマンドを使用して、コンポーネントを有効にします：

   ```
   kesl-control --set-permission-manager-settings Enabled=Yes
   ```

2. **ユーザー権限を設定する**

   既定では、アプリケーションには定義済みユーザーグループ（*kesladmin*、*kesluser*、*keslaudit*）のユーザー権限が設定されています。

   これらのグループのユーザー権限を設定するか、新しいユーザーまたはユーザーグループを作成します。

   > アプリケーションを正しく動作させるために、少なくとも 1 つのグループに対して権限を設定することを推奨します。

   Web コンソールでカスタム権限を設定する方法

   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. ［**全般設定**］→［**セルフディフェンス**］に移動します。
   5. コンポーネントのトグルスイッチが **パスワードによる保護は有効です** の位置にあることを確認します。
   6. ［**ユーザー権限**］リンクをクリックします。
      ユーザーとその権限が表示されたウィンドウが開きます。
   7. 定義済みグループの権限を変更する場合は、グループ名をクリックします。
      別のユーザーまたはグループの権限を変更する場合は、次の操作を行います：
      a. ［**追加**］をクリックします。
      b. Active Directory からユーザーまたはグループを選択するか、名前を手動で入力します。
   8. ユーザーまたはグループに付与する権限の横にあるチェックボックスをオンにします。

9. 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。

セルフディフェンス

コマンドラインでカスタム権限を設定する方法

1. 現在のパスワードによる保護設定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-permission-manager-settings
```

2. ユーザーまたはグループの権限を変更するには、次のコマンドを実行します：

```
kesl-control --set-permissions <principal> [--group] <permissions>=<Yes|No> [--file <file name>] [--
json]
```

3. 権限が設定されているユーザーまたはグループを削除するには、次のコマンドを実行します：

```
kesl-control --remove-permissions <principal> [--group]
```

記号

コマンドオプション

設定	説明
`--group`	この設定はグループに適用されます。 `--group` オプションが指定されていない場合、この設定は個々のユーザーに適用されます。
`--file <file name>`	パラメータをファイルに出力するか、ファイルからパラメータをインポートします。 `<file name>` を入力します。
`--json`	パラメータを JSON ファイルに出力するか、JSON ファイルからパラメータをインポートします。 このオプションは、 `--file <file name>` オプションが指定されている場合にのみ指定できます。
`principal`	ユーザー名またはユーザーグループ名。
`permissions`	カスタム権限。ユーザーに処理を許可するには `Yes` を指定し、拒否するには `No` を指定します。 • `StopProtection` 保護コンポーネントの停止。 • `StopSecurityControl` 管理コンポーネントの停止 • `StartProtection` 保護コンポーネントの有効化。 • `StartSecurityControl` 管理コンポーネントの有効化 • `ApplicationSettings` アプリケーションの設定 • `ViewReports` レポートの表示 • `RestoreFromBackup` バックアップからの復元 • `RemoveLicenseKey` ライセンスの削除 • `AddLicense` ライセンスの追加 • `DisablePolicy` Kaspersky Security Center ポリシーの無効化

例

kesluser グループからレポートの表示権限を取り消します：

```
kesl-control --set-permissions kesluser --group ViewReports=No
```

new-user に管理コンポーネントの管理を許可します：

```
kesl-control --set-permissions new-user startSecurityControl=Yes StopSecurityControl=Yes
```

パスワードによる保護に関する特別な考慮事項

- パスワードによる保護が無効になっている場合、ユーザーにアプリケーションの管理が許可されるかどうかは、ユーザーロールによって決まります。
- ユーザーのアクセスレベルがグループの権限と個別の権限の両方によって制御されている場合、個別の権限がグループの権限よりも優先されます。つまり、ユーザーの個別の権限が同じユーザーのグループの権限よりも制限の厳しいものであっても、より制限の厳しい権限が優先されます。

  たとえば、*kesluser* グループに対してアプリケーションの管理が禁止されている場合でも、このグループのメンバーである個別のユーザーに対してアプリケーションの管理を許可できます。このようなユーザーには、グループの権限で許可されていない場合でも、アプリケーションの管理が許可されます。
- パスワードによる保護が有効になっていて、ユーザーに個別の権限もグループの権限もない場合、すべての操作が禁止されます。

カスタム権限について

パスワードによる保護が有効になっている場合、Kaspersky Endpoint Security の管理へのアクセスは、*ユーザー権限*を使用して制御されます。ユーザー権限は、ユーザーの権限を定義します（下表を参照）。

カスタム権限

権限	権限
アプリケーションの設定	製品設定の表示と編集。 `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タスク設定を管理します。 ユーザーへのロールの割り当て。 ユーザーロールを取り消す（管理者には、自分から管理者のロールを取り消す権利はありません）。 *ロールバック*タスクの管理。 コンポーネントの管理： • Managed Detection and Response • Endpoint Detection and Response Optimum

権限	権限
保護コンポーネントの有効化。	コンポーネントの管理： • ファイル脅威対策 • 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 • 有害 USB 攻撃ブロック • メール脅威対策 • ウェブ脅威対策 • ネットワーク脅威対策 • ファイアウォール管理 • システム変更監視 • オブジェクトの実行防止 (EDR Optimum) (*EDRO_Prevention*) • Endpoint Detection and Response Expert（オンプレミス） • Endpoint Detection and Response Expert（クラウド） • Network Detection and Response (KATA) • Sandbox • KUMA との連携
保護コンポーネントの停止	
管理コンポーネントの有効化	コンポーネントの管理： • デバイスコントロール • アプリケーションコントロール • ウェブコントロール
管理コンポーネントの停止	
レポートの表示	タスクレポートの表示 イベントの表示
バックアップからの復元	ユーザーの保管領域の表示と管理。
ライセンスの削除	製品のライセンスの管理。
ライセンスの追加	
Kaspersky Security Center ポリシーの無効化	デバイス上で Kaspersky Security Center のポリシーを無効または有効にします。

カスタム権限に関する特記事項

- ユーザー権限は、タスクのリストの表示、バックアップ内のオブジェクトの表示、アプリケーションの設定とステータスの表示には影響しません。

  すべてのユーザーは、次のタスクを管理できます：

  - *スキャンタスク（オブジェクトスキャン、コンテナスキャン、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*
  - *システム整合性チェック*
  - *IOC 検索*

- デバイスが Kaspersky Security Center のポリシーによって管理されている場合、グラフィカルインターフェイスでメインライセンスを追加または削除することはできません。*ライセンスの追加*権限と*ライセンスの削除*権限を持つユーザーは、予備のライセンスを追加したり、他のカスペルスキー製品をアクティベートするためのライセンス（アドオン）を追加したりできます。

  デバイスがポリシーによって管理されていない場合、ユーザーはメインライセンスを削除または追加できます。

既定のユーザー権限

既定では、アプリケーションには定義済みユーザーグループ（*kesladmin*、*kesluser*、*keslaudit*）のユーザー権限が設定されています。これらのグループのメンバーではないユーザーは、アプリケーションに対するすべての操作が禁止されています。

定義済みユーザーグループのユーザー権限

権限	kesladmin	kesluser	keslaudit
アプリケーションの設定	✓	–	–
保護コンポーネントの有効化。	✓	–	–
保護コンポーネントの停止	✓	–	–
管理コンポーネントの有効化	✓	–	–
管理コンポーネントの停止	✓	–	–
レポートの表示	✓	–	✓
バックアップからの復元	✓	–	–
ライセンスの削除	✓	–	–
ライセンスの追加	✓	–	–
Kaspersky Security Center ポリシーの無効化	✓	–	–

パフォーマンス設定

Kaspersky Endpoint Security を使用してコンピューターをスキャンすると、大量のシステムリソースが使用される場合があります。システムの負荷を最適化するには、次の操作を実行できます：

- 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
- スキャンタスクの CPU 使用率を制限する（%）
- アプリケーションによる常駐メモリ使用量を制限する
- 一部のプロセスのメモリをスキャン対象から除外する

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

デバイスがバッテリー駆動で動作しており、Kaspersky Endpoint Security によるリソース使用量を削減したい場合は、スケジュールされたタスクをスキップできます：

- すべてのスキャンタスク（オブジェクトスキャン、コンテナスキャン、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*

- *アプリケーション整合性チェック*
- *IOC スキャン*

必要に応じてタスクを手動で実行できます。

Web コンソールを使用してバッテリー駆動時にスケジュールされたタスクをキャンセルする方法

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. ［**全般設定**］→［**パフォーマンス**］に移動します。
5. **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** 機能を有効にします。
   Kaspersky Endpoint Security がスケジュールされているタスクを キャンセルします。
6. 変更内容を保存します。

コマンドラインを使用してバッテリー駆動時にスケジュールされたタスクをキャンセルする方法

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。

バッテリー駆動時にスケジュールされたタスクをキャンセルするには、次のコマンドを実行します：

```
kesl-control --set-app-settings PowerSaveMode=Yes
```

スキャンタスクの CPU 使用率を制限する（%）

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（タイプ：ODS、ContainerScan、およびInventoryScan）の CPU とメモリの使用量を制限できます。既定では、メモリ使用量の制限は 8192 MB に設定されています。CPU 使用率には制限が設定されていません。

> スキャンタスクが使用可能な RAM をすべて消費してアプリケーションが再起動されることを防ぐため、スキャンタスクのメモリ使用量の制限は常駐メモリ使用量の制限よりも低く設定することを推奨します。

> すべての CPU コアの合計容量は 100% と見なされることに注意してください。

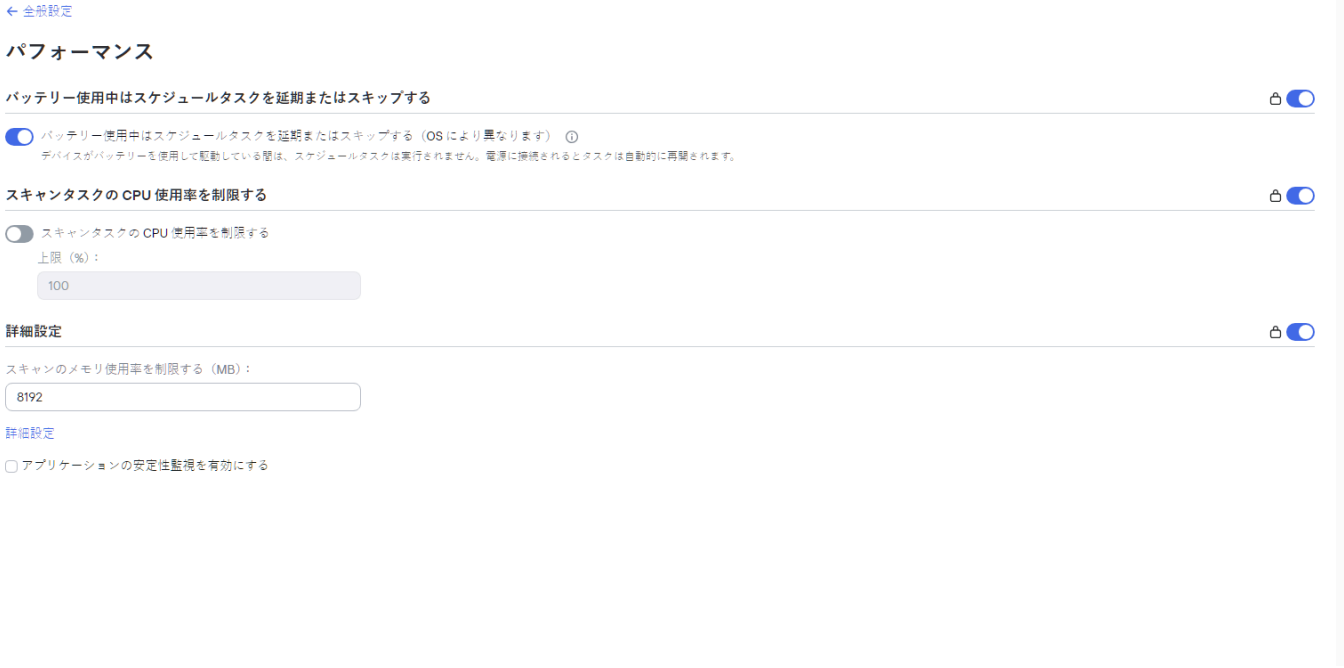
`top` のユーティリティの出力では、100% は単一コアの完全使用率に相当します。したがって、10 コアの CPU（`top` のユーティリティでは合計 1000% とレポートされます）の場合、400% の値は CPU 全体（すべてのコアを合わせた）の使用率が 40% であることを意味します。`top` ユーティリティの出力の値が、同じ 10 個のコアで 150% を超えないようにするには、CPU 使用率の制限を `15%` に設定します。

CPU 使用率の制限は、*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*コンテナスキャン*のタスクに適用されます。つまり、CPU 使用率が設定された値を超える可能性があります。

> CPU 使用率の制限は、CentOS 5.2 および 5.4 を実行しているデバイスでは実行できません。

Web コンソールでメモリと CPU リソースの使用を制限する方法

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. ［**全般設定**］→［**パフォーマンス**］に移動します。
5. **スキャンタスクの CPU 使用率を制限する** 機能を有効にします。
6. **上限（%）** フィールドに、すべての CPU コアの最大負荷を指定します。値は 10 から 100 までの整数である必要があります。
7. ［**詳細設定**］で、対応するフィールドにスキャンタスクのメモリ使用量の制限（MB）を指定します。既定値です：8192.
8. 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。



パフォーマンス

コマンドラインでメモリと CPU リソースの使用を制限する方法

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、スキャンタスクの CPU リソース使用量の制限を設定できます。

1. 次のコマンドを実行して、スキャンタスクに対する CPU 制限を有効にします：

```
kesl-control --set-app-settings UseOnDemandCPULimit = Yes
```

2. 次のコマンドを実行して、CPU 制限を設定します：

```
kesl-control --set-app-settings OnDemandCPULimit =<value>
```

   制限はパーセンテージで指定します。指定可能な値は 10 から 100 までの整数です。

3. kesl.ini 設定情報ファイルの `ScanMemoryLimit` 設定を管理して、スキャンタスクのメモリ使用量の制限を指定します。

アプリケーションによる常駐メモリ使用量を制限する

アプリケーションによる常駐メモリ使用量を制限できます。既定では、制限はメモリの最大 50%（ただし 2 GB 以上 16 GB 以下）に設定されています。

Web コンソールで常駐メモリ使用量を制限する方法

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. ［**全般設定**］→［**パフォーマンス**］に移動します。

5. ［**詳細設定**］で、［**詳細設定**］リンクをクリックし、表示されたウィンドウで［**アプリケーションのメモリ使用量を制限する**］チェックボックスをオンにします。
   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。

   - **正確な値を設定する（%）** この項目を選択すると、［**正確な値（%）**］フィールドが使用可能になり、パーセンテージ値を指定できます。既定値は 50 % です

   - **正確な値を設定する（MB）** この項目を選択すると、［**正確な値（MB）**］フィールドが使用可能になり、メガバイト単位の値を指定できます。既定値は 2000 MB です。

   - **2 つの値のうち最も高いものを使用する（% または MB）** この項目を選択すると、［**正確な値（%）**］および［**正確な値（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。

- **2 つの値のうち最も低いものを使用する（% または MB）** この項目を選択すると、［**正確な値（%）**］および［**正確な値（MB）**］フィールドが使用可能になり、必要な値を指定できます。
- **自動で制限（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）。

6. 変更内容を保存します。

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。

コマンドラインで常駐メモリ使用量を制限する方法

コマンドラインで `MaxMemory` 設定を管理することはできません。常駐メモリの制限を設定するには、kesl.ini 設定情報ファイルを使用します。

既定値の変更は、テクニカルサポートの担当者の監督の下、その指示に従う場合にのみ推奨されます。

［`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。
- `<value>%` – RAM の 1 ～ 100 パーセントの値。
- `<value>MB` – メガバイト単位の値。
- `lowest/<value>%/<value>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/<value>%/<value>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`（既定） – 自動制限。

プロセスメモリのスキャンからの除外

選択したプロセスのメモリをスキャン対象から除外できます。

Web コンソールでプロセスメモリをスキャン対象から除外する方法

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. ［**全般設定**］→［**パフォーマンス**］に移動します。
5. ［**詳細設定**］セクションで、［**プロセスメモリのスキャンからの除外を設定**］をクリックします。

6. ウィンドウが開きます。このウィンドウで［**追加**］ボタンをクリックし、プロセスの実行ファイルへのパスを指定します。

   パスの要件：

7. `/`（絶対パス）で始まる必要があります

   a. 次の禁止文字を含めることはできません：

      - `\0`（ヌルバイト）：オペレーティングシステムで禁止されています。
      - ファイル名またはディレクトリ名内のスラッシュ（`/`）：区切り文字として使用されます。

8. 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。

コマンドラインでプロセスメモリをスキャン対象から除外する方法

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。

`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。

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。

役立つ記事

マスクを指定する方法

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。

製品によるリソース消費の最適化

ネットワークの設定

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。

プロキシ設定の管理方法

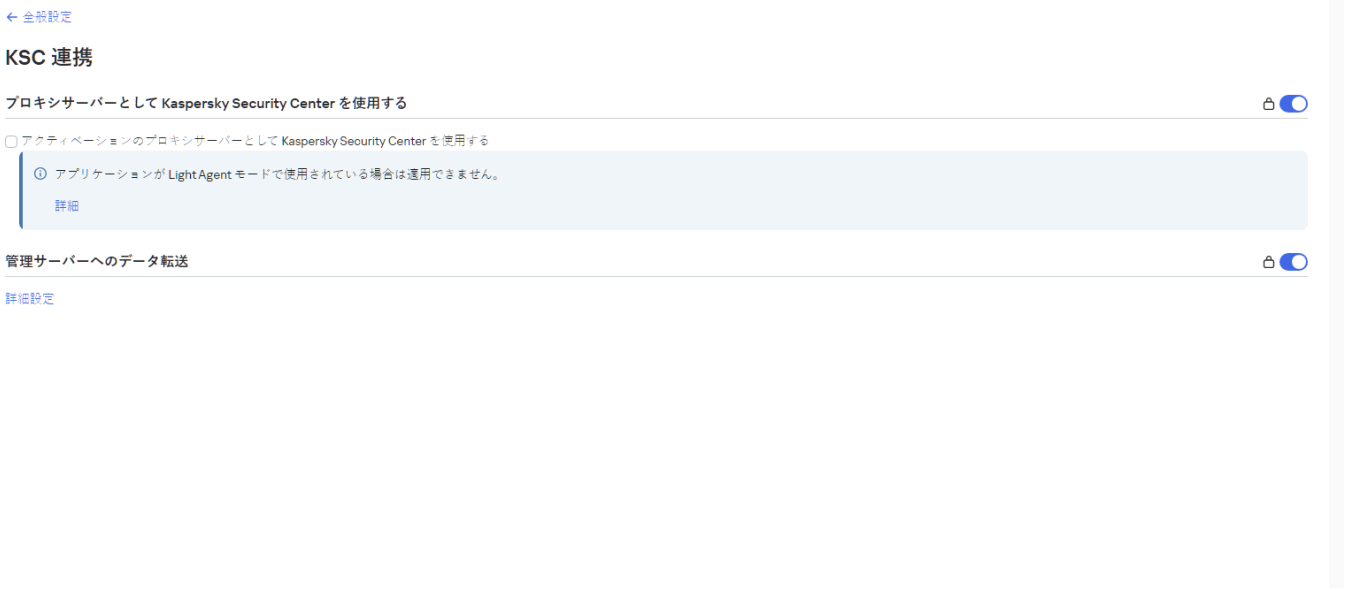
クライアントデバイスのユーザーがプロキシサーバーを使用してインターネットに接続する場合、プロキシサーバーの設定を行うことができます。Kaspersky Endpoint Security は、カスペルスキーアクティベーションサーバーに接続したり、定義データベースと機能のソースをアップデートしたり、Kaspersky Security Network に接続したり、ウェブ脅威対策コンポーネントを使用して Web サイトの証明書を検証したりするときに、プロキシサーバーを使用できます。

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 コンソールでアプリケーションをアクティベートするために Kaspersky Security Center をプロキシサーバーとして使用する設定方法

1. Web コンソールのメインウィンドウで、［**アセット管理**］ → ［**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. ［**全般設定**］ → ［**KSC 連携**］セクションに移動します。
5. ［**アクティベーション用のプロキシサーバーとして Kaspersky Security Center を使用する**］をオンにします。
6. ［**保存**］をクリックします。

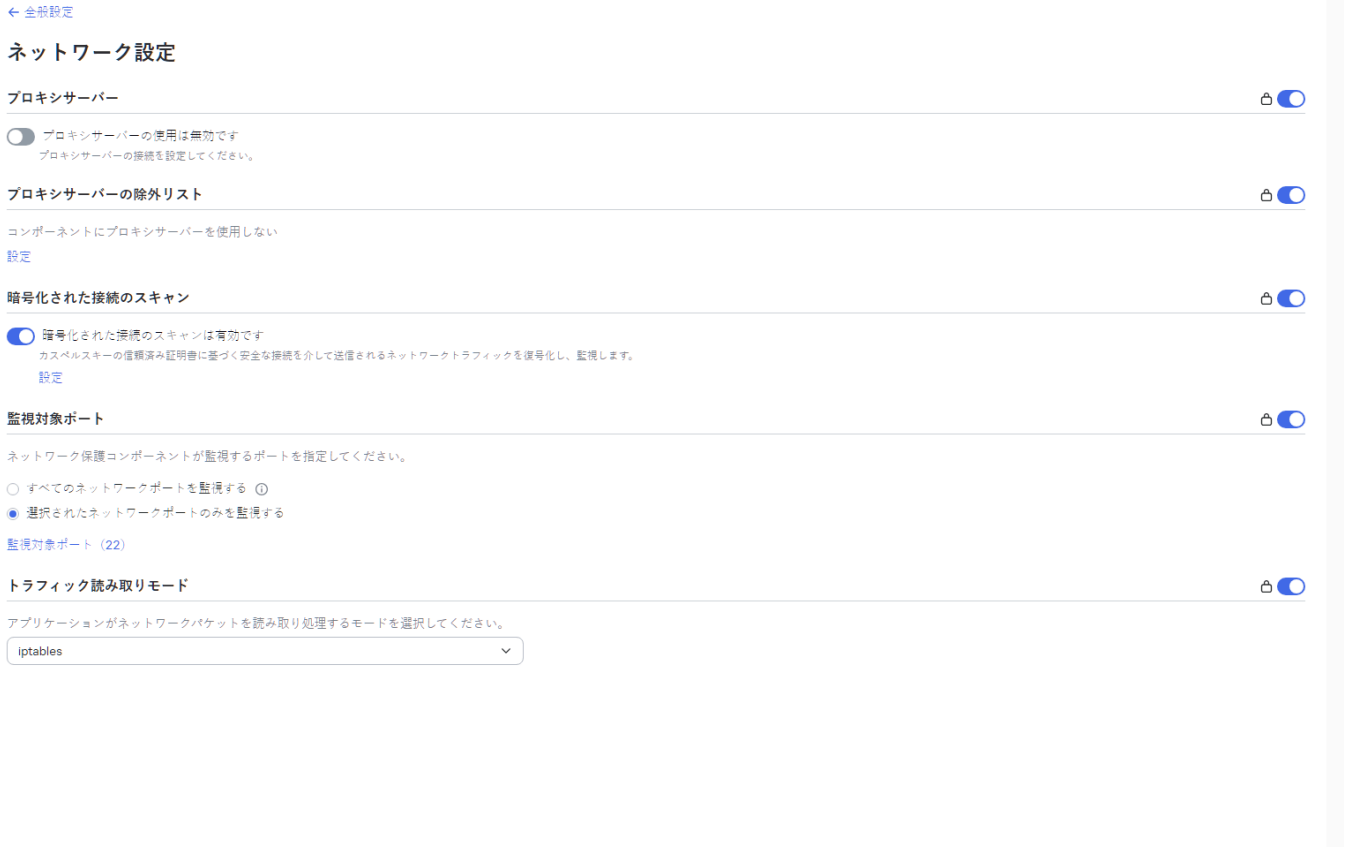


Kaspersky Security Center との連携

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。また、Light Agent モードでは、カスペルスキーのアクティベーションサーバーへのアクセスに管理サーバーをプロキシサーバーとして使用することはサポートされません。

Web コンソールでのプロキシ設定の管理方法

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. ［**全般設定**］→［**ネットワーク設定**］に移動します。
5. トグルスイッチを［**プロキシサーバーの使用は有効です**］にします。
6. 表示されたウィンドウで、次のフィールドに入力します：
   - **プロキシサーバーのアドレス**
   - **ポート**
7. 必要に応じて、プロキシサーバー認証を有効にします：
   a. ［**プロキシサーバー認証を使用する**］チェックボックスをオンにします。
   b. 次のフィールドに入力します：
      - **ユーザー名**
      - **パスワード**
8. 変更内容を保存します。



ネットワークの設定

コマンドラインでのプロキシ設定の管理方法

1. プロキシサーバー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-net-settings UseProxy=Yes ProxyServer=<proxy server address>
```

2. ネットワーク設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-net-settings
```

記号

コマンドオプション

設定	説明
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。 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>://]<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>]@]<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。IPv6 アドレスを指定する場合は、角括弧で囲んで入力してください。 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。

プロキシサーバーの除外リスト

一部のアドレスへの接続にプロキシサーバーを使用する必要がない場合は、そのようなアドレスを除外リストに追加できます。

また、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)、サンドボックスの各コンポーネントについて、プロキシサーバーの使用を無効にすることもできます。これらのコンポーネントの Integration Server に接続する際、プロキシサーバーは使用されません。

Web コンソールでプロキシサーバーの除外を設定する方法

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. ［**全般設定**］→［**ネットワーク設定**］に移動します。

5. ［**プロキシサーバーの除外リスト**］セクションで、［**設定**］をクリックします。
   プロキシサーバーの除外ウィンドウが開きます

6. プロキシサーバーを使用しないコンポーネントの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 Sandbox**
   - **Network Detection and Response (KATA)**
7. プロキシサーバーを使用しない IP アドレスを追加します。例：`1.2.3.4/24`、`1234::cdef/96`。
8. 変更内容を保存します。

コマンドラインでプロキシサーバーの除外を設定する方法

1. プロキシサーバーを使用しないアドレスを追加するには、次のコマンドを実行します：

```
kesl-control --set-net-settings ProxyBypass=<address:port>
```

2. カスペルスキー Detection and Response ソリューションとの連携でプロキシサーバーをバイパスするには、次のコマンドを実行します：

```
kesl-control --set-net-settings [ProxyBypassEdr=<Yes|No>] [ProxyBypassNdr=<Yes|No>] [ProxyBypassSandbox=
<Yes|No>]
```

3. ネットワーク設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-net-settings
```

記号

コマンドオプション

設定	説明
`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、`<address>[:<port>]`の形式で指定します。アドレスを指定する際は、マスク（`*`記号）および`\`記号の後に記述するコメントを使用できます。
`ProxyBypassEdr`	Kaspersky Endpoint Detection and Response Expert（オンプレミス）Integration Server に接続するときにプロキシサーバーを使用するかどうか。プロキシサーバーは、既定では使用されません（`No`）。
`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。プロキシサーバーは、既定では使用されません（`No`）。
`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。プロキシサーバーは、既定では使用されません（`No`）。

本製品がトラフィックをインターセプトする方法

本製品は、eBPF または iptables 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。既定では、iptables モードが選択されています。

この設定は、Elbrus CPUを搭載したデバイスには適用されません。

eBPF によるネットワークトラフィックの傍受について

eBPF 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（network linux namespace）を作成し、そこでローカルネットワークインターフェイスの `tc`（linux traffic control）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、受信接続のネットワークトラフィックを転送します。
- `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転送します。

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。

iptables によるネットワークトラフィックの傍受について

iptables モードでは、tproxy カーネルメカニズムを使用して傍受が実行されます。

mangle テーブルの PREROUTING チェーンに対応するルールが作成され、本製品によって開かれた特別なポートにトラフィックが転送されます。本製品はまた、オペレーティングシステムの Firewall の各種テーブルに追加ルールを追加して、パケットを tproxy に転送します。本製品のネットワークインターセプターはクライアントとサーバーの間に配置され、それぞれと個別の接続を確立し、両者間のトラフィックをスキャンして転送します。

傍受された受信接続と送信接続にはそれぞれ別のラベルが付けられます。このラベルは、kesl.ini 設定情報ファイルで変更できます。

送信接続の場合、傍受対象ポートの送信トラフィックを tproxy のループバックインターフェイスにリダイレクトする追加のルーティングルールが導入されます。

トラフィック傍受モードの選択

Web コンソールでネットワークトラフィック傍受モードを選択する方法

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. ［**全般設定**］→［**ネットワーク設定**］に移動します。

5. **トラフィック読み取りモード** で、本製品のトラフィック傍受モードを選択します：

   - **iptables**既定ではオンです。本製品は、iptables ツールを使用してトラフィックを傍受します。

   - **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。

6. 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。

コマンドラインでネットワークトラフィック傍受モードを選択する方法

1. 次のコマンドを実行します：

```
kesl-control --set-net-settings NetInterceptorMode=<UseEBPF|UseIPTables>
```

2. ネットワーク設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-net-setting
```

特別な考慮事項と制限事項

- 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。

- 本製品が eBPF モード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 モードが使用されます。

証明書検証ポリシーの設定方法

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。

既定では、ウェブ脅威対策は、暗号化された接続を介して送信される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。そのため、本製品は証明書チェーン全体を検証します。

証明書検証ポリシーには、次の設定が含まれます：

- 検証方法（ローカルまたはインターネット経由）

- 信頼されていない証明書を持つ Web サイトへのアクセス

- 証明書の検証エラーがある Web サイトへのアクセス

デバイスがインターネットに直接接続されていない場合は、ローカルでの証明書検証方法を選択できます。

既定では、本製品は、信頼されていない証明書を持つドメインへのネットワーク接続の確立を許可します。本製品は、警告と、該当するドメインへのアクセスが推奨されない理由に関する情報が記載された HTML ページを表示します（下図を参照してください）。HTML の警告ページにあるリンクをクリックすると、リクエストされた Web リソースへアクセスできます。

サードパーティのアプリケーションまたはサービスが信頼されていない証明書を持つドメインとの接続を確立した場合、本製品はトラフィックをスキャンするために独自の証明書を作成します。新しい証明書のステータスは*ブロック*になっています。HTML ページはこの場合表示できず、接続はバックグラウンドモードで確立可能であるため、サードパーティの製品に信頼されていない接続に関して通知するためにこのようになっています。

証明書の検証はエラーで終了する場合があります。例えば、クラウドストレージを使用している場合や、自己署名証明書を検証する場合です。既定では、本製品はこのような Web サイトのドメイン名を除外リストに追加し、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制御しません。本製品は、暗号化された接続のスキャンエラーに関するイベントも生成します。

暗号化された接続のスキャンでエラーが発生したドメインのリストは、本製品のローカルインターフェイスでのみ表示できます。

Web コンソールで証明書検証ポリシーを設定するには

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. ［**全般設定**］→［**ネットワーク設定**］に移動します。
5. **暗号化された接続のスキャン**で、トグルスイッチが**暗号化された接続のスキャンは有効です**の位置になっていることを確認します。

   このトグルスイッチをオフにすると、Kaspersky Endpoint Security は「`https://`」で始まるアドレスの Web サイトのコンテンツにアクセスしません。
6. **設定** のリンクをクリックして、証明書検証ポリシーを設定します：
   - **信頼されない証明書を持つドメインへのアクセス**信頼されない証明書の検出時の動作
     - **接続を許可する**本製品は、信頼されていない証明書を持つドメインへの接続を許可します。本製品は、警告と、該当するドメインへのアクセスが推奨されない理由に関する情報が記載された HTML ページを表示します（下図を参照してください）。HTML の警告ページにあるリンクをクリックすると、リクエストされた Web リソースへアクセスできます。
     - **接続をブロックする**信頼されていない証明書を持つドメインにアクセスすると、Kaspersky Endpoint Security はネットワーク接続をブロックし、そのドメインがブロックされる理由を示す HTML ページを表示します。
   - **暗号化された接続のスキャンでエラーが発生するドメインへのアクセス**暗号化された接続のスキャンエラー時の処理：
     - **許可して除外リストにドメインを追加する**暗号化された接続のスキャンエラーが発生すると、本製品はエラーが発生したドメインを除外リストに追加し、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監視しません。
     - **接続をブロックする**暗号化された接続のスキャンエラーが発生すると、Kaspersky Endpoint Security はネットワーク接続をブロックします。

- **証明書検証ポリシー**本製品による証明書の検証方法：
  - **完全チェック**製品は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確認してダウンロードします。
  - **ローカルチェック**本製品は、コンピューター上でローカルに証明書を検証します。

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。

コマンドラインで証明書検証ポリシーを設定する方法

1. 暗号化された接続のスキャンを有効にするには、次のコマンドを実行します：

```
kesl-control --set-net-settings EncryptedConnectionsScan=Yes
```

2. 証明書の検証方法を選択するには、次のコマンドを実行します：

```
kesl-control --set-net-settings CertificateVerificationPolicy=<FullCheck|LocalCheck>
```

3. 信頼されていない証明書が見つかった場合に実行する処理を選択するには、次のコマンドを実行します：

```
kesl-control --set-net-settings UntrustedCertificateAction=<Allow|Block>
```

4. 暗号化された接続のスキャン中にエラーが発生した場合に実行する処理を選択するには、次のコマンドを実行します：

```
kesl-control --set-net-setting EncryptedConnectionsScanErrorAction=<AddToAutoExclusions|Disconnect>
```

5. ネットワーク設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-net-setting
```

記号

コマンドオプション

設定	説明
`EncryptedConnectionsScan`	暗号化された接続のスキャンモード： `Yes` （既定）。暗号化された接続のスキャンは有効です。 `No` 暗号化された接続のスキャンは無効です。
`CertificateVerificationPolicy`	証明書検証ポリシー： `FullCheck` （既定）。製品は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確認してダウンロードします。 `LocalCheck` 本製品は、コンピューター上でローカルに証明書を検証します。
`UntrustedCertificateAction`	信頼されない証明書の検出時の動作 `Allow` （既定）。本製品は、信頼されていない証明書を持つドメインへの接続を許可します。本製品は、警告と、該当するドメインへのアクセスが推奨されない理由に関する情報が記載された HTML ページを表示します（下図を参照してください）。HTML の警告ページにあるリンクをクリックすると、リクエストされた Web リソースへアクセスできます。 `Block` 信頼されていない証明書を持つドメインにアクセスすると、Kaspersky Endpoint Security はネットワーク接続をブロックします。信頼されていない証明書を持つドメインをブラウザーで開こうとすると、Kaspersky Endpoint Security は、そのドメインがブロックされる理由が記載された HTML ページを表示します。

設定	説明
`EncryptedConnectionsScanErrorAction`	暗号化された接続のスキャンエラー時の処理： `AddToAutoExclusions`（既定）。暗号化された接続のスキャンエラーが発生すると、本製品はエラーが発生したドメインを除外リストに追加し、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監視しません。 `Disconnect` 暗号化された接続のスキャンエラーが発生すると、Kaspersky Endpoint Security はネットワーク接続をブロックします。

監視対象ポートの設定方法

Kaspersky Endpoint Security の実行中、ネットワーク脅威対策は、一部のネットワークポートを介して送信されるデータを監視します。本製品が監視するネットワークポートのリストは、カスペルスキーのエキスパートの推奨事項に従って設定されています。

ふるまい検知と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プロセスに対して、ネットワークポートも監視します。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。

本製品で監視するポートを設定できます：

- **すべてのネットワークポートを監視する**本製品が、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を通過するデータストリームを監視するネットワークポート監視モード。

  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。

- **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。

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。

Web コンソールで監視対象ポートを設定する方法

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. ［**全般設定**］→［**ネットワーク設定**］に移動します。
5. ［**監視対象ポート**］で、本製品のポート監視モードを選択します：
   - **すべてのネットワークポートを監視する**
   - **選択されたネットワークポートのみを監視する**（既定値）：

6. ［**選択されたネットワークポートのみを監視する**］を選択した場合は、監視するポートのリストを設定します：

   a. ［**監視対象ポート**］リンクをクリックします。

   b. 監視対象ポートのリストを編集します。

   > 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、110、143、465、587、993、および 995 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。

7. 変更内容を保存します。

コマンドラインで監視対象ポートを設定する方法

1. ポート監視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-net-settings MonitorNetworkPorts=<All|Selected>
```

2. 選択したポートのみを監視するように設定した場合（`MonitorNetworkPorts=Selected`）、監視するポートのリストを指定します：

```
kesl-control --set-net-settings NetworkPorts.item_#.PortName=<port name> NetworkPorts.item_#.Port=<port number>
```

   監視リストからポートを削除するには、設定情報ファイルを使用してリストを編集します。

3. ネットワーク設定の現在の値を確認するには、次のコマンドを実行します：

```
kesl-control --get-net-settings
```

記号

コマンドオプション

設定	説明
`MonitorNetworkPorts`	`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。
`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。指定可能な値：`1` ～ `65535`。 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、110、143、465、587、993、および 995 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。

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。

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。

ファイル操作のインターセプト

ファイル操作インターセプトモードは、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、オブジェクトの実行防止処理、およびリムーバブルドライブスキャンタスクに影響します。

ファイル操作のインターセプトのブロックモードが有効な場合

- 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。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。

- 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。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。

- オブジェクトの実行防止処理がファイルを実行できるかどうかを判定している間、本製品がデバイス上のファイルをブロックする場合があります。スキャンの結果、オブジェクトの実行防止処理でファイルの実行が許可された場合、本製品はそのファイルの実行を許可します。

- アプリケーションは、スキャン中にリムーバブルドライブ上のファイルへのアクセスをブロックする場合があります。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。

ファイル操作のインターセプトのブロックモードが無効な場合

- ファイル脅威対策コンポーネントは、選択した動作モードに関係なく通知モードで動作し、ファイルへのアクセスを許可して、スキャンを非同期で実行します。

- デバイスコントロールコンポーネントは、選択した動作モードに関係なく通知モードで動作し、デバイスへのアクセスを常に許可します。

- オブジェクトの実行防止処理は、選択した動作モードに関係なく通知モードで動作し、オブジェクトの実行を常に許可します。

- アプリケーションは常にリムーバブルドライブ上のファイルへのアクセスを許可し、非同期でスキャンを実行します。

このファイル操作インターセプトモードでは、スキャン中のシステムパフォーマンスへの影響は小さくなりますが、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。これは、スキャン中に、このファイルに関連付けられたプロセスが、アプリケーションがこのファイルのステータスを判定する前にファイル名を変更した場合に発生する可能性があります。

既定では、ファイル操作インターセプトのブロックモードが有効になっています。

Web コンソールでファイル操作のインターセプトモードを設定するには

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. ［**全般設定**］→［**検知の設定**］に移動します。

5. ［**ファイル操作のインターセプトモード**］で、［**スキャン中にファイルへのアクセスをブロックする**］チェックボックスをオフまたはオンにします。既定では、このチェックボックスはオンです。

6. 変更内容を保存します。

コマンドラインでファイル操作のインターセプトモードを設定するには

`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。

ファイル操作のインターセプ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-app-settings FileBlockDuringScan=<Yes|No>
```

記号

コマンドオプション

設定	説明
FileBlockDuringScan	Yes（既定値）：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、およびリムーバブルドライブスキャンタスクによってファイルがスキャンされている間、ファイルへのアクセスをブロックします。 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。

システムイベントインターセプターの設定

Web コンソール、コマンドライン、または管理コンソールで、システムイベントインターセプトメカニズムを選択できます。

システムイベントのインターセプトに関する設定は、fanotify テクノロジー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のみ管理できます。

システムイベントインターセプトの設定は、Elbrus CPU を搭載したデバイスでは使用できません。

Web コンソールでシステムイベントインターセプトメカニズムを設定するには

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. ［**全般設定 → OS 連携設定**］に移動します。

5. **システムイベントインターセプターの設定**で、システムイベントのインターセプトメカニズムを選択します：

   - **fanotify テクノロジー**
   - **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した場合は、更新可能なカーネルモジュールを起動できない場合にアプリケーションが実行する処理を選択します：
     - **fanotify を使用する**
     - **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）**

OS 連携設定

コマンドラインでシステムイベントインターセプトメカニズムを設定するには

1. システムイベントのインターセプトメカニズムを選択するには、次のコマンドを実行します：

```
kesl-control --set-app-settings InterceptorMode=<UseFanotify|UseUpdatableKernelModule>
```

2. 更新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を設定するには、次のコマンドを実行します：

```
kesl-control --set-app-settings InterceptorFallbackStrategy=<FallbackToFanotify|FallbackToLimitedMode>
```

3. 更新可能なカーネルモジュールの起動に失敗した場合にアプリケーションを再起動するには、次のコマンドを実行します：

```
kesl-control --set-app-settings InterceptorApplyStrategy=<RestartServiceAutomatically|RestartServiceManually>
```

4. 現在のアプリケーション設定を確認するには、次のコマンドを実行します：

```
kesl-control --get-app-settings [--json]
```

記号

コマンドオプション

設定	説明
`InterceptorMode`	`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。
`InterceptorFallbackStrategy`	`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`	`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。この設定の使用を推奨します。 `RestartServiceManually`（既定）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。

OS が更新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、本製品は更新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。

本製品のインストール中に更新可能なカーネルモジュールをインストールできなかった場合は、お使いの OS のサポートが利用可能になった時点で後からインストールできます。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。

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。

更新可能なカーネルモジュールのステータスに関する情報

更新可能なカーネルモジュールの状態と利用可否に関する情報は、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ますが、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。

デバイス上の更新可能なカーネルモジュールのステータスは、Web コンソールおよびコマンドラインで確認できます。

Web コンソールで更新可能なカーネルモジュールのステータスを確認する方法

1. Web コンソールのメインウィンドウで、［**アセット管理**］ →［**アセット（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。下位グループを選択するには、ウィンドウ上部の **階層を表示** ボタンをクリックします。
   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. デバイス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. ［**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。

コマンドラインで更新可能なカーネルモジュールのステータスを確認する方法

更新可能なカーネルモジュールのステータスを確認するには、次のコマンドを実行します：

```
kesl-control --app-info [--json]
```

ここで、 `--json` は、データを JSON 形式で出力することを意味します。 `--json` 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。

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。

コマンドラインで本製品のセーフモードを無効にする方法

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
```

セーフモードは無効です。

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 コンソールで追加のテレメトリ設定を構成する方法

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. ［**全般設定**］→［**OS 連携設定**］に移動します。
5. **テレメトリ設定**で、Kaspersky Endpoint Security がテレメトリの収集に使用するソースを指定します：
   - **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 のみを使用する**オプションが選択されている場合、Detection and Response ソリューションのテレメトリには制限がある場合があります。

   - **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。
6. auditd サービスのモードも指定します：
   - **排他**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**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**既定**に設定されている場合にのみ適用されます。

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。

コマンドラインで追加のテレメトリ設定を構成する方法

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。

1. テレメトリソースを有効にするには、次のコマンドを実行します：

```
kesl-control --set-settings 20 TelemetrySource=<Default|OnlyEBPF>
```

2. auditd サービスの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 20 UseTelemetryMonopolyMode=<True|False>
```

記号

コマンドオプション

設定	説明
`TelemetrySource`	`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。 `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。

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。

バックアップ設定の構成

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、デバイスのバックアップ設定を管理できます。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。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。
- **バックアップの最大サイズ。**既定では、バックアップの最大サイズとして次の値が設定されています：
  - ポリシーが適用されていない場合は 0 MB
  - ポリシーが適用されている場合は 1024 MB

  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。
- **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）。既定では、/var/opt/kaspersky/kesl/common/objects-backup/ ディレクトリが、ファイルのバックアップコピーおよび隔離されたファイルの保存に使用されます。

Web コンソールでバックアップ設定を指定する方法

ポリシーのプロパティでバックアップ設定を管理するには：

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. ［**全般設定**］→［**レポートと保管領域**］セクションに移動します。
5. ［**バックアップ**］セクションで、次の設定を指定します：
   - **オブジェクトを削除するまでの期間（日）**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。既定では、このチェックボックスはオンです。
     有効な値は 0 ～ 10000 です。
   - **バックアップのサイズを制限する（MB）**このチェックボックスをオンにすると、保管領域の最大サイズは指定した値に制限されます。既定では、このチェックボックスはオンです。
     有効な値は 1 ～ 4000 です。
6. 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。

管理対象デバイスのプロパティでバックアップ設定を管理するには：

1. Web コンソールのメインウィンドウで、［**アセット管理 → アセット（デバイス）**］を選択します。
   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。下位グループを選択するには、ウィンドウ上部の **階層を表示** ボタンをクリックします。

   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. デバイス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. ［Kaspersky Endpoint Security］を選択します

6. ［**アプリケーション設定 → ストレージ設定**］に移動します。

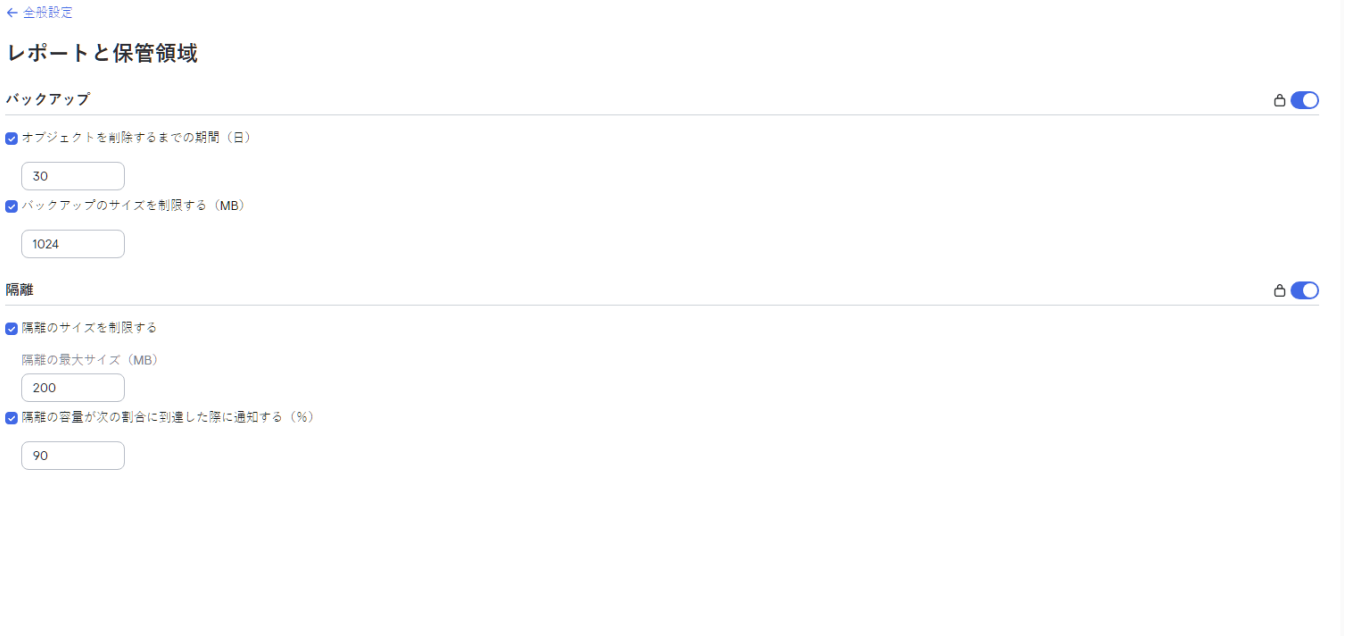
   - **オブジェクトを削除するまでの期間（日）** このチェックボックスをオンにすると、ファイルの最長保管期間は指定した期間に制限されます。既定では、このチェックボックスはオンです。

     有効な値は 1 ～ 10000 です。

   - **バックアップのサイズを制限する（MB）** このチェックボックスをオンにすると、保管領域の最大サイズは指定した値に制限されます。既定では、このチェックボックスはオンです。

     有効な値は 1 ～ 4000 です。

7. 変更内容を保存します。



レポートおよびストレージ

コマンドラインでバックアップを設定する方法

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。

1. バックアップ内のオブジェクトの保存期間を設定するには、次のコマンドを実行します：

```
kesl-control --set-app-settings BackupDaysToLive=<days>
```

2. バックアップの最大サイズを設定するには、次のコマンドを実行します：

```
kesl-control --set-app-settings BackupSizeLimit=<Backup size>
```

3. バックアップオブジェクトと隔離オブジェクトが保存されるディレクトリを設定するには、次のコマンドを実行します：

```
kesl-control --set-app-settings QuarantineBackupFolder=<path to folder>
```

4. 現在のアプリケーション設定を確認するには、次のコマンドを実行します：

```
kesl-control --get-app-settings
```

コマンドオプション

設定	説明
`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。
`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。
`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。

Backup オブジェクトの表示

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ってバックアップに配置されたファイルの全般リストは、Kaspersky Security Center で生成され、Web コンソールおよび管理コンソール（**詳細設定 → リポジトリ → バックアップ**）で利用できます。

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。

Web コンソールでバックアップ内のオブジェクトに関する情報を表示する方法

1. メインの Web コンソールウィンドウで、［**リポジトリ**］ → ［**ファイルバックアップ**］を選択します。

   これにより、クライアントデバイス上でカスペルスキー製品によってバックアップに配置されたファイルのリストが開きます。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。

2. 保護対象デバイスのバックアップストレージにあるファイルのプロパティを表示します：

- **ファイル名**
- **ステータス：**
  - *警告*
  - *感染の可能性あり*
  - *ユーザーにより追加*
  - *誤検知*
  - *駆除済み*
  - *感染なし*
  - *パスワード保護*
  - *削除済み*
  - *カスペルスキーに送信する必要あり*
- **デバイス名**
- **実行された処理**：
  - *削除*
  - *駆除*
  - *スキャン*
  - *復元*
- **オブジェクト**
- **リポジトリに配置済み**
- **エントリの追加者**
- **サイズ（バイト）**
- **フォルダーが復元されました**
- **User**
- **説明**
- **仮想管理サーバーの名前**

コマンドラインでバックアップ内のオブジェクトに関する情報を表示する方法

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 ["<filter conditions>"] [-n <objects number>] [--json]
```

説明：

- `<filter conditions>` は、クエリの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 `<field> <comparison operator> '<value>'` 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。
- `<objects number>` 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。

グラフィカルインターフェイスでバックアップ内のオブジェクトに関する情報を表示する方法

1. アプリケーションの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。

バックアップからのオブジェクトの復元

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。
- 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。ファイルを復元する際、アプリケーションは MAC ラベルが 3（cnnr フラグ）のディレクトリを作成します。

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。

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。

Web コンソールでバックアップからオブジェクトを復元する方法

1. メインの Web コンソールウィンドウで、［**リポジトリ**］ → ［**ファイルバックアップ**］を選択します。

   これにより、クライアントデバイス上でカスペルスキー製品によってバックアップに配置されたファイルのリストが開きます。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。

2. 復元するファイルの横にあるチェックボックスをオンにします。

3. ［**復元**］をクリックします。

クライアントデバイス上のバックアップ内のオブジェクトが復元されます。

コマンドラインでバックアップからオブジェクトを復元する方法

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 <object id>
```

ここで、`<object 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 <object id> --file <path to file>
```

ここで、`--file <path to file>` 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。

グラフィカルインターフェイスでバックアップからオブジェクトを復元する方法

バックアップからオブジェクトを元のディレクトリに復元するには：

1. アプリケーションの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。
3. 復元するオブジェクトを選択します。
4. ［**復元**］をクリックします。

バックアップからオブジェクトが復元され、元のディレクトリで使用できるようになります。

> 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。

バックアップからのオブジェクトの削除

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。

Web コンソールでバックアップからオブジェクトを削除する方法

1. メインの Web コンソールウィンドウで、［**リポジトリ**］ → ［**ファイルバックアップ**］を選択します。
   これにより、クライアントデバイス上でカスペルスキー製品によってバックアップに配置されたファイルのリストが開きます。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。
2. 削除するファイルの横にあるチェックボックスをオンにします。
3. ［**削除**］をクリックします。

   クライアントデバイス上のバックアップ内のオブジェクトが削除されます。

コマンドラインでバックアップからオブジェクトを削除する方法

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 "<filter conditions>"
```

ここで、`<filter conditions>` は、クエリの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 `<field> <comparison operator> '<value>'` 形式の1つ以上の 論理式を指定します。

例：

ID=15 のオブジェクトを削除する

```
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

```
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
```

グラフィカルインターフェイスでバックアップからオブジェクトを削除する方法

1. アプリケーションの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。
3. 削除するオブジェクトを選択します。
4. ［**削除**］をクリックします。

バックアップ内のオブジェクトが削除されます。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。

高度な脅威と標的型攻撃からの保護

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。Detection and Response 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できるようにします。

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 アプリケーションのコンポーネントである 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。
- Open Single Management Platform (OSMP) 上の Kaspersky Endpoint Detection and Response Expert（クラウド）。連携は、Kaspersky Endpoint Security アプリケーションのコンポーネントである Endpoint Detection and Response Expert（クラウド）（以下、*EDR Expert*（クラウド）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。

Detection and Response ソリューションの統合機能

- Kaspersky Endpoint Security を EDR Agent モードで使用している場合、連携に対応しているのは、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 コンポーネントと Kaspersky Network Detection and Response コンポーネントのみです。
- Kaspersky Endpoint Security が Kaspersky Managed Detection and Response および Kaspersky Anti Targeted Attack Platform と連携している場合、組み込みエージェントが systemd-journald ログに大量のイベントを記録することがあります。監査イベントの systemd-journald ログへの記録を無効にする場合、systemd-journald-audit ソケットを無効にしてから、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

  ```
  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）と正しく統合するための参照イメージを準備する方法

対応処理

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 Expert（クラウド）、Kaspersky Endpoint Detection and Response (KATA)、または Kaspersky Managed Detection and Response と連携している場合、ネットワーク分離は Detection and Response ソリューション側で有効化または無効化されます。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 と連携している場合、タスクは Detection and Response 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 Expert（クラウド）、Kaspersky Endpoint Detection and Response (KATA)、または Kaspersky Managed Detection and Response と連携している場合、脅威対応処理は Detection and Response ソリューション側で生成されます。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。

  Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Endpoint Detection and Response Expert（クラウド）、Kaspersky Endpoint Detection and Response (KATA)、または Kaspersky Managed Detection and Response と連携している場合、脅威対応処理は Detection and Response ソリューション側で生成されます。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 Expert（オンプレミス）、Kaspersky Endpoint Detection and Response Expert（クラウド）、または Kaspersky Endpoint Detection and Response (KATA) と連携している場合、脅威対応処理は Detection and Response ソリューション側で生成されます。

  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 と連携している場合、タスクは Detection and Response 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 Expert（オンプレミス）、Kaspersky Endpoint Detection and Response Expert（クラウド）、または Kaspersky Endpoint Detection and Response (KATA) と連携している場合、タスクは Detection and Response 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 と連携している場合、タスクは Detection and Response 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 と連携している場合、タスクは Detection and Response 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。

- *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）および Kaspersky Endpoint Detection and Response Expert（クラウド）ソリューション側で作成され、実行されます。

- 実行防止

- フォレンジックの取得。

  Kaspersky Endpoint Detection and Response Expert（オンプレミス）および Kaspersky Endpoint Detection and Response Expert（クラウド）と連携している場合、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、Kaspersky Endpoint Detection and Response Expert（オンプレミス）および Kaspersky Endpoint Detection and Response Expert（クラウド）ソリューション側で作成され、実行されます。

侵害の兆候の調査

*セキュリティ侵害インジケーター（IOC）*とは、コンピューターへの認証されないアクセス（コンピューターの侵害）の痕跡を示すオブジェクトまたは活動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。*IOC スキャンタスク*は、コンピューターのセキュリティ侵害インジケーターを検索し、脅威への対応方法を確立するのに役立ちます。

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。

  この場合、IOC 検索は *IOC スキャンタスク*を使用して実行されます。

- 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っており、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ています。

  この場合、IOC スキャンは対応するソリューション側で実行されます。

IOC スキャンタスクは、オペレーティングシステムの主要な名前空間でのみ、IOC 用語（IOC オブジェクトのプロパティ、たとえばファイルハッシュ）をチェックします。*IOC* スキャンタスクでは、200 MB を超えるファイルのハッシュは計算されません。

侵害の兆候を検索するために、Kaspersky Endpoint Security はユーザーが準備した IOC ファイルを使用します。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。

IOC スキャンタスクの作成

IOC スキャンタスクは、手動で作成することができます：

- アラートの詳細（EDR Optimum のみ）で作成する。

  *アラートの詳細（Alert details）*は、収集済みの検知した脅威に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれます。アラートの詳細の管理について詳しくは、Kaspersky Endpoint Detection and Response Optimum のヘルプおよび Kaspersky Endpoint Detection and Response Expert のヘルプを参照してください。

- タスクウィザードを使用する。

- コマンドラインでローカルに実行します。

Web コンソールでIOC スキャンタスクを作成する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。

   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**］から［**Kaspersky Endpoint Security for Linux 12.5**］を選択します。

   b. ［**タスク種別**］から［**IOC スキャン**］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**］で、タスクの範囲の定義方法を選択します。

4. 選択したタスク範囲の定義方法に従ってデバイスを選択します。次のステップに進みます。

5. 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。

6. 新しい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。

7. ［**アプリケーション設定**］タブを選択します。

8. ［**脅威のスキャン**］に移動します。

9. 侵害インジケーターを検索するために IOC ファイルをアップロードします。

   IOC ファイルをアップロードすると、チェックに通過しなかったインジケーターのリストなど、ファイルに関する概要情報が本製品に表示されます。IOC ファイルをアップロードしたら、タスクのプロパティで直接、組み込みエディターを使用してファイルを手動で編集できます。Kaspersky Endpoint Security は、OpenIOC 1.1 標準に準拠した IOC ファイルの編集をサポートしています。OpenIOC バージョン 1.0 に準拠した IOC ファイルの内容を変更することはできません。

   IOC コレクションに IOC ファイルが追加されます。必要に応じて、IOC ファイルをタスク範囲から一時的に除外できます。

   > このタスクを開始した後は、IOC ファイルを追加または削除しないことは推奨します。これにより、以前に実行したタスクの IOC スキャン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追加することを推奨します。

10. ［**スキャン設定**］に移動します。

11. 必要に応じて、レトロスペクティブ IOC スキャンを設定します。

    遡及的 IOC スキャンは、Kaspersky Endpoint Security が一定期間のデータ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する *IOC* スキャンタスクのモードです。このモードは、ネットワーク動作、プロセス、ファイル、その他のテレメトリなど、保護対象コンピューターのテレメトリでセキュリティ侵害インジケーターを検索することを目的としています。Kaspersky Endpoint Security は、コンピューターのオペレーティングシステムのログとブラウザーのログ内のデータを分析します。遡及的 IOC スキャンは、Google Chrome、Mozilla Firefox、Microsoft Edge（バージョン 79 以降）のブラウザーのログを分析します。

    a. ［**遡及的 IOC スキャン**］で、検索設定に移動します。

    b. **遡及的 IOC スキャン** トグルスイッチを有効にします。

    c. レトロスペクティブ IOC スキャンの時間間隔を設定します。

12. タスクの一部として分析される必要のあるデータ種別（IOC ドキュメント）を選択します。

    > Kaspersky Endpoint Security は、読み込まれた IOC ファイルの内容に従って *IOC* スキャンタスク用のデータ種別（IOC ドキュメント）を自動で選択します。選択されたデータ種別の選択解除は推奨されません。

    さらに、**ファイル - FileItem** データ種別の検索範囲を設定できます。事前定義された範囲を使用してコンピューター上の IOC スキャン範囲を設定します。

13. ［**レスポンスの設定**］に移動します。

14. タスクの動作モードとして、**アラートのみ**または**アラートとレスポンス**を選択します。

15. IOC が検知された場合の応答処理を選択します：

- **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*簡易スキャン*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。

  Kaspersky Endpoint Security がスキャンする重要な領域

  - /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。

  このチェックボックスをオフにすると、タスクを手動で実行した後でファイルを手動で隔離できます。*IOC* スキャンタスクでデータを危険にさらす可能性のあるファイルが検知された場合、IOC スキャン結果からこのファイルを直接隔離することができます（［**アプリケーション設定**］→［**IOC スキャン結果**］）。この結果、Kaspersky Endpoint Security は、検知されたファイルの事前設定されたデータを使用してタスク作成ウィザードを起動します。タスクのスケジュールの設定など、追加のタスク設定のみを管理する必要があります。

- **デバイスをネットワークから分離する**このオプションを選択した場合、Kaspersky Endpoint Security は脅威の拡散を防ぐためにコンピューターをネットワークから分離します。分離時間は Endpoint Detection and Response コンポーネントの設定で設定できます。

  このチェックボックスをオフにすると、タスクを手動で実行した後でコンピューターをネットワークから分離できます。*IOC* スキャンタスクでデータを危険にさらす可能性のあるファイルが検知された場合、IOC スキャン結果からこのファイルを直接隔離することができます（［**アプリケーション設定**］→［**IOC スキャン結果**］）。この結果、Kaspersky Endpoint Security は、検知されたファイルの事前設定されたデータを使用してタスク作成ウィザードを起動します。タスクのスケジュールの設定など、追加のタスク設定のみを管理する必要があります。

16. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。

17. タスクのスケジュールを設定します。

> このタスクでは Wake-on-LAN は使用できません。コンピューターの電源がオンになっていて、タスクを実行できることを確認してください。

18. 変更内容を保存します。

19. タスクの横にあるチェックボックスをオンにします。

20. ［**開始**］をクリックします。

Web コンソールの［**IOC スキャン結果**］にあるタスクのプロパティで、*IOC* スキャンタスクの結果を確認できます。IOC スキャンの結果は 30 日間保存されます。この時間が経過すると、Kaspersky Endpoint Security は古いエントリを自動的に削除します。

コマンドラインでIOC スキャンタスクを作成する方法

次のコマンドを実行します：

```
kesl-control [-T] --scan-ioc --path <path to the directory or file> [--process on|off] [--hint <regular expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

記号

マルウェアのスキャンタスクの設定

設定	説明
`--path`	スキャンを実行するために使用する、.IOC または .XML 拡張子を持つ IOC ファイル、またはそれらの IOC ファイルを含むディレクトリへのパス。*IOC ファイル*は、本製品が検知の判断時に一致させる一連のインジケーターを含むファイルです。IOC ファイルは OpenIOC 標準に準拠している必要があります。 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`	IOC スキャンの実行中にプロセスデータを分析します（ProcessItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security はスキャンの実行時にコンピューター上で実行されているプロセスを分析しません。IOC ファイルに IOC ドキュメント ProcessItem の IOC タームが含まれている場合、無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント ProcessItem が記述されている場合のみプロセスデータを分析します。
`--hint`	IOC スキャンの実行時にファイルのデータを分析します（ProcessItem および FileItem）。 次のいずれかの方法でファイルを選択することができます： • `<full path to the executable file of the process>` – ProcessItem ターム。 • `<full path to the file>` – FileItem ターム。
`--arpentry`	IOC スキャンの実行中、ARP テーブル内の項目のデータを分析します（ArpEntryItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security は ARP テーブルをスキャンしません。IOC ファイルに IOC ドキュメント ArpEntryItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント ArpEntryItem が記述されている場合のみローカルの ARP テーブルを分析します。
`--ports`	IOC スキャンの実行中、待機しているポートに関するデータを分析します（PortItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security は端末上のアクティブな接続のテーブルをスキャンしません。IOC ファイルに IOC ドキュメント PortItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント PortItem が記述されている場合のみアクティブな接続のテーブルを分析します。
`--system`	IOC スキャンの実行中に環境のデータを分析します（SystemInfoItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security は環境データを分析しません。IOC ファイルに IOC ドキュメント SystemInfoItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント SystemInfoItem が記述されている場合のみ環境データを分析します。
`--files`	IOC スキャンの実行時にファイルのデータを分析します（FileItem）。 引数の値が「`off`」の場合、Kaspersky Endpoint Security はファイルのデータを分析しません。IOC ファイルに IOC ドキュメント FileItem が含まれている場合、IOC タームは無視されます（一致なしと判断される）。 引数が指定されていない場合、IOC ファイルで IOC ドキュメント FileItem が記述されている場合のみファイルに関するデータを分析します。
`--drives`	IOC ドキュメント FileItem のデータを分析する際の IOC スキャン範囲を設定します。 スキャン範囲には次の値を設定できます： • `<all>`：すべての利用可能なファイル範囲 • `<system>`：オペレーティングシステムがインストールされているフォルダーにあるファイル • `<critical>`：ユーザーおよびシステムフォルダー内の一時ファイル • `<custom>`：ユーザー定義の範囲のファイル（`/scope=<list of folders to scan>`） 引数が指定されていない場合、スキャンは重要な領域に対して実行されます。
`--excludes`	IOC ドキュメント FileItem のデータを分析する際に除外する範囲を設定します。スペースで区切って複数のパスを指定することができます。
`--scope`	IOC ドキュメント FileItem でデータを分析する際のユーザー定義の IOC スキャン範囲です（`/drives=custom`）。スペースで区切って複数のパスを指定することができます。

設定	説明
`--action`	侵害の兆候が検知された場合に実行される処理： • `Skip` このオプションを選択した場合、Kaspersky Endpoint Security は、データ侵害の原因となる可能性があるファイルのみを検知します。 • `QuarantineFile` 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。 • `IsolateHost` このオプションを選択した場合、Kaspersky Endpoint Security は脅威の拡散を防ぐためにコンピューターをネットワークから分離します。 • `ScanCriticalAreas` このオプションを選択した場合、Kaspersky Endpoint Security は*簡易スキャン*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。

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っており、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ています。
- 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 Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Endpoint Detection and Response (KATA)、および Kaspersky Managed Detection and Response と連携している場合、デバイスのネットワーク分離の有効化または無効化、およびネットワーク分離の除外の設定は、Detection and Response ソリューション側で行われます。詳細については、Kaspersky Endpoint Detection and Response Expert（オンプレミス）のヘルプ、Kaspersky Anti Targeted Attack Platform のヘルプ、またはKaspersky Managed Detection and Response のヘルプを参照してください。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) と連携している場合のみ）
- 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 EDR Agent モードで使用している場合、ネットワーク分離の使用時には、以下を推奨します：

- Kaspersky Security Network と対話するには、KSN プロキシサーバーを使用します。
- Kaspersky Security Center を製品のアクティベーションのプロキシサーバーとして使用します。

  Kaspersky Security Center をプロキシサーバーとして使用できない場合は、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. 必要に応じて管理グループを選択し、デバイスを見つけて、その名前をクリックします。

3. 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。

4. 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。

5. 開いたアプリケーションプロパティウィンドウの［**製品設定**］タブで、［**組み込みエージェント**］→［**Endpoint Detection and Response**］を選択します。

6. 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。このボタンは、［**Endpoint Detection and Response**］トグルスイッチが有効になっている場合にのみ使用できます。

     このボタンをクリックすると、デバイスは*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*、分離されます。

   - 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。このボタンは、［**Endpoint Detection and Response**］トグルスイッチが有効か無効かにかかわらず使用できます。

7. ［**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。
- アラートの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 と連携している場合、ネットワーク分離の除外は 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、Kaspersky Anti Targeted Attack Platform のヘルプ、またはKaspersky Managed Detection and Response のヘルプを参照してください。

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のプロパティで。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。

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。

Web コンソールでネットワーク分離の除外を追加する方法

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. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response**］に移動します。
5. ［**ネットワーク分離**］セクションで、［**除外リスト**］をクリックします。
   ネットワーク分離の除外リストを含むウィンドウが開きます。
6. 次のいずれかの方法でネットワーク接続を除外できます：
   - ［**追加**］をクリックし、ネットワーク接続に関する情報を入力します。

     コンポーネントがネットワーク接続をブロックしないアプリケーションを追加できます。この設定は、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。

   - ［**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。
7. 変更内容を保存します。

Web コンソールでネットワーク分離の除外を削除する方法

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. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response**］に移動します。
5. ［**ネットワーク分離**］セクションで、［**除外リスト**］をクリックします。
   ネットワーク分離の除外リストを含むウィンドウが開きます。
6. 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、［**削除**］をクリックします。
7. 変更内容を保存します。

ファイルを隔離する

脅威への対応として、Kaspersky Endpoint Detection and Response は*ファイルの隔離*タスクを作成します。これは脅威の影響を最小限にとどめるために必要です。*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。

次の方法で*ファイルの隔離*タスクを作成できます：

- アラートの詳細（EDR Optimum のみ）で作成する。

  *アラートの詳細（Alert details）*は、収集済みの検知した脅威に関する情報を全体的に表示するツールです。アラートの詳細には、コンピューター上に表示されるファイルの履歴が含まれます。アラートの詳細から、削除するファイルを直接選択できます。この結果、Kaspersky Endpoint Security は、検知されたファイルの事前設定されたデータを使用してタスク作成ウィザードを起動します。タスクのスケジュールの設定など、追加のタスク設定のみを管理する必要があります。

- タスクウィザードを使用する。

  新規タスクウィザードでは、削除するファイルまたはディレクトリへのパスとファイルのハッシュを手動で入力できます。タスクのスケジュールの設定など、追加のタスク設定も管理できます。

- *IOC* スキャンタスク設定を使用する。

  IOC スキャンタスクでデータを危険にさらす可能性のあるファイルが検知された場合、IOC スキャン結果からこのファイルを直接隔離することができます（［**アプリケーション設定**］→［**IOC スキャン結果**］）。この結果、Kaspersky Endpoint Security は、検知されたファイルの事前設定されたデータを使用してタスク作成ウィザードを起動します。タスクのスケジュールの設定など、追加のタスク設定のみを管理する必要があります。

ファイルのサイズは 100 MB を超えることはできません。

［ファイルの隔離］タスクを作成する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。

   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**］から［**Kaspersky Endpoint Security for Linux**］を選択します。

   b. ［**タスク種別**］から［**ファイルの隔離**］を選択します。

   c. ［**タスク名**］に簡潔な内容を入力します。

   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

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。

5. ［**終了**］をクリックして、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。

6. 新しいタスクをクリックします。

7. タスクのプロパティウィンドウが表示されます。

8. ［**アプリケーション設定**］タブを選択します。

9. ファイルのリストで、［**追加**］をクリックします。

   ファイルの追加ウィザードが開始されます。

10. ファイルを追加するには、ファイルパスまたはディレクトリパスとファイルのハッシュを入力する必要があります。

11. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。

12. タスクのスケジュールを設定します。

13. 変更内容を保存します。

14. タスクの横にあるチェックボックスをオンにします。

15. ［**開始**］をクリックします。

    Kaspersky Endpoint Security はファイルを隔離します。

ファイルが別のプロセスでロックされている場合は、タスクは*完了*として表示されますが、ファイルそのものはコンピューターが再起動されてから隔離されます。コンピューターの再起動後、ファイルが隔離されたことを確認してください。

実行中のファイルを隔離しようとした場合、*ファイルの隔離*タスクはエラー「*アクセスが拒否されました*」で終了することがあります。ファイルに対してプロセスの終了タスクを作成してから再度実行してください。

サイズが大きいファイルを隔離しようとした場合、*ファイルの隔離*タスクはエラー「*隔離の保管領域に十分な空き容量がありません*」で終了することがあります。隔離を削除するか、隔離のサイズを大きくします。再度実行してください。

デバイスからのファイルの受信

ユーザーのコンピューターからファイルを取得することができます。たとえば、サードパーティのアプリケーションによって生成されたイベントログファイルを取得するようにアプリケーションを設定できます。タスクの実行結果として、ファイルのコピーは隔離に保存されます。*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。Web コンソール（**操作 → リポジトリ → 隔離**）を使用して、隔離からこのファイルをコンピューターにダウンロードできます。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、［*ファイルの取得*］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。

ファイルのサイズは 100 MB を超えることはできません。

［ファイルの取得］タスクを作成する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。

   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**］から［**Kaspersky Endpoint Security for Linux**］を選択します。

   b. ［**タスク種別**］から［**ファイルの取得**］を選択します。

   c. ［**タスク名**］に簡潔な内容を入力します。

   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

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。

5. ［**終了**］をクリックして、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。

6. 新しいタスクをクリックします。

7. タスクのプロパティウィンドウが表示されます。

8. ［**アプリケーション設定**］タブを選択します。

9. ファイルのリストで、［**追加**］をクリックします。
   ファイルの追加ウィザードが開始されます。

10. ファイルを追加するには、ファイルパスまたはディレクトリパスとファイルのハッシュを入力する必要があります。

11. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。

12. タスクのスケジュールを設定します。

13. 変更内容を保存します。

14. タスクの横にあるチェックボックスをオンにします。

15. ［**開始**］をクリックします。

この結果、Kaspersky Endpoint Security はファイルのコピーを作成し、コピーを隔離に移動します。Web コンソールで隔離からファイルをダウンロードします。

［*ファイルの取得*］タスクは、次の場合に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）。

デバイスからのファイルの削除

*ファイルの削除*タスクを使用してリモートからファイルを削除できます。たとえば、脅威への対応としてリモートからファイルを削除する場合などです。

［ファイルの削除］タスクを作成する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
   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**］から［**Kaspersky Endpoint Security for Linux**］を選択します。
   b. ［**タスク種別**］から［**ファイルの削除**］を選択します。
   c. ［**タスク名**］に簡潔な内容を入力します。
   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。
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。
5. ［**終了**］をクリックして、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。
6. 新しいタスクをクリックします。
7. タスクのプロパティウィンドウが表示されます。
8. ［**アプリケーション設定**］タブを選択します。
9. ファイルを追加するには、ディレクトリパスとファイルのハッシュを入力する必要があります。
10. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。
11. タスクのスケジュールを設定します。
12. 変更内容を保存します。
13. タスクの横にあるチェックボックスをオンにします。
14. ［**開始**］をクリックします。

Kaspersky Endpoint Security はコンピューターからファイルを削除します。ファイルが別のプロセスでロックされている場合は、タスクは*完了*として表示されますが、ファイルそのものはコンピューターが再起動されてから削除されます。コンピューターの再起動後、ファイルが隔離されたことを確認してください。

プロセスの開始

*プロセスの開始*タスクを使用してリモートからファイルを実行できます。たとえば、コンピューターの設定ファイルを作成するユーティリティをリモートから実行したりすることができます。次に、*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 Kaspersky Security Center Web コンソールで受け取ることができます。

オペレーティングシステムの SELinux が `Enforcing` モードの場合、*プロセスの開始* タスクを開始するには、SELinux の追加設定を行う必要があります。

「プロセスの開始」タスクを実行するための SELinux の設定方法

オペレーティングシステムで SELinux を `Enforcing` モードで使用する予定の場合、Detection and Response ソリューションとの連携時に対応アクションを実行するには、SELinux の設定を追加で管理する必要があります。

この SELinux の設定には root 権限が必要です。

対応アクション用に SELinux を設定するには：

1. SELinux を Permissive モードに切り替えます：

   - SELinux が有効になっている場合は、次のコマンドを実行します：

     SELinux を Permissive モードに切り替えます

     ```
     setenforce Permissive
     ```

   - SELinux が無効になっている場合は、設定情報ファイル /etc/selinux/config で `SELINUX=permissive` を設定し、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. Detection and Response ソリューションとの連携の一環として使用する対応アクションを実行するには、すべてのタスクを実行します。

4. audit.log ファイルにエラーがないことを確認します。

   audit.log ファイルを表示します

   ```
   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読み込み、エラーを修正してから、対応アクションのタスクを再度実行します。

   ブロック 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読み込みます：

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

6. SELinux を Enforcing モードに切り替えます。

```
setenforce Enforcing
```

［プロセスの開始］タスクを作成する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
   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**］から［**Kaspersky Endpoint Security for Linux**］を選択します。

   b. ［**タスク種別**］から［**プロセスの開始**］を選択します。

   c. ［**タスク名**］に簡潔な内容を入力します。

   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

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。

5. ［**終了**］をクリックして、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。

6. 新しいタスクをクリックします。

7. タスクのプロパティウィンドウが表示されます。

8. ［**アプリケーション設定**］タブを選択します。

9. プロセスの開始コマンドを入力します：

   - **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` ユーティリティを実行する場合は、`/opt/kaspersky/klnagent/bin/klnagchk` と入力します。

   - **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。

   - **作業フォルダーのパス（省略可能）**プロセスがファイルを配置する作業ディレクトリへのパスを入力するフィールドです。

     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。

10. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。

11. タスクのスケジュールを設定します。

12. 変更内容を保存します。

13. タスクの横にあるチェックボックスをオンにします。

14. ［**開始**］をクリックします。

この結果、Kaspersky Endpoint Security はコマンドをサイレントモードで実行し、プロセスを開始します。［**実行結果**］のタスクのプロパティでタスクの結果を確認できます。

プロセスの終了

*プロセスの終了*タスクを使用してリモートからプロセスを終了することができます。たとえば、悪意のある動作の結果として開始されたプロセスをリモートで終了できます。

ファイルの実行をブロックする場合は、実行防止機能を設定することができます。実行ファイル、スクリプト、Office 形式のファイルの実行を禁止することができます。

［プロセスの終了］タスクを作成する方法

1. Web コンソールのメインウィンドウで、［**タスク**］を選択します。
   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**］から［**Kaspersky Endpoint Security for Linux**］を選択します。

   b. ［**タスク種別**］から［*プロセスの終了*］を選択します。

   c. ［**タスク名**］に簡潔な内容を入力します。

   d. ［**タスクを割り当てるデバイス**］ブロックで、タスク範囲を選択します。

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。

5. ［**終了**］をクリックして、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。

6. 新しいタスクをクリックします。

7. タスクのプロパティウィンドウが表示されます。

8. ［**アプリケーション設定**］タブを選択します。

9. プロセスを終了するには、終了するプロセスのファイルを選択する必要があります。次のいずれかの方法でファイルを選択することができます：

   - ファイルの完全名を入力します。

   - ファイルのハッシュとパスを入力します。

- プロセスの PID を入力します（ローカルタスクのみ）。
- ファイルがネットワークドライブにある場合は、ドライブ文字ではなく「`\\`」から開始されるファイルのパスを入力してください。例：「`\\server\shared_folder\file.exe`」。ファイルのパスにドライブ文字があると、*ファイルが見つかりません*というエラーになります。

10. コンピューターのプロパティウィンドウで、［**スケジュール**］タブを選択します。
11. タスクのスケジュールを設定します。
12. 変更内容を保存します。
13. タスクの横にあるチェックボックスをオンにします。
14. ［**開始**］をクリックします。

この結果、Kaspersky Endpoint Security はコンピューター上でそのプロセスを終了します。［**履歴**］のタスクのプロパティでタスクの結果を確認できます。

オブジェクトの実行防止

Kaspersky Endpoint Security が実行防止ルールを受信するカスペルスキー Detection and Response ソリューションと連携する場合、このレスポンスアクションを適用できます。

オブジェクトがルールに一致する場合、Kaspersky Endpoint Security はそのオブジェクトの実行を防止します。

オブジェクトの実行防止（EDR Expert（オンプレミス））

Kaspersky Endpoint Detection and Response Expert（オンプレミス）、Kaspersky Endpoint Detection and Response Expert（クラウド）、または Kaspersky Endpoint Detection and Response (KATA) と連携している場合、対応するソリューションのコンソールで、オブジェクトの実行をブロックするルールを設定できます。

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（**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。

オブジェクトの実行防止を有効にするには、トグルスイッチを **実行防止は有効です** に設定します。

オブジェクトの実行防止（EDR Optimum）

Kaspersky Endpoint Detection and Response Optimum と連携している場合、Web コンソールでオブジェクトの実行防止および実行防止ルールを設定できます。

Kaspersky Security Center ポリシーでオブジェクトの実行防止を有効にする方法

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. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response**］に移動します。
5. ［**実行防止**］タブに移動します。
6. トグルスイッチを［**実行防止は有効です**］にします。
7. オブジェクトを開始または開く時の処理を選択
   - **ブロックしイベントログへ追加する**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を開く操作をブロックし、オブジェクトの実行またはドキュメントを開く操作の試行に関するイベントをイベントログに記録します。
   - **イベントログに追加する**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またはドキュメントを開く操作の試行に関するイベントをログに記録しますが、実際にはオブジェクトの実行やドキュメントを開く操作はブロックしません。
8. 変更内容を保存します。

管理対象デバイスのプロパティでオブジェクトの実行防止を有効にする方法

1. Web コンソールで、［**資産管理**］ →［**アセット（デバイス）**］に移動します。
2. 必要なデバイスの名前のリンクをクリックします。
3. これにより、選択した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、［<**Kaspersky Endpoint Security** アプリケーション名>］リンクをクリックします。
   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. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response**］に移動します。
   5. ［**実行防止**］タブに移動します。
   6. トグルスイッチを［**実行防止は有効です**］にします。

7. オブジェクトを開始または開く時の処理を選択

   - **ブロックしイベントログへ追加する**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を開く操作をブロックし、オブジェクトの実行またはドキュメントを開く操作の試行に関するイベントをイベントログに記録します。

   - **イベントログに追加する**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またはドキュメントを開く操作の試行に関するイベントをログに記録しますが、実際にはオブジェクトの実行やドキュメントを開く操作はブロックしません。

8. 変更内容を保存します。

4. ［**アプリケーション設定**］タブを選択します。

5. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response**］に移動します。

6. ［**実行防止**］サブセクションに移動します。

7. トグルスイッチを［**実行防止は有効です**］にします。

8. オブジェクトの実行防止モードを選択します：

   - **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。

9. 変更内容を保存します。

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。

Web コンソールで EDR Optimum コンポーネントのオブジェクトの実行防止ルールを追加する方法

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. 必要に応じて、［**パスの大文字小文字を区別する**］をオンにします。

5. ポリシーまたは管理対象デバイスのプロパティで、オブジェクトの実行防止ルールのリストの上にあるツールバーで［**追加**］ボタンをクリックします。

6. 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。

7. 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。

8. ［**種別**］ドロップダウンリストで、ブロックするオブジェクトの種別を選択します：

- **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。

9. オブジェクトを追加するには、対応するフィールドに、オブジェクトのパスとオブジェクトのチェックサム（ファイルの SHA256 ハッシュまたは MD5 ハッシュ）の一方または両方を指定します。

10. 変更内容を保存します。

    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。

Kaspersky Endpoint Security は、実行可能ファイルとスクリプトの実行、およびデバイス上でオフィスアプリケーションファイルを開く操作を制御します。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。

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 Detection and Response Optimum ソリューションとの連携が有効になっており、EDR Optimum コンポーネントがアクティベートされています。
- 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っており、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ています。
- Kaspersky Endpoint Detection and Response Expert（クラウド）との連携が有効になっており、EDR Expert（クラウド）コンポーネントがアクティベートされています。

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、オブジェクトの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。

オブジェクトの実行防止に関する制限事項と特記事項

オブジェクトの実行防止の制限事項

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。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）および Kaspersky Endpoint Detection and Response (KATA) と連携する場合のオブジェクトの実行防止に関する特記事項

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 コンソールまたは管理コンソールで、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 と連携する場合のオブジェクトの実行防止に関する特記事項

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。

  アラートの詳細ウィンドウでファイルの実行を防止することで、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。

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）。

Web コンソールでの隔離設定の管理方法

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. ［**全般設定**］→［**レポートと保管領域**］に移動します。
5. ［**隔離**］セクションで、次の設定を指定します：
   - **隔離のサイズを制限する**隔離を指定したサイズ（メガバイト単位）に制限します。既定では、このチェックボックスはオンです。
   - **隔離の最大サイズ（MB）隔離のサイズを制限する** 設定が有効な場合、隔離の最大サイズをメガバイト単位で指定できます（既定では 200 MB）。隔離のサイズは 999,999 MB を超えることはできません。
   - **隔離のサイズの上限に達した場合通知する**隔離の使用率がこの割合に達したことに関する通知。既定では、このチェックボックスはオンです。
     通知が送信される割合を指定できます（既定では 90%）。
6. 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。

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。

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 の連携が有効になっており、EDR Optimum コンポーネントがアクティベートされています。
- 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っており、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ています。
- Kaspersky Endpoint Security と Kaspersky Managed Detection and Response の連携が有効になっており、MDR コンポーネントがアクティベートされています。

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) と連携している場合、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 のヘルプ を参照してください。
- プロセスメモリに対して IOC スキャンタスクを実行した結果。

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。

Endpoint Detection and Response Optimum

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 Security 12.5 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 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。

EDR Optimum コンポーネントを含む Kaspersky Endpoint Security アプリケーションを一元管理するには、Kaspersky Security Center Windows 15.1 または Kaspersky Security Center Linux 15.3、15.4、16.0、16.1、16.2 を使用してください。

このコンポーネントは、Elbrus CPU を搭載したデバイスでは使用できません。

Kaspersky Endpoint Detection and Response Optimum の動作

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 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 Detection and Response Optimum 連携の設定

事前に満たすべき要件

Kaspersky Endpoint Detection and Response Optimum 連携を設定する前に：

- この機能を使用するための別のライセンスを購入している場合は、EDR Optimum のライセンスをアプリケーションに追加します。

Kaspersky Endpoint Detection and Response Optimum を含むライセンスで Kaspersky Endpoint Security を使用している場合、操作は必要ありません。

> Kaspersky Endpoint Security を Light Agent モードで使用する場合、ライセンスは SVM に追加されます。

- 次の項目が有効になっていて、正常に動作していることを確認してください：
  - Kaspersky Security Network（標準モードまたは拡張モード）：

    > 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。

  - Kaspersky Endpoint Security アプリケーションの次のコンポーネント：
    - ファイル脅威対策
    - ふるまい検知

完全なテレメトリを取得し、Kaspersky Security Center で脅威の活動連鎖を構築するには、追加でウェブ脅威対策を有効にする必要があります。

オブジェクトの実行防止を有効にすることもできます。

基本的な設定手順

1. **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。インストール手順の説明については、Kaspersky Endpoint Detection and Response Optimum ヘルプを参照してください。

   インフラストラクチャで Kaspersky Endpoint Detection and Response Optimum の管理にKaspersky Security Center Cloud コンソールを使用している場合、プラグインは既定でインストールされています。

2. **Kaspersky Endpoint Detection and Response Optimum 連携設定の構成**

   次の方法で設定できます：

   - Web コンソールを使用する（Kaspersky Security Center コンソールおよび / またはOSMP コンソール）。
   - 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。

3. **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 Security Center コンソールの脅威レポートから EDR アラートに移動できます。

- 管理対象デバイス上のサードパーティ製アプリケーションイベントに関する情報の送信を有効にします。これを行うには、管理対象デバイスで次のコマンドを実行します：

```
kesl-control --set-app-settings SystemEventsTransmission=Yes
```

> この設定を有効にすると、オペレーティングシステムの負荷が大幅に増大する場合があります。

4. **Kaspersky Endpoint Detection and Response Optimum への接続が正常に確立されていることを確認する**

Kaspersky Endpoint Detection and Response Optimum の状態を都合のよい方法で確認します。Kaspersky Endpoint Detection and Response Optimum 連携が設定されています。脅威が検知されると、アラートが生成されます。アラートの詳細ウィンドウでは、脅威に関する情報を表示し、対応処理を実行できます。

EDR Optimum 連携を有効にする方法

Web コンソールでは、ポリシーのプロパティで、EDR Optimum コンポーネントを有効または無効にし、Kaspersky Endpoint Detection and Response Optimum との連携を設定できます。

Web コンソールで Kaspersky Endpoint Detection and Response Optimum との連携を有効にする方法

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**］タブを選択します。
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. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response**］に移動します。
5. **Endpoint Detection and Response は有効です** トグルスイッチを有効にします。
6. 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 Kaspersky Endpoint Detection and Response Optimum との連携を有効にする方法

EDR Optimum コンポーネントを有効にするには、次のコマンドを実行します：

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

1. Web コンソールのメインウィンドウで、**資産管理** → **資産（デバイス）**セクションを選択します。
2. 必要なデバイスの名前のリンクをクリックします。
3. 選択したデバイスのプロパティウィンドウが開きます。このウィンドウで、**アプリケーション**タブに移動し、<Kaspersky Endpoint Security application name>リンクをクリックします。
4. **アプリケーション設定**タブに移動し、**Detection and Response**セクションをクリックしてから、**Endpoint Detection and Response Optimum**リンクをクリックします。
5. ウィンドウが開きます。このウィンドウで、連携を有効にするために、トグルスイッチを**Endpoint Detection and Response Optimum が有効**に設定します。
6. 必要に応じて、次の設定を管理します：
   - 自動ネットワーク隔離の一環としてのデバイスのブロック期間。

     デバイスのブロック解除を設定するリンクをクリックし、ブロック時間を指定します。
   - 自動ネットワーク隔離の除外リスト
7. 変更内容を保存します。

管理対象デバイスは、Kaspersky Endpoint Detection and Response Optimum との連携用に設定されています。

EDR Optimum 連携が稼働中であることを確認する方法

表示される可能性がある連携ステータスと、その表示タイミングについて確認してください。

EDR Optimum コンポーネントは、次の方法でテストできます：

- コマンドラインで次のコマンドを使用します：

  ```
  kesl-control --app-info
  ```

  EDR Optimum 連携は、**実行中**ステータスで表示されます。
- 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。
  - **アセット管理** → **アセット**セクション → <device name> リンク → **アプリケーション**タブ → <name of the Kaspersky Endpoint Security application> リンク → **全般**タブ → **コンポーネント**の順に移動します。

    Endpoint Detection and Response Optimum コンポーネントは、**実行中**ステータスで表示されます。

Cloud Sandbox

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。

Cloud Sandbox が動作するには、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。

クラウドサンドボックステクノロジーは常に有効になっており、ライセンスの種類に関係なく、Kaspersky Security Network のすべてのユーザーが利用できます。Endpoint Detection and Response Optimum ソリューションを導入済みの場合は、Cloud Sandbox で検知された脅威向けの個別のカウンターを有効にすることができます。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。また、Kaspersky Endpoint Security では Kaspersky Security Center コンソールの*脅威レポート*で Cloud Sandbox 脅威検知技術が表示されます。

Web コンソールで Cloud Sandbox カウンターを有効にする方法

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. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response**］に移動します。
5. ［**Cloud Sandbox**］タブを選択します。
6. **Cloud Sandbox は有効です** トグルスイッチを有効にします。
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。

Endpoint Detection and Response Expert（オンプレミス）

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。Kaspersky Endpoint Detection and Response Expert（オンプレミス）のコンポーネントは、Open Single Management Platform (OSMP) 上に導入されます。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）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。

このコンポーネントは、Elbrus CPU を搭載したデバイスでは使用できません。

Endpoint Detection and Response Expert（オンプレミス）の仕組み

1. **Kaspersky Endpoint Security がインストールされたデバイスは、OSMP の脅威対応処理サーバーおよび OSMP のテレメトリ収集サーバーとの安全な接続を確立します**
2. **Kaspersky Endpoint Security は、OSMP プラットフォーム上のテレメトリ収集サーバーにデータを送信します**

   以下の情報が送信されます：

   - デバイス上のイベントに関する情報
   - アプリケーションによって検出された脅威に関する情報
   - これらの脅威の処理結果に関する情報
   - プロセス、開いているネットワーク接続、変更されたファイルに関する監視データ
3. **Kaspersky Endpoint Security が脅威対応処理を実行します**

   対応処理は、OSMP プラットフォーム上の脅威対応処理サーバーからのコマンドに基づいて実行されます。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携の設定

事前に満たすべき要件

Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携を設定する前に、次の操作を実行します：

- ポート 443 および 8443 での接続を許可します。
- 必要なテレメトリを送信するために、ふるまい検知コンポーネントを有効にします。

  他の保護コンポーネントで検知された脅威に関する情報を取得する場合は、次のコンポーネントを有効にします：

  - 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

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。

- この機能を使用するための個別のライセンスを購入している場合は、EDR Expert（オンプレミス）のライセンスをアプリケーションに追加します。

  Kaspersky Endpoint Security を、Kaspersky Endpoint Detection and Response Expert（オンプレミス）を含むライセンスで使用している場合、対応は必要ありません。

  アプリケーションをLight Agent モードで使用している場合、EDR Expert（オンプレミス）のライセンスは SVM に追加されます。

- また、OSMP プラットフォーム上でコレクター、コリレーター、ストレージを設定する必要があります。

基本的な設定手順

1. **OSMP サーバーによって発行された証明書を取得して処理する**

   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。

   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。

   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。

   証明書を処理するには、PFX 証明書を PEM 形式に変換するの記事に記載されている手順に従います。

   サーバー証明書および / またはクライアント証明書を使用できます。どちらを選択するかは、組織のセキュリティポリシーによって決まります。

2. **Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携設定を行う**

   次の方法で設定できます：

   - Web コンソールを使用する（Kaspersky Security Center コンソールおよび / またはOSMP コンソール）。
   - コマンドラインを使用する。

   オブジェクト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できます。

3. **Endpoint Detection and Response Expert（オンプレミス）プラットフォームへの接続が正常に確立されたことを確認する**

   EDR Expert（オンプレミス）のステータスを任意の方法で確認します。

4 **必要に応じて追加設定を管理する**

- オペレーティングシステムで SELinux が Enforcing モードに設定されている場合、対応処理を実行するには、追加でSELinux を設定する必要があります。
- **メモリダンプ**または**プロセスダンプ**の対応処理を実行するには、ptrace のブロックを解除します。
- ネットワーク分離の制限事項を確認します。
- 管理対象デバイス上のサードパーティ製アプリケーションイベントに関する情報の送信を有効にします。これを行うには、管理対象デバイスで次のコマンドを実行します：

```
kesl-control --set-app-settings SystemEventsTransmission=Yes
```

この設定を有効にすると、オペレーティングシステムの負荷が大幅に増大する場合があります。

EDR Expert（オンプレミス）と正しく統合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。

EDR Expert（オンプレミス）との連携を設定する方法

Web コンソールでは、Kaspersky Endpoint Security のポリシーのプロパティで、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）との連携を設定できます。

Web コンソールで Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携を設定する方法

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. ［**組み込みエージェントの設定**］ → ［**Endpoint Detection and Response Expert（オンプレミス）**］の順に移動します。

5. ［**Endpoint Detection and Response Expert バージョン 8.0 以降**］を選択します。

6. テレメトリ収集サーバーと脅威対応サーバーを追加します。

   これを行うには、［**テレメトリ収集サーバーへの接続**］セクションおよび［**脅威対応サーバーへの接続**］セクションで、［**追加**］ボタンをクリックします。表示されたウィンドウで、サーバーアドレス（IPv4、IPv6）とサーバーに接続するためのポートを指定します。

7. 証明書を追加するには、［**テレメトリ収集サーバーへの接続**］セクションおよび［**脅威対応サーバーへの接続**］セクションで［**接続設定**］リンクをクリックし、表示されたペインで次の操作を実行します：

   a. 対応するセクションで［**アップロード**］ボタンをクリックして、サーバー証明書を追加します。

   b. 追加の保護が必要な場合は、暗号化されたコンテナを作成します。

      これを行うには、［**追加の接続保護**］セクションで次の操作を行います：

      1. ［**相互認証を使用する**］チェックボックスをオンにします。

      2. ［**アップロード**］ボタンをクリックし、メインの連携シナリオを完了したときに受け取ったクライアント証明書を追加します。

      3. 対応するフィールドに、暗号化されたコンテナのパスワードを入力します。

      ［**暗号化されたコンテナのパスワード**］フィールドは必須です。クライアント証明書（暗号化されたコンテナ）のパスワードを入力しないと、設定を保存できません。

8. 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 Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携を設定する方法

1. レスポンスサーバー証明書を追加するには、次のコマンドを実行します：

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type response
```

2. テレメトリサーバー証明書を追加するには、次のコマンドを実行します：

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
```

3. 連携設定を行うには、次のコマンドを実行します：

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

設定項目と指定可能な値を次の表に示します。

4. レスポンスサーバーへの接続用のクライアント証明書を追加するには、次のコマンドを実行します：

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
```

5. テレメトリサーバーへの接続に使用するクライアント証明書を追加するには、次のコマンドを実行します：

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
```

6. EDR Expert（オンプレミス）との連携を有効にするには、次のコマンドを実行します：

```
kesl-control --start-task 24
```

Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携設定

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 アプリケーションは OSMP プラットフォーム上のサーバーと通信します。 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（オンプレミス）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 Expert（オンプレミス）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`。

設定	説明	値
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	デバイス上のイベントに関するデータ（テレメトリ）を OSMP テレメトリ収集サーバーに送信します。	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。		
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 Expert（オンプレミス）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	IOA があるテレメトリ のみを送信します。*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。	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	リクエスト数を制限します。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。	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。

設定	説明	値
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。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携の設定では、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で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）との連携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**を選択します。これにより、Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携設定を編集できるようになります。

Web コンソールまたはコマンドラインを使用してカスペルスキー Endpoint Detection and Response（オンプレミス）と連携するには、EDR Expert（オンプレミス）コンポーネントの設定で EDR（オンプレミス）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。デバイスでカスペルスキー Endpoint Detection and Response（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 以降およびバージョン 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。
- 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。

EDR Expert（オンプレミス）との連携が稼働していることを確認する方法

EDR Expert（オンプレミス）コンポーネントをテストする方法：

- コマンドラインで次のコマンドを使用します：

```
kesl-control --app-info
```

- Web コンソールで。
  - Kaspersky Security Center コンソール内：

    *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。
  - OSMP 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。
    - ［**資産管理 → 資産**］セクションに移動し、［**分析と対応**］タブを選択します。

      デバイスは、テレメトリステータスが［**通常のアクティビティ**］としてリストに表示されます。
    - ［**脅威ハンティング**］セクションに移動します。

      デバイスからのテレメトリイベントがイベントリストに表示されます。

Endpoint Detection and Response Expert（クラウド）

Kaspersky Endpoint Security for Linux と Kaspersky Endpoint Detection and Response Expert（クラウド）の連携機能は、現在一時的にご利用いただけません。この機能は 2026 年末までにサポートされる予定です。アプリケーションのアップグレードと新機能について知るには、リリースノートを確認してください。

Kaspersky Endpoint Security for Linux は、Kaspersky Endpoint Detection and Response Expert（クラウド）ソリューションとの連携をサポートしています。*Kaspersky Endpoint Detection and Response Expert（クラウド）*は、組織がほとんどの種別のサイバーリスクを防ぎ、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カスペルスキー製品を含むクラウドベースのエンタープライズ向けのサイバーセキュリティソリューションです。EDR Expert（クラウド）コンポーネントは、Open Single Management Platform (OSMP) に配備されます。このプラットフォームは、単一のインターフェイスでクロスプラットフォームのシナリオを実行し、カスペルスキー製品とサードパーティ製品を包括的なセキュリティシステムに統合することを可能にします。

ソリューションの中心的な要素の 1 つは *SIEM* です。SIEM は、すべてのコンポーネントからのイベントを追跡し、ベンダーおよびユーザー定義のルールを使用してこれらのイベントを相互に関連付けます。EDR Expert（クラウド）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調べて攻撃を自動的に検出し、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（クラウド）で収集されたすべてのイベントを組み合わせた統合調査グラフを使用してインシデントの調査を可能にします。

高度なインシデントに対応するために、EDR Expert（クラウド）は、事前設定されたシナリオとユーザー定義のシナリオを使用します。サードパーティ製品からの対応処理や、複数のアプリケーションが関係する対応シナリオを使用することもできます。

脅威インテリジェンスツール

Kaspersky Endpoint Detection and Response は次の脅威インテリジェンス（Threat Intelligence）ツールを使用します。

- Kaspersky Threat Intelligence Portal との連携。ファイルや Web アドレスの評価に関する情報を蓄積し、表示できます。
- Kaspersky Threats データベース。
- Kaspersky Security Network（以下、「KSN」とも表記）。クラウドサービスのインフラストラクチャで、カスペルスキーの情報基盤に基づいたリアルタイムのファイル、Web サイト、ソフトウェアの評価情報を提供します。Kaspersky Security Network のデータを使用することにより、新しい脅威に対するカスペルスキー製品の対応が迅速化され、一部の保護機能の効果が高まり、誤検知の可能性が低減されます。

ソリューションの動作原理

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。

コンピューター上のイベントに関する情報（テレメトリ）が EDR Expert（クラウド）サーバーに送信されます。この場合、Kaspersky Endpoint Security は、本製品が検知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テレメトリ収集サーバーに送信します。

EDR Expert（クラウド）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、Open Single Management Platform (OSMP) を使用して管理されるようになります。

EDR Expert（クラウド）の制限事項

- Kaspersky Endpoint Security は、Light Agent モードでは EDR Expert（クラウド）との連携をサポートしていません。
- EDR Expert（クラウド）は、Elbrus CPU を搭載したデバイスでは使用できません。
- EDR Expert（クラウド）は、Arm アーキテクチャに基づくデバイスではサポートされていません。
- EDR Expert（クラウド）は、64 ビット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では使用できません。

組み込みエージェントと EDR Expert（クラウド）の連携を設定する方法

Kaspersky Endpoint Detection and Response Expert（クラウド）ソリューションと連携するには、Endpoint Detection and Response Expert（クラウド）コンポーネントを有効にし、テレメトリ収集サーバーおよび応答サーバーへの接続を設定する必要があります。

*テレメトリの収集サーバー*は、コンピューター上で発生するイベントに関する情報を収集、正規化、関連付け、分析、保存する SIEM ソリューションの一部であるサーバーです。

*応答サーバー*は、データを受信してスキャンし、オブジェクトのふるまいを調査し、そのような調査結果を公開するためのサーバーです。

> *Endpoint Detection and Response（クラウド）*コンポーネントと*Endpoint Detection and Response Expert（オンプレミス）*コンポーネントには互換性がありません。

EDR Expert（クラウド）の動作条件

EDR Expert（クラウド）が動作するには、以下の条件を満たす必要があります。

- Kaspersky Endpoint Detection and Response Expert（クラウド）インフラストラクチャが、お客様の地域で使用可能である。お客様の地域で EDR Expert（クラウド）インフラストラクチャが使用できるかどうかについては、テクニカルサポートにお問い合わせください。
- OSMP（Open Single Management Platform）がインストールされている。
- Kaspersky Endpoint Security が 標準モードでインストールされている。

- Kaspersky Endpoint Security がアクティベートされており、ライセンスがこの機能をサポートしている。
- Kaspersky Endpoint Detection and Response Expert（クラウド）のデータ処理契約の条項に同意している。
- Endpoint Detection and Response Expert（クラウド）機能が有効です。
- 必要なテレメトリを送信するためのふるまい検知コンポーネントが有効になっています。

  他の保護コンポーネントで検知された脅威に関する情報を取得する場合は、次のコンポーネントを有効にします：

  - 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

EDR Expert（クラウド）との連携手順

EDR Expert（クラウド）の連携を設定するには、次の手順を実行します：

1. **EDR Expert モードの選択**

   Kaspersky Endpoint Security は、オンプレミスとクラウドの 2 つの EDR Expert モードをサポートしています。Kaspersky Endpoint Detection and Response Expert（クラウド）と連携するには、アプリケーションのインストール時に対応するモードを有効にする必要があります。既定では、アプリケーションは Endpoint Detection and Response Expert（オンプレミス）との連携を使用します。

2. **Kaspersky Endpoint Detection and Response Expert（クラウド）のアクティベーション**

   Kaspersky Endpoint Detection and Response Expert（クラウド）の個別ライセンスを購入する必要があります。

   この機能は、Kaspersky Endpoint Detection and Response Expert（クラウド）向けの別のライセンスを追加すると使用できるようになります。結果として、Kaspersky Endpoint Security のライセンスおよび Kaspersky Endpoint Detection and Response Expert（クラウド）のライセンスの 2 種類のライセンスがコンピューターに追加されることになります。

   スタンドアロンの Endpoint Detection and Response Expert（クラウド）のライセンスは、Kaspersky Endpoint Security のライセンスと同じです。

   EDR Expert（クラウド）機能がライセンスの対象であり、Kaspersky Security Center または保護対象デバイス上で動作することを確認してください。

3. **テレメトリ収集サーバーおよび応答サーバーへの接続の設定**

Kaspersky Endpoint Detection and Response Expert（クラウド）には、Kaspersky Endpoint Security と 2 つのサーバー（テレメトリ収集サーバーおよび応答サーバー）の間に信頼済み接続が必要です。Kaspersky Endpoint Detection and Response Expert（クラウド）のデータ処理に関する契約の利用条件に同意すると、アプリケーションは信頼済み接続の確立に使用するサーバーアドレスと証明書を自動的に受信します。したがって、サーバーへの接続に関する詳細設定（TCP トンネルを使用するかどうか、およびサーバーと同期するためのリクエストを送信する間隔）のみを管理する必要があります。

Kaspersky Endpoint Security と EDR Expert（クラウド）の接続に関する追加設定を Web コンソールで設定する方法

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**］タブを選択します。

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. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response Expert（クラウド）**］に移動します。

5. ［**Endpoint Detection and Response Expert（クラウド）は無効です**］トグルスイッチを使用してコンポーネントを有効にします。

6. 現在のポリシーが子ポリシーであり、親ポリシーが EDR Expert（クラウド）連携設定の変更を禁止している場合（閉じた南京錠マーク）は、［**継承**］セクションで設定の継承を構成できます。

   - **ポリシーから接続設定を継承する**（既定値）：接続設定は親ポリシーから継承されます。設定を編集することはできません。

   - **カスタム接続設定を使用する**接続設定は手動で構成できます。

7. ［**応答サーバー**］タブには、自動で取得した応答サーバーの完全修飾ドメイン名とポート番号が表示されます。インフラストラクチャのセキュリティポリシーで EDR Expert（クラウド）サーバーへの直接接続が許可されていない場合は、 TCP トンネル経由で接続を設定できます。

   a. ［**応答に TCP トンネルを使用する**］チェックボックスをオンにします。

   b. サーバーアドレス（IPv4、IPv6）とトンネルに接続するポートを指定します。

8. 必要に応じて、［**サーバーに同期リクエストを送信する間隔（分）**］フィールドで、サーバーへの同期要求の送信頻度を設定します。同期中に、Kaspersky Endpoint Security は脅威対応タスクを受信し、タスクの結果を送信します。

9. ［**テレメトリ収集サーバー**］タブに移動します。

10. テレメトリ収集サーバーの接続設定を構成します：

    a. ［**編集**］リンクをクリックします。

    b. ウィンドウが開きます。このウィンドウで、リストからテレメトリ収集サーバーを選択します。KUMA コレクターは、EDR Expert（クラウド）ではテレメトリ収集サーバーとして機能します。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。

    テレメトリ収集サーバーへの接続中にエラーが発生した場合は、別のサーバーを選択してください。テレメトリ収集サーバーに接続できない場合は、テクニカルサポートにお問い合わせください。

    c. 必要に応じて、応答サーバーの場合と同様に、 TCP トンネルを介してテレメトリ収集サーバーへの接続を設定できます。

11. 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。

コマンドラインで証明書情報を表示する方法

1. 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 --query-cloudxdr-client-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-client-certificate --server-type response
```

2. 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 --query-cloudxdr-server-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-server-certificate --server-type response
```

その結果、Kaspersky Endpoint Security によって証明書情報が次のように表示されます：

```
Serial number: 12 34 56 78 AB CD EF GH
Subject: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Issuer: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Valid from: 2022-07-27 13:25:35
Expires on: 2072-07-14 13:25:35
SHA1 fingerprint: a14f12df23fg3465bgh6345g567df
```

コンポーネントの動作状態は*製品コンポーネントのステータスレポート*で表示できます。また、保護対象デバイス上のコンポーネントのステータスを表示することもできます。

EDR Expert（クラウド）のテレメトリ送信を最適化する方法

*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、同期中にテレメトリ収集サーバーに送信します。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。

既定では、本製品は 30 分間隔またはバッファ内のイベントが 1024 件に達すると同期します。同期については Kaspersky Endpoint Security のポリシーで設定できるので、ネットワーク負荷に応じて最適な値を選択することができます（以下の手順を参照）。

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。イベント転送設定で、1 時間ごとの最大イベントを設定するなどしてイベント転送を最適化することができます（以下の手順を参照）。

Web コンソールでテレメトリ送信を最適化する方法

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**］タブを選択します。
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. ［**組み込みエージェントの設定**］→［**Endpoint Detection and Response Expert（クラウド）**］に移動します。
5. 表示されたウィンドウで、**データ転送設定**タブを選択します。
6. ［**テレメトリの送信は有効です**］がオンになっていることを確認してください。
7. 必要に応じて、**IOA のあるテレメトリのみ送信する**機能を有効にします。*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。この機能は既定で無効になっています。
8. 必要に応じて、サーバーの同期設定を構成します。
   - **最大イベント転送遅延時間（秒）**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。既定値は 30 秒です。
   - **イベントパッケージの最大数**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。既定値は 1024 イベントです。
9. ［**リクエストの調整**］タブに移動します。

10. 必要に応じて、［**リクエストの調整が有効です**］トグルスイッチを使用してリクエストの調整をオフにします。

    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。既定で、このオプションはオンです。

11. サーバーへのイベント送信の最適化を設定します：

    - **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。1 時間あたりの既定値は 3000 イベントです。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。既定値は 15 % です。

12. 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。

コマンドラインでテレメトリ送信を最適化する方法

1. テレメトリの送信を有効にするには、次のコマンドを実行します：

```
kesl-control --set-settings 39 [EnableTelemetry=<Yes|No>] [TelemetrySettings.OnlyTaggedEvents=<Yes|No>]
```

2. サーバーとの同期設定を構成するには、次のコマンドを実行します：

```
kesl-control --set-settings 39 [TelemetrySettings.EventTransferSettings.UseRequestCountLimits=<Yes|No>]
[TelemetrySettings.EventTransferSettings.MaximumDataTransferTime=<delay in sending events in seconds>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInHour=<number of events>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInPackage=<number of event packages>]
[TelemetrySettings.EventTransferSettings.EventLimitExceededPercentage=<percentage of exceeding the event
limit>]
```

カスペルスキー Endpoint Detection and Response Expert（クラウド）連携設定

設定	説明
`EnableTelemetry`	デバイス上のイベントに関するデータ（テレメトリ）を OSMP テレメトリ収集サーバーに送信します。 既定で、テレメトリの送信は有効です（`Yes`）。
`TelemetrySettings.OnlyTaggedEvents`	IOA があるテレメトリ のみを送信します。*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。 既定では、IOA があるテレメトリのみの送信は無効です（`No`）。
`[TelemetrySettings.EventTransferSettings]` 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。	
`UseRequestCountLimits`	リクエストの調整これは、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。 既定で、このオプションはオンです。
`MaximumDataTransferTime`	最大イベント転送遅延時間（秒）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。既定値は 30 秒です。

設定	説明
`MaximumNumberOfEventsInHour`	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。1 時間あたりの既定値は 3000 イベントです。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。
`MaximumNumberOfEventsInPackage`	1 パッケージあたりの最大イベント数。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。既定値は 1024 イベントです。
`EventLimitExceededPercentage`	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。既定値は 15 % です。

EDR Expert（クラウド）のテレメトリの除外を設定する方法

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追加できます。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。

使用するルールが多すぎると、テレメトリ収集サーバーへの負荷が増え、コンピューターのパフォーマンスが低下することがあります。必要なルールのみを追加することを推奨します。

Web コンソールでテレメトリの除外を作成するには：

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**］タブを選択します。
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. ［**全般設定**］→［**テレメトリの設定**］に移動します。
5. ［**EDR Expert（クラウド）のテレメトリ**］タブを選択します。
6. ［**全般的な除外**］ブロックの［**追加**］をクリックします。
   テレメトリの除外ルールを追加するウィンドウが開きます。
7. テレメトリの除外ルールを設定します：
   a. 必要に応じて、ルールのステータスを変更します。既定では、ルールは有効になっています。
   b. ルール名を入力します。

c. ルールが適用された際に実行する処理を選択します：

- **収集しない**フィルタリングされたイベントは、送信対象のテレメトリから除外されます。
- **IOA を除外**IOA ルールの適用イベントは、送信対象のテレメトリから除外されます。*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。

d. ［**IOA を除外**］を選択した場合は、除外対象に追加する IOA ルールを指定します：

- **すべて除外**指定した条件が満たされると、本製品はすべての IOAルールに基づいて生成されたイベントをテレメトリから除外します。
- **GUID による除外**IOA ルールの GUID を指定します。「`,`」を使用すると、複数の GUID を指定できます。IOA ルールについて詳しくは、EDR Expert（クラウド）のヘルプを参照してください。

e. フィルタリング条件を指定します：

必要に応じて、**AND**、**OR**、**NOT** 演算子を使用して複数のフィルター条件や条件グループを追加することで、複雑なフィルター条件を作成できます。条件グループには、ネストされた条件や条件グループを追加することもできます。

8. 必要に応じて、［**すべてのイベント種別**］で、イベントの種別ごとにテレメトリ除外を追加します。

a. イベントの種別名をクリックします。

b. 表示されたウィンドウで、［**手動で設定する**］をクリックします。

c. ［**除外ルール**］ブロックの［**追加**］をクリックします。

テレメトリの除外ルールを追加するウィンドウが開きます。テレメトリの除外ルールでは、イベントの種別に対応する `EventType` フィルタリング条件が、ルールにあらかじめ設定されています。

d. フィルタリング条件を指定します：

9. ポリシーをコンピューターに適用するには、南京錠のアイコンが閉じていることを確認し（🔒）、変更を保存します。

EDR Expert（クラウド）のイベントフィルターをエクスポートまたはインポートする方法

除外リストを JSON ファイルにエクスポートすることができます。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、イベントフィルターのバックアップをとったり、別のサーバーにリストを移行することができます。

使用するルールが多すぎると、テレメトリ収集サーバーへの負荷が増え、コンピューターのパフォーマンスが低下することがあります。必要なルールのみを追加することを推奨します。

Web コンソールでイベントフィルターをエクスポートおよびインポートするには、次の操作を行います：

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**］タブを選択します。
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. ［**全般設定**］→［**テレメトリの設定**］に移動します。
5. ［**EDR Expert（クラウド）のテレメトリ**］タブを選択します。
6. イベントフィルターをエクスポートするには：
   a. ［**エクスポート**］をクリックします。
   b. 表示されたウィンドウで、イベントフィルターをエクスポートする JSON ファイルの名前とそのファイルを保存するフォルダーを指定します。
   c. ファイルを保存します。
      Kaspersky Endpoint Security は、イベントフィルターを JSON ファイルにエクスポートします。
7. イベントフィルターをインポートするには：
   a. ［**インポート**］をクリックします。
   b. 表示されたウィンドウで、イベントフィルターをインポートする JSON ファイルを選択します。
   c. イベントフィルタリングルールをインポートする方法として、既存のルールに追加するか、既存のルールを破棄して新しいルールに置き換えるかを選択します。
   d. ファイルを開きます。
8. ポリシーをコンピューターに適用するには、南京錠のアイコンが閉じていることを確認し（🔒）、変更を保存します。
   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**］タブを選択します。
   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. ［**全般設定**］→［**テレメトリの設定**］に移動します。
   5. ［**EDR Expert（クラウド）のテレメトリ**］タブを選択します。
   6. イベントフィルターをエクスポートするには：
      a. ［**エクスポート**］をクリックします。
      b. 表示されたウィンドウで、イベントフィルターをエクスポートする JSON ファイルの名前とそのファイルを保存するフォルダーを指定します。

c. ファイルを保存します。

Kaspersky Endpoint Security は、イベントフィルターを JSON ファイルにエクスポートします。

7. イベントフィルターをインポートするには：

a. ［**インポート**］をクリックします。

b. 表示されたウィンドウで、イベントフィルターをインポートする JSON ファイルを選択します。

c. イベントフィルタリングルールをインポートする方法として、既存のルールに追加するか、既存のルールを破棄して新しいルールに置き換えるかを選択します。

d. ファイルを開きます。

8. ポリシーをコンピューターに適用するには、南京錠のアイコンが閉じていることを確認し（🔒）、変更を保存します。

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform は、組織の IT インフラストラクチャを保護し、ゼロデイ攻撃、標的型攻撃、高度な持続的脅威（以下、APT とも表記）などの脅威を早期に検知するためのソリューションです。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)

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) と連携している場合、Kaspersky Endpoint Security は次の機能を実行します：

- デバイス上のイベントに関する情報（テレメトリ）を、Kaspersky Endpoint Detection and Response (KATA) との連携を提供する Central Node サーバー（以下「*KATA サーバー*」とも表記）に送信します。

  Kaspersky Endpoint Security は、プロセス、開いているネットワーク接続、変更されたファイルに関する監視データを Central Node コンポーネントに送信するとともに、アプリケーションが検知した脅威に関するデータと、それらの脅威の処理結果に関する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、セキュリティを確保するために脅威への対応処理を実行します。

Kaspersky Endpoint Detection and Response (KATA) 7.1 以前との連携がサポートされています。

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

Kaspersky Endpoint Security アプリケーションは、スキャンのためにファイルを、サンドボックスとの連携を処理する Central Node サーバーに送信します。

Kaspersky Endpoint Security の次のコンポーネントにより、Kaspersky Anti Targeted Attack Platform との連携が可能になります：

- 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）。

  Kaspersky Endpoint Security 12.4 for Linux 以降、Endpoint Detection and Response (KATA) コンポーネントの名前は Endpoint Detection and Response Expert（オンプレミス）に変更されました。現在、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) との連携だけでなく、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)（以下、*NDR (KATA)* とも表記）。
- Sandbox。

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。

このコンポーネントは、Elbrus CPU を搭載したデバイスでは使用できません。

Kaspersky Anti Targeted Attack Platform との連携の設定

事前に満たすべき要件

Kaspersky Network Detection and Response (KATA) との連携を設定する前に、ポート 8085 での接続を許可してください。

Kaspersky Endpoint Detection and Response (KATA) コンポーネントとの連携を設定する前に：

- ポート 443、8443 での接続を許可します。
- 必要なテレメトリを送信するために、ふるまい検知コンポーネントを有効にします。

  ふるまい分析コンポーネントは、カーネルバージョン 3.13 以降のデバイスで利用できます。

  他の保護コンポーネントで検知された脅威に関する情報を取得する場合は、次のコンポーネントを有効にします：

  - 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

eBPF ネットワークトラフィックインターセプトモードを有効にすると、テレメトリデータがより包括的になります。eBPF テクノロジーは、eBPF をサポートするカーネルバージョン 4.18 以降を搭載した 64 ビット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で利用できます。

> お使いのコンピューターが、テレメトリの送信に必要なコンポーネントをサポートしているかどうかを確認することを推奨します。

- この機能を使用するために別途ライセンスを購入している場合は、EDR Expert（オンプレミス）のライセンスをアプリケーションに追加します。

  Kaspersky Endpoint Security を、Kaspersky Endpoint Detection and Response Expert（オンプレミス）を含むライセンスで使用している場合、対応は必要ありません。

> 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 に追加する必要があります。

基本的な設定手順

1. **Central Node サーバーが発行した証明書を取得して処理する**

   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。

   > 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に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 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。

   証明書を処理するには、PFX 証明書を PEM 形式に変換するの記事に記載されている手順に従います。

   サーバー証明書および / またはクライアント証明書を使用できます。どちらを選択するかは、組織のセキュリティポリシーによって決まります。

2. **Kaspersky Anti Targeted Attack Platform との連携設定を構成する**

   次の方法で設定できます：

   - Web コンソール（Kaspersky Security Center コンソールの EDR (KATA) および NDR (KATA)、または OSMP コンソール）を使用する。
   - Kaspersky Security Center 管理コンソール（EDR (KATA) および NDR (KATA)）を使用する。
   - コマンドライン（EDR (KATA) および NDR (KATA)）を使用する。

3. **Kaspersky Anti Targeted Attack Platform への接続が正常に確立されたことを確認します。**

   Kaspersky Anti Targeted Attack Platform コンポーネントのステータスを任意の方法で確認します。

4 **必要に応じて追加設定を管理する**

- オペレーティングシステムで SELinux が Enforcing モードに設定されている場合、対応処理を実行するには SELinux を追加で設定する必要があります。
- ネットワーク分離の制限事項を確認します。

EDR (KATA) との連携の設定方法

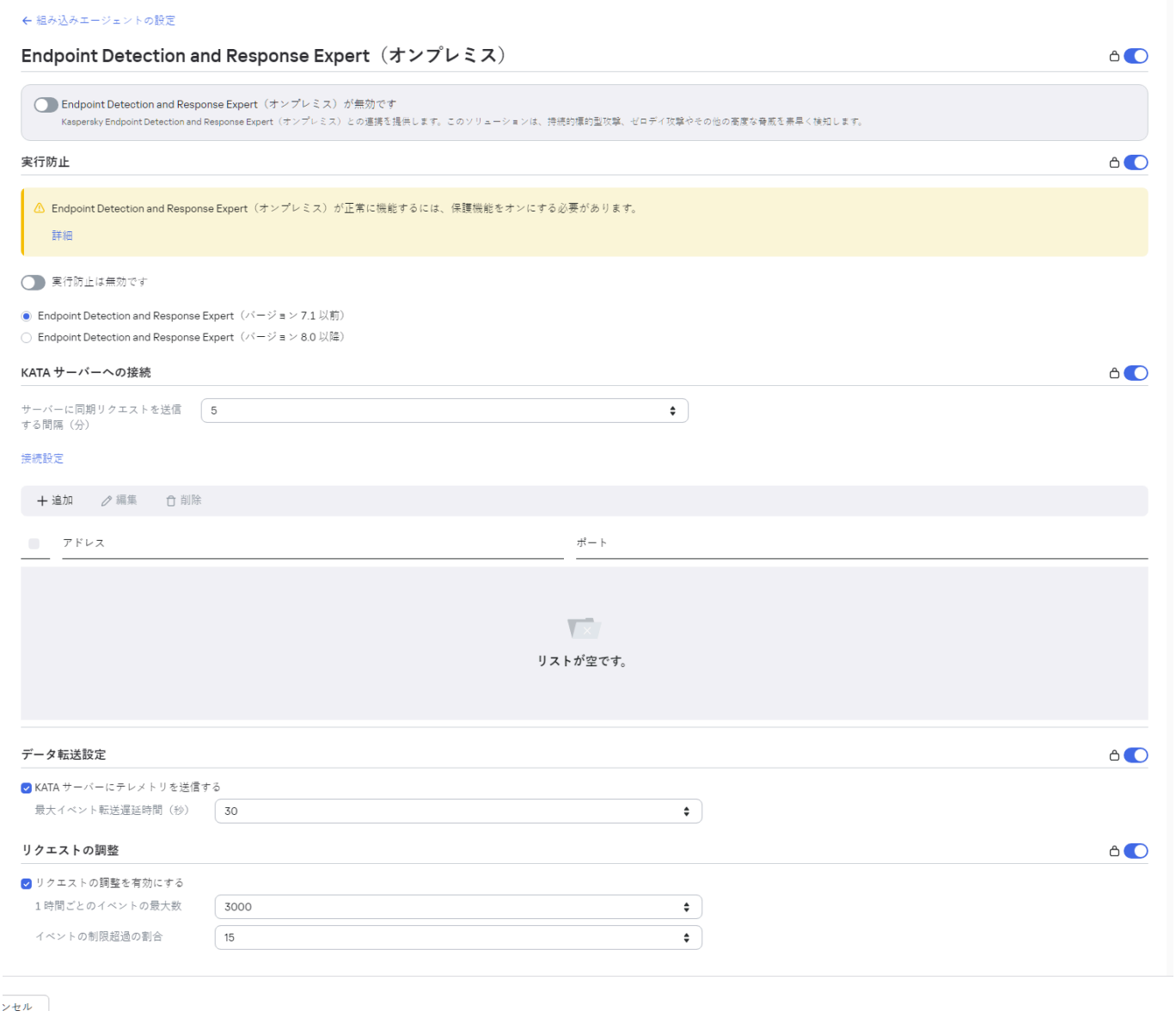
Web コンソールでは、Kaspersky Endpoint Detection and Response (KATA) コンポーネントを有効または無効にし、Kaspersky Endpoint Security アプリケーションとこのコンポーネントとの連携を設定できます。

Web コンソールで Kaspersky Endpoint Detection and Response (KATA) との連携を設定する方法

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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーション設定**］タブを選択します。
5. ［**組み込みエージェントの設定**］ → ［**Endpoint Detection and Response Expert（オンプレミス）**］の順に移動します。
6. 画面の右側で、次の操作を行います：
   a. ［**Endpoint Detection and Response Expert バージョン 7.1 以前**］オプションを選択します。
   b. ［**テレメトリ収集サーバーへの接続**］セクションで、ツールバーの ［**追加**］ボタンをクリックしてテレメトリ収集サーバーを選択し、［**サーバーを選択**］をクリックします。
   c. ［**レスポンスサーバーへの接続**］セクションで、ツールバーの ［**追加**］ボタンをクリックしてレスポンスサーバーを選択し、［**サーバーを選択**］をクリックします。
   d. ［**テレメトリ収集サーバーへの接続**］セクションと［**脅威対応サーバーへの接続**］セクションで、［**接続設定**］リンクをクリックし、表示されたペインで次の操作を行います：
      1. ［**アップロード**］ボタンをクリックして、サーバー証明書を追加します。
      2. 追加の保護が必要な場合は、暗号化されたコンテナを作成します。
         これを行うには、［**追加の接続保護**］セクションで次の操作を行います：
         - ［**相互認証を使用する**］チェックボックスをオンにします。
         - ［**アップロード**］ボタンをクリックし、メインシナリオの手順1で取得したクライアント証明書を追加します。
         - 対応するフィールドに、暗号化されたコンテナのパスワードを入力します。

［**暗号化されたコンテナのパスワード**］フィールドは必須です。クライアント証明書（暗号化されたコンテナ）のパスワードを入力しないと、設定を保存できません。

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。



Endpoint Detection and Response Expert（オンプレミス）

コマンドラインで Kaspersky Endpoint Detection and Response (KATA) との連携を設定する方法

1. EDR (KATA) との連携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 24 Mode=EDRKATA
```

2. Central Node サーバーを追加するには、次のコマンドを実行します：

```
kesl-control --set-settings 24 Endpoints.item_001.Address=<central node server address>
Endpoints.item_001.Port=<central node server port>
```

3. レスポンスサーバー証明書を追加するには、次のコマンドを実行します：

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

4. 連携設定を行うには、次のコマンドを実行します：

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

設定項目と指定可能な値を次の表に示します。

5. レスポンスサーバーへの接続用のクライアント証明書を追加するには、次のコマンドを実行します：

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

6. EDR (KATA) との連携を有効にするには、次のコマンドを実行します：

```
kesl-control --start-task 24
```

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 アプリケーションは OSMP プラットフォーム上のサーバーと通信します。 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（オンプレミス）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 Expert（オンプレミス）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。
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	イベントデータ（テレメトリ）の KATA への送信。	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。

設定	説明	値
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。

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）** オプションを選択します。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 以降またはバージョン 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。
- 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。

NDR (KATA) との連携の設定方法

Web コンソールでは、Kaspersky Network Detection and Response (KATA) コンポーネントを有効または無効にし、Kaspersky Endpoint Security とこのコンポーネントとの連携を設定できます。

Web コンソールで Kaspersky Network Detection and Response (KATA) との連携を設定する方法

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. ［**組み込みエージェントの設定**］ → ［**Network Detection and Response (KATA)**］の順に移動します。
5. ［**Network Detection and Response (KATA)**］切り替えボタンを有効にします。
6. ［**接続設定**］をクリックします。
7. サーバー接続を設定します：
   - **タイムアウト（秒）** 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。

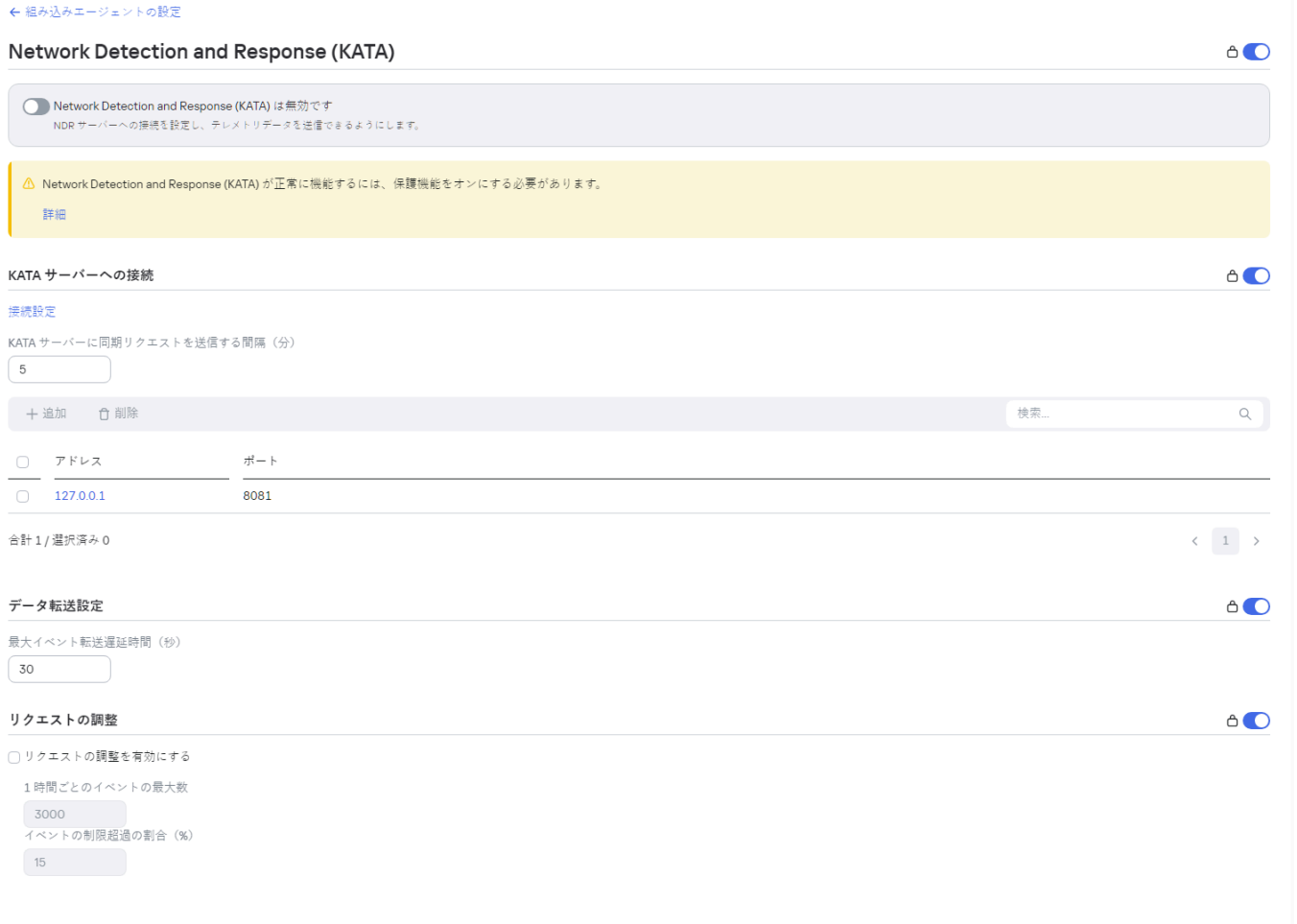
> 暗号化コンテナはパスワードで保護されている必要があります。パスワードを空白にして暗号化コンテナを追加することはできません。

8. ［**OK**］をクリックします。

9. Central Node サーバーを追加します。追加するには、サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定する必要があります。

10. 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。

11. 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。



Network Detection and Response (KATA)

コマンドラインで Kaspersky Network Detection and Response (KATA) との連携を設定する方法

1. Central Node サーバーを追加するには、次のコマンドを実行します：

```
kesl-control --set-settings 31 Endpoints.item_001.Address=<cenral node server address> Endpoints.item_001.Port=
<central node server port>
```

2. レスポンスサーバー証明書を追加するには、次のコマンドを実行します：

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

3. 連携設定を行うには、次のコマンドを実行します：

```
kesl-control --set-settings 31 [<setting name>=<setting value>]
```

設定項目と指定可能な値を次の表に示します。

4. レスポンスサーバーへの接続用のクライアント証明書を追加するには、次のコマンドを実行します：

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

5. NDR (KATA) との連携を有効にするには、次のコマンドを実行します：

```
kesl-control --start-task 31
```

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。
［**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。

設定	説明	値
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。

KATA 連携が正常に動作していることを確認する方法

Kaspersky Anti Targeted Attack Platform コンポーネントは、次の方法でテストできます：

- コマンドラインで次のコマンドを使用します：

  ```
  kesl-control --app-info
  ```

  EDR（オンプレミス）および NDR (KATA) コンポーネントとの連携では、ステータス**利用可能で実行中**が表示されます。

- Web コンソールで：

  - Kaspersky Security Center 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に関するレポート*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。

  - OSMP 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。

    - ［**資産管理 → 資産**］セクションに移動し、［**分析と対応**］タブを選択します。

      デバイスは、テレメトリステータスが **通常のアクティビティ**としてリストに表示されます。

    - ［**脅威ハンティング**］セクションに移動します。

      デバイスからのテレメトリイベントがイベントリストに表示されます。

- Kaspersky Anti Targeted Attack Platform で：

  ［**アセット → デバイス**］セクションに移動します。デバイスが表に表示されます。必要に応じて、**EPP アプリケーション**、**EPP 接続**、**EPP への最終接続**で表をフィルタリングできます。

  デバイスの名前をクリックすると、ペインが開きます。［**エンドポイントエージェント**］セクションで、接続ステータスは［**アクティブ**］です。

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 アプリケーションは、Open Single Management Platform（OSMP）または Kaspersky Anti Targeted Attack Platform を介して Sandbox と連携できます。

このコンポーネントは、Elbrus CPU を搭載したデバイスでは使用できません。

Sandbox との連携を設定する方法

Sandbox との連携の設定を開始する前に：

- 次の受信接続と送信接続を許可します：
  - 受信（管理インターフェイス）：
    - TCP 22
    - TCP 443
    - TCP 8443
  - 送信（管理インターフェイス）：
    - TCP 80 または TCP 443
  - 送信方向および対応する受信方向（処理されたオブジェクトへのアクセス用インターフェイス）：任意のポート。
- ファイルまたはディレクトリのコンテキストメニューから手動でファイルを Sandbox に送信する場合は、グラフィカルインターフェイス（kesl-gui パッケージ）をインストールします。

基本的な設定手順

1. **プラットフォームで Sandbox サーバー接続リクエストを作成し、Sandbox 管理コンソールで接続を確認します**

   詳細については、それぞれのソリューションのヘルプを参照してください：

   - Kaspersky Anti Targeted Attack Platform
   - Open Single Management Platform

   Sandbox サーバーの IP アドレスを任意の方法で保存します。連携の以降の設定で必要になります。

2. **OSMP サーバーまたは中央ノードサーバーによって発行された証明書を取得して処理します**

   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。

   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。

   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。

証明書を処理するには、PFX 証明書を PEM 形式に変換するの記事に記載されている手順に従います。

サーバー証明書および / またはクライアント証明書を使用できます。どちらを選択するかは、組織のセキュリティポリシーによって決まります。

3 Sandbox との連携設定の管理

スキャン用にファイルを送信するには、KATA Sandbox との統合を有効にし、ソリューション内に導入されている Central Node サーバーを追加する必要があります。

Web コンソールで Sandbox との連携を設定する方法

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. ［**組み込みエージェントの設定**］→［**Sandbox**］に移動します。
5. ［**スキャン用ファイルの送信種別**］ドロップダウンリストで、必要な方法を選択します：
   - **手動**このモードでは、コマンドを使用して手動で、または［**Sandbox でのスキャン**］コンテキストメニューから、スキャンするオブジェクトを Sandbox に送信できます。

     > Sandbox のバージョンが 8.0 より前の場合は、このタイプを選択することを推奨します。

   - **自動**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。
   - **複合**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。
6. ［**Sandbox サーバーへの接続**］セクションで：
   - ツールバーの **追加** ボタンをクリックして、Integration Server を追加します。

     アドレスとして、KATA / OSMP プラットフォームの IP アドレスまたは FQDN を指定できます。

     > Sandbox サーバーが OSMP に接続されている場合は、エージェントサーバーの FQDN のみ指定できます。

   - メインシナリオの手順 2で受け取った Kaspersky Anti Targeted Attack Platform または OSMP のサーバー証明書を追加します。

     これを行うには、［**サーバーの接続設定**］リンクをクリックし、表示されたペインの［**サーバー TLS 証明書**］セクションで［**アップロード**］ボタンをクリックします。
   - 追加の保護が必要な場合は、暗号化されたコンテナを作成します。

これを行うには、［**追加の接続セキュリティ**］セクションで次の操作を行います：

- ［**相互認証を使用する**］チェックボックスをオンにします。
- ［**アップロード**］ボタンをクリックし、クライアント証明書を追加します。
- 対応するフィールドに、暗号化されたコンテナのパスワードを入力します。

［**暗号化されたコンテナのパスワード**］フィールドは必須です。クライアント証明書（暗号化されたコンテナ）のパスワードを入力しないと、設定を保存できません。

7. ［**脅威の検知時の処理**］ブロックで関連する操作を選択します。

- **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*簡易スキャンタスク*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 スキャン（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 スキャンタスク*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。

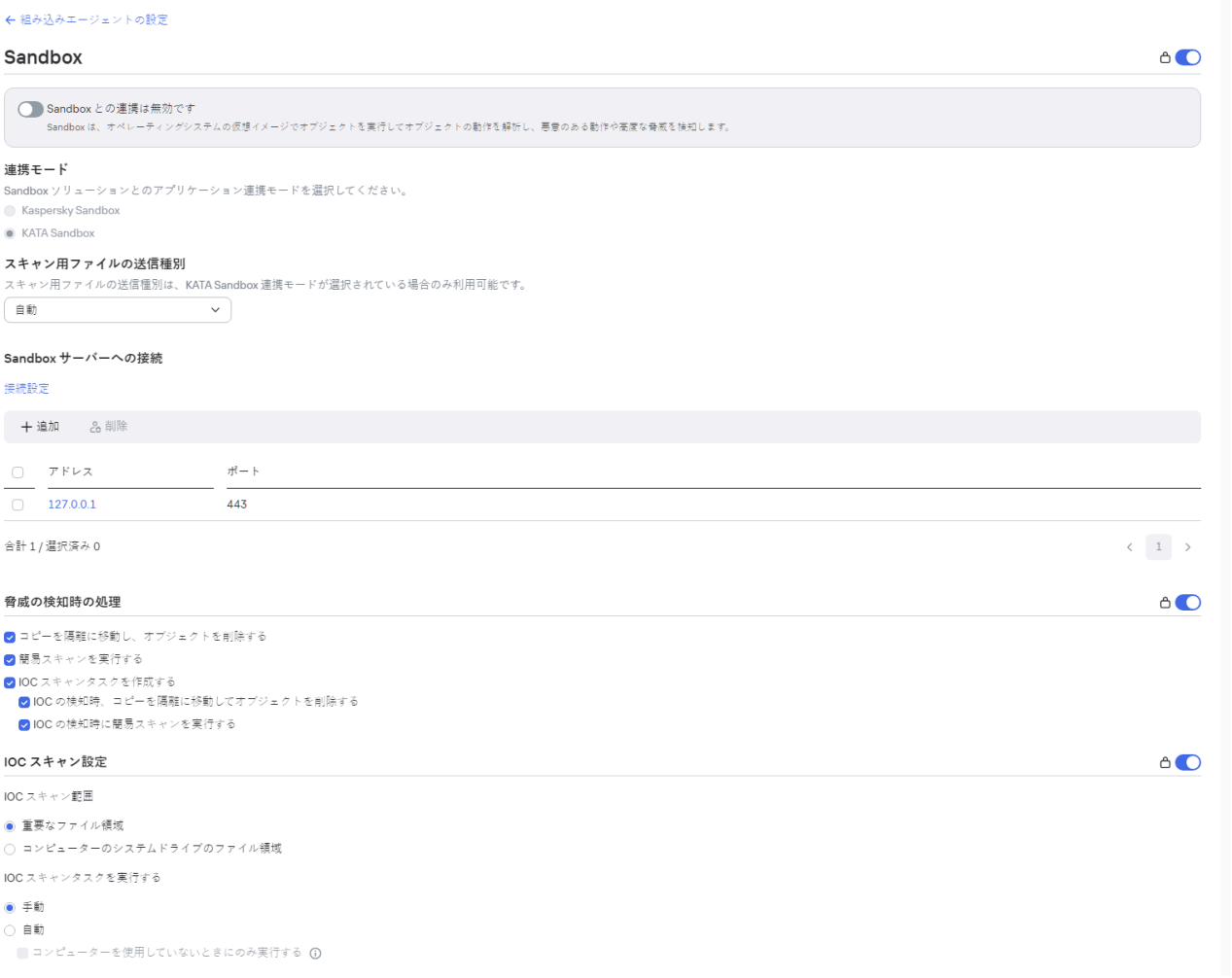
8. 必要に応じて、［**IOC スキャン範囲**］ブロックの［*IOC スキャン*］タスクを設定します。

- **重要なファイル領域**このオプションを選択すると、Kaspersky Endpoint Security はユーザーディレクトリとシステムディレクトリ内でのみ IOC のスキャンを実行します。
- **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すると、Kaspersky Endpoint Security はルートファイルシステム内のすべてのファイルを対象に IOC のスキャンを実行します。

9. 必要に応じて、［**IOC スキャンタスクを実行する**］ブロックの［*IOC スキャン*］タスクを設定します。

- **手動**都合の良いときに手動で *IOC スキャンタスク*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。

10. 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。



Sandbox

コマンドラインで Sandbox との連携を設定する方法

1. サーバー証明書を追加するには、次のコマンドを実行します：

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

2. Central Node または OSMP サーバーを追加するには、次のコマンドを実行します：

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port>
```

3. 連携設定を行うには、次のコマンドを実行します：

```
kesl-control --set-settings 29 [<setting name>=<setting value>]
```

設定項目と指定可能な値を次の表に示します。

4. クライアント証明書を追加するには、次のコマンドを実行します：

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

5. Sandbox との連携を有効にするには、次のコマンドを実行します：

```
kesl-control --start-task 29
```

サンドボックスの連携タスクの設定

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。		

設定	説明	値
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。
[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。

4 **Sandbox への接続が正常に確立されたことを確認する**

Sandbox のステータスを任意の方法で確認します。

Sandbox との連携が正常に動作していることを確認する方法

Sandbox コンポーネントは、次の方法でテストできます：

- コマンドラインで次のコマンドを使用します：

```
kesl-control --app-info
```

  Sandbox との連携は、**使用可能で実行中**ステータスで表示されます。

- Web コンソールで：
  - Kaspersky Security Center コンソール内：

    *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。

  - OSMP 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。
    - ［**脅威ハンティング**］セクションに移動します。

      Sandbox への接続が成功したイベントがイベントのリストに表示されます。

- Kaspersky Anti Targeted Attack Platform で：

  ［**アセット → デバイス**］セクションに移動します。デバイスが表に表示されます。必要に応じて、**EPP アプリケーション**、**EPP 接続**、**EPP への最終接続**で表をフィルタリングできます。

  デバイスの名前をクリックすると、ペインが開きます。［Endpoint Agent］セクションで、接続ステータスが**アクティブ**になります。

ファイルを Sandbox に手動で送信する方法

Kaspersky Endpoint Security では、ユーザーはコンテキストメニューからファイルまたはディレクトリを手動で Sandbox に送信してスキャンできます。

ファイルを Sandbox でスキャンするために送信するには、次の条件を満たす必要があります：

- Kaspersky Endpoint Security のグラフィカルインターフェイスがインストールされている必要があります。
- Kaspersky Endpoint Security が Sandbox と連携されている必要があります。
- スキャン用ファイルの送信モードは、**手動** または **複合** に設定する必要があります。

ファイルまたはディレクトリを Sandbox でスキャンするために送信するには：

1. スキャンするファイルまたはディレクトリの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開くアプリケーションとして、**Kaspersky Endpoint Security 12.5 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. 次に、コンテキストメニューで［**Sandbox でのスキャン**］を選択します。

Kaspersky Managed Detection and Response

Kaspersky Endpoint Security には、Kaspersky Managed Detection and Response ソリューションと統合するための組み込みエージェントが含まれています。*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。

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。コンポーネントは、統合シナリオに記載されているいずれかの方法でアクティベートする必要があります。

このコンポーネントは、Elbrus CPU を搭載したデバイスでは使用できません。

MDR との連携のための Kaspersky Endpoint Security の設定

MDR を使用するには、以下の設定を使用できます：

- **[KES + 組み込みエージェント]**：この設定において、Kaspersky Endpoint Security は、コンピューターのセキュリティを確保するアプリケーションと MDR を操作するアプリケーションの両方の役割を果たします。
- **[サードパーティ製 EPP+EDR エージェント]**.この設定において、IT インフラストラクチャのセキュリティはサードパーティエンドポイント保護プラットフォーム（Endpoint Protection Platform、EPP）によって確保されます。MDR との連携は、Endpoint Detection and Response Agent（EDR Agent）構成の Kaspersky Endpoint Security によって提供されます。この構成では、EDR Agent はサードパーティ製 EPP アプリケーションと互換性があります。

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。

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 コンソールで KPSN 設定情報ファイルをアップロードする方法

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（MMC）で KPSN 設定情報ファイルをアップロードする方法

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。

コマンドラインで KPSN 設定情報ファイルをアップロードする方法

次のコマンドを実行します：

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

MDR 連携を設定する方法

Kaspersky Managed Detection and Response 統合を設定する前に：

- ポート 443 および 1443 での接続を許可します。
- 次のアドレスへの接続を許可します：
  - *.ksn.kaspersky-labs.com
  - ksn-*.kaspersky-labs.com
  - ds.kaspersky.com

> アドレスのリストは変更される場合があります。正確なアドレスを入手するには、テクニカルサポートにお問い合わせください。

- 次の項目が有効になっていて、正常に動作していることを確認してください：
  - Kaspersky Security Network（拡張モード）：
  - ふるまい検知

    テレメトリを完全に取得するために、ウェブ脅威対策、ネットワーク脅威対策、ファイル脅威対策、メール脅威対策の各コンポーネントを追加で有効にできます。

基本的な設定手順

1. **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します**

   - ライセンスを使用します。

     この機能を使用するために別途ライセンスを購入している場合は、MDR ライセンスをアプリケーションに追加します。

     Kaspersky Endpoint Security を、Kaspersky Managed Detection and Response を含むライセンスで使用している場合、操作は必要ありません。

     > Kaspersky Endpoint Security がLight Agent モードで使用されている場合、MDR ライセンスは SVM に追加されます。

   - MDR BLOB ファイルを使用します。

     MDR コンソールで、MDR 設定情報ファイルをダウンロードします。このファイルは、MDR BLOB ファイルと KPSN 設定情報ファイルを含む ZIP アーカイブです。

     次に、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します。

   Kaspersky Endpoint Security アプリケーションのバージョンによって、MDR コンポーネントのアクティベーション方法と、KPSN 設定情報ファイルを使用する必要があるかどうかが決まります。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 Security Center 管理サーバーが階層構造で構成されており、セカンダリサーバーがインターネットに直接アクセスできない場合、プライマリ管理サーバーがインターネットにアクセスできても、Kaspersky Managed Detection and Response は動作しません。

2. **KPSN 設定情報ファイルのアップロード**

   組織に複数のテナントがある場合、または MDR BLOB を使用して MDR コンポーネントをアクティベートした場合は、KPSN ファイルを Kaspersky Security Center 管理サーバーにアップロードします。このファイルには、テレメトリの送信に必要な設定が含まれています。このファイルは、MDR 設定情報ファイルが含まれる ZIP アーカイブ内にあります。

3. **Kaspersky Managed Detection and Response 統合設定を行う**

   Web コンソールで Kaspersky Managed Detection and Response の連携を有効にする方法

   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**］セクションを選択します。
   2. 目的の Kaspersky Endpoint Security ポリシーをクリックします。
   3. 表示されたポリシーのプロパティウィンドウで、［**アプリケーション設定**］タブを選択します。

4. ［**組み込みエージェントの設定**］セクションで［**Managed Detection and Response**］を選択し、画面右側で次の設定を管理します：

   - トグルスイッチを［**Managed Detection and Response は有効です**］にします。

   - テナントがある場合、または 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した場合は、MDR BLOB ファイルを追加するために［**アップロード**］をクリックします。

5. 設定を保存します。

Managed Detection and Response

コマンドラインで Kaspersky Managed Detection and Response の連携を有効にする方法

1. MDR コンポーネントを有効にするには、次のコマンドを実行します：

```
kesl-control --set-app-settings UseMDR=Yes
```

2. BLOB ファイルを追加するには、次のコマンドを実行します：

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

4 KSN ポリシーを設定する

Web コンソールで KSN 設定を管理する方法

1. Kaspersky Endpoint Security ポリシーの［**アプリケーション設定**］タブで、［**全般設定**］セクションに移動します。

2. ［**Kaspersky Security Network**］を選択し、画面右側で次の設定を指定します：

   a. トグルスイッチを［**Kaspersky Security Network（KSN）の使用は有効です**］にします。

   b. ［**KSN 設定**］サブセクションで、［**拡張 KSN モードを使用する**］をオンにします。

c. ［**KSN プロキシサーバー**］サブセクションで、次のチェックボックスをオンにします：

- **管理サーバーを KSN プロキシサーバーとして使用する**
- **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**

設定されたオプションを使用できるかどうかに応じて、テレメトリは管理サーバーまたはデバイスから収集されます。

3. 設定を保存します。

コマンドラインで KSN 設定を行う方法

KSN を拡張モードで有効にするには、次のコマンドを実行します：

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

5. **KSN を有効にする**

Web コンソールで KSN を有効にする方法

1. メインメニューで、管理サーバーの名前をクリックします。
2. 開いたウィンドウの［**全般**］タブで、［**KSN プロキシ**］セクションを選択します。
3. トグルスイッチを［**KSN プロキシの管理サーバーでの有効化が［有効］です**］にします。
4. 使用している KSN インフラストラクチャソリューションに応じて、トグルスイッチを有効にします：
   - **Kaspersky Security Network の使用が［有効］です**
   - ［**Kaspersky Private Security Network の使用が［有効］です**］を有効にしてから、KPSN 設定情報ファイルをアップロードします。
5. 設定を保存します。

6. **Kaspersky Managed Detection and Response への接続が正常に確立されていることを確認します**

任意の方法で Kaspersky Managed Detection and Response のステータスを確認します。

MDR 統合が有効になっていることを確認する方法

Kaspersky Managed Detection and Response コンポーネントの正常性は、次の方法で確認できます：

- コマンドラインで次のコマンドを使用します：

```
kesl-control --app-info
```

Kaspersky Managed Detection and Response の統合は、**利用可能で実行中**のステータスで表示されます。

- MDR コンソールで、**アセット**セクションに移動します。デバイスは**OK**（緑色）のステータスで表示されます。

コンポーネントが無効な場合：

1. アプリケーションの定義データベースをアップデートします。
2. Kaspersky Security Network が拡張モードで有効になっていて、実行中であることを確認します。
3. Kaspersky Endpoint Security と MDR のライセンスを確認します。
4. BLOB ファイルがポリシーに追加されていることを確認します。
5. MDR に必要なコンポーネントが正常に動作していることを確認します。

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Endpoint Security for Linux 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。

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 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。

> このコンポーネントは、Elbrus CPU を搭載したデバイスでは使用できません。

KUMA 連携を設定する方法

Kaspersky Unified Monitoring and Analysis Platform との連携を設定する前に：

- ポート 443 および 1443、または KUMA コレクター側で設定されているポートでの接続を許可します。
- この機能を使用するために別途ライセンスを購入している場合は、KUMA ライセンスをアプリケーションに追加します。

  Kaspersky Unified Monitoring and Analysis Platform が含まれるライセンスに基づいて Kaspersky Endpoint Security を使用している場合、操作は必要ありません。

  アプリケーションを Light Agent モードで使用している場合、KUMA ライセンスは SVM に追加されます。

基本的な設定手順

1. **KUMA で、コレクターとノーマライザーを設定します。**

   > クライアント証明書を使用する場合は、**トランスポート**タブでコレクターを設定するときに、TCP コネクタータイプを選択します。次に、**詳細設定**タブの**TLS モード**ドロップダウンリストで、**クライアント認証付きカスタム PFX** を選択します。

2 **接続先のコレクターのアドレスをコピーする**

KUMA の **リソース → アクティブなサービス** セクションの サービスのテーブル で、**FQDN / IP アドレス** 列と **ポート** 列の値をコピーし、任意の方法で保存します。

> 接続に TLS を使用している場合は、完全修飾ドメイン名（FQDN）のみを指定します。設定値では大文字と小文字が区別されます。

3 **KUMA サーバーによって発行された証明書を取得して処理する**

> KUMA サーバーへの UDP 接続では、接続の保護に証明書を使用することはサポートされていません。

> 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。

サーバー証明書（マイクロサービス CA 証明書）を取得します。詳細は、CA 証明書のダウンロードを参照してください。証明書を処理するには、PFX 証明書の PEM 形式への変換の記事の手順に従って、DER 形式または PEM 形式に変換します。

保護を強化するために、コレクターの設定時に取得したクライアント証明書も使用できます。手順 1 を参照してください。

4 **Kaspersky Unified Monitoring and Analysis Platform との連携設定を行う**

Kaspersky Security Center Web コンソールで KUMA 連携を設定する方法

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. ［**組み込みエージェントの設定**］→［**KUMA 連携**］に移動します。
5. **KUMA 連携は有効です** トグルスイッチを有効にします。
6. KUMA サーバーを追加します。
   a. ［**追加**］をクリックします。
      これにより、KUMA サーバーを追加できるフォームが開きます。
   b. KUMA サーバーに接続するためのプロトコル（**HTTP/HTTPS**、**TCP**、**UDP**）を選択します。
      Kaspersky Endpoint Security でコレクターに接続するためのプロトコルは、KUMA のコネクタタイプ（**http**、**tcp**、または**udp**）と一致している必要があります。
      HTTP/HTTPS プロトコルを選択した場合、本製品は既定で KUMA サーバーへの接続に HTTPS を使用します。HTTP を使用するには、サーバーアドレスにこのプロトコルを手動で指定する必要があります（例：`http://server.com`）。

c. サーバーアドレス（IPv4、IPv6）とサーバーに接続するポートを指定します（既定ではポート 443 が指定されています）。

KUMA コンソールのコネクタプロパティでサーバーアドレスを確認できます。KUMA コネクタの詳細については、Kaspersky Unified Monitoring and Analysis Platform のヘルプを参照してください。

d. ［**OK**］をクリックします。

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。

7. 必要に応じて、［**サーバーの接続設定**］ブロックの［**イベント送信時の最大遅延（秒）**］を設定します。指定された時間が経過すると、Kaspersky Endpoint Security は同じコレクターへの接続を試みます。コレクターが複数ある場合は、リスト内の次のコレクターに接続します。既定値は 30 秒です。

8. 変更内容を保存します。

コマンドラインで KUMA 連携を設定する方法

1. KUMA サーバーを追加するには、次のコマンドを実行します：

```
kesl-control --set-settings 33 Servers.item_001.ServerAddress=<kuma server address>
Servers.item_001.Port=<kuma server port> Servers.item_001.ServerProtocol=<tcp|HTTPWithCompression|udp>
```

2. KUMA サーバー証明書を追加するには、次のコマンドを実行します：

```
kesl-control [-M] --add-kuma-server-certificate <path to the file>
```

3. 連携設定を行うには、次のコマンドを実行します：

```
kesl-control --set-settings 33 [<setting name>=<setting value>]
```

設定項目と指定可能な値を次の表に示します。

4. レスポンスサーバーへの接続用のクライアント証明書を追加するには、次のコマンドを実行します：

```
kesl-control [-M] --add-kuma-client-certificate <path to the file>
```

5. EDR (KATA) との連携を有効にするには、次のコマンドを実行します：

```
kesl-control --start-task 33
```

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。 HTTPWithCompression — イベント圧縮を使用する HTTP 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。
[KumaTransferSettings] 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。

5 Kaspersky Unified Monitoring and Analysis Platform への接続が正常に確立されたことを確認する

KUMA のステータスを任意の方法で確認します。

KUMA 連携が正常に動作していることを確認する方法

KUMA コンポーネントは次の方法でテストできます：

- コマンドラインで次のコマンドを使用します：

  ```
  kesl-control --app-info
  ```

  KUMA との連携は、**使用可能で実行中**ステータスで表示されます。

- Web コンソール（OSMP コンソール）で：

  脅威ハンティングセクションに移動します：該当するデバイスの「KUMA への接続が確立されました」ステータスのテレメトリイベントがイベントリストに表示されます。

- Kaspersky Unified Monitoring and Analysis Platform で：

  KUMA コンソールのメインメニューで、**イベント**セクションに移動します：Kaspersky Endpoint Security のテレメトリイベントがリストに表示されます。

仮想環境の保護

Kaspersky Endpoint Security は、Kaspersky Security for Virtualization Light Agent の一部として動作するための Light Agent モードをサポートしています。*Kaspersky Security for Virtualization Light Agent* は、ネットワーク攻撃やフィッシング攻撃を含む様々なセキュリティ上の脅威から仮想マシンを包括的に保護する統合ソリューションです。このソリューションを使用するには、本製品を Light Agent モードでインストールする必要があります。

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または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 は、仮想マシンと SVM 間の連携を処理します。*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。

Light Agent と SVM の接続

1. **使用可能な SVM のリストの取得**

   Light Agent は、使用可能な SVM のリストを取得します。

2. **最適な Protection Server（SVM）の選択**

   Light Agent が、SVM 選択アルゴリズムに基づいて、接続に最適である使用可能な Protection Server（SVM）を決定します。

3. **追加の接続設定の確認**

   Light Agent は、追加の SVM 接続設定（タグ、接続の保護ステータス、ライセンスに含まれる製品機能）を確認します。

4. **Light Agent と SVM の接続**

   Light Agent は、選択した SVM との接続を確立し、維持します。

SVM 検出を設定する方法

Light Agent の SVM 検出方法を 1 つ選択できます：

- Integration Server (VIIS) の使用

  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したり、接続可能な SVM のリストを生成するソリューションのコンポーネントです。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、大規模な仮想インフラストラクチャにおいて特に有用です。VM 間の負荷を自動的に分散し、利用可能な SVM に関する情報を取得し、この情報を分析し、接続に最適な Protection Server (SVM) のリストを Light Agent に提供するためです。

  Light Agent が SVM のリストを取得できるようにするのに必要な操作は、Integration Server のアドレスを入力することだけです。

- Integration Server の高可用性クラスターを使用する。

  Kaspersky Security for Virtualization Light Agent 6.4 では、Integration Server の高可用性クラスターを導入できます。Integration Server の高可用性クラスターでは、プライマリ Integration Server に障害が発生した場合に SVM と Light Agent がバックアップ Integration Server にフェイルオーバーするため、仮想環境を中断なく保護できます。サーバーのフェイルオーバーは、クラスターの特別なコンポーネントである*ロードバランサー*が担います。Integration Server の高可用性クラスターについて詳しくは、Kaspersky Security for Virtualization Light Agent のヘルプを参照してください。

  Light Agent が SVM のリストを取得するには、ロードバランサーがインストールされているデバイスのアドレスを入力する必要があります。

- SVM アドレスのカスタムリストの使用。

  Light Agent が接続する個々の SVM を指定する必要がある場合は、リストを手動で準備できます。

  Light Agent が接続できる使用可能な SVM のアドレスをリストアップする必要があります。

Web コンソールで Light Agent による SVM 検出を設定する方法

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. ［**Light Agent モード**］→［**SVM 検出設定**］に移動します。

5. SVM 検出方法を選択します。

- **Integration Server を使用する**インフラストラクチャに応じて、Integration Server への接続設定を入力してください：

  - **単一の Integration Server**。Integration Server への接続設定として、デバイスの IPv4 アドレスまたは完全修飾ドメイン名（FQDN）を入力してください。

  - **Integration Server の高可用性クラスター**。クラスターに含まれるロードバランサーの IP アドレスとポートを入力してください。

- **SVM アドレスのカスタムリストを使用する**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。各リスト項目は新しい行に入力するか、セミコロン（`;`）で前の項目と区切る必要があります。

  > 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。

6. 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 Light Agent と Integration Server との接続に関する情報を表示するには：

1. アプリケーションが Light Agent モードでインストールされていることを確認します：

   ```
   kesl-control -V --ksvla-info
   ```

   コンポーネントのステータスは**オン**である必要があります。

2. Light Agent と Integration Server との接続に関する情報を出力します：

   ```
   kesl-control -V --viis-info
   ```

コマンドは次の情報をコンソールに出力します：

- Light Agent が接続する Integration Server のアドレスとポート。
- Integration Server への接続のステータスです。
- Light Agent と Integration Server 間の最終接続日時。

コマンドラインで Light Agent と Integration Server との接続に関する情報を表示する方法

1. アプリケーションが Light Agent モードでインストールされていることを確認します：

   ```
   kesl-control -V --ksvla-info
   ```

   コンポーネントのステータスは**オン**である必要があります。

2. Light Agent と Integration Server との接続に関する情報を出力します：

   ```
   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 が SVM を選択する方法

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

Light Agent は、接続に次の SVM 選択アルゴリズムを適用できます：標準アルゴリズム（既定）および拡張アルゴリズム。

標準アルゴリズム	拡張アルゴリズム
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。 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。 SVM 上の Protection Server に対して大規模インフラストラクチャ保護モードが有効になっている場合、アプリケーションは SVM が Light Agent に対してローカルであるかどうかを判断しません。この場合、拡張 SVM 選択アルゴリズムを使用し、SVM 検出方法として Integration Server を選択することを推奨します。 Light Agent に対して SVM がローカルとみなされるかどうかは、仮想インフラストラクチャの種別によって異なります。	このアルゴリズムを適用する場合、次の SVM 選択設定を定義できます： • 接続用の SVM を選択する際にインフラストラクチャ内の SVM の場所を考慮するか無視するか • SVM の場所を考慮する場合、Light Agent に対して SVM がローカルかどうかを判断する方法 Light Agent がインフラストラクチャ内の SVM の場所を無視する場合、Light Agent は接続可能な任意の SVM に接続できるようになります。 Light Agent がインフラストラクチャ内の SVM の場所を考慮する必要がある場合は、Light Agent に対して SVM がローカルかどうかを判断する際に考慮する SVM パスタイプを選択する必要があります。Light Agent に対して SVM がローカルであるかどうかは、仮想インフラストラクチャの種別に応じて決定されます。 Light Agent が接続先の SVM を選択する際にインフラストラクチャ内の SVM の場所を考慮する場合、Light Agent はローカルの SVM にのみ接続できます。 たとえば、ハイパーバイザーのクラスタを SVM パスの種別として指定した場合、このハイパーバイザーのクラスタに導入された SVM はすべて Light Agent によりローカルであると判断され、Light Agent はこの SVM にのみ接続可能となります。Light Agent が動作している同じクラスタに接続できる SVM がない場合、Light Agent は SVM に接続しません。 SVM の選択時に、Light Agent は 接続されている Light Agent の数も考慮して、接続のために使用できる SVM の中で Light Agent を均等に分散します。 Light Agent が高度な SVM 選択アルゴリズムを使用し、SVM アドレスのリストが SVM 検出方法として選択されており、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っている場合、Light Agent をこの SVM に接続できるのは、SVM パスが無視された場合のみです。
Basis Dynamix Enterprise	
Basis Dynamix Enterprise ベースの仮想インフラストラクチャでは、Light Agent がインストールされている仮想マシンと同じノード上に SVM が導入されている SVM は Light Agent のローカルと判断されます。	Basis Dynamix Enterprise ベースの仮想インフラストラクチャでは、次のいずれかの場合に、Light Agent に対して SVM がローカルであると判断されることがあります： • SVM が、Light Agent がインストールされた仮想マシンと同一のノードに導入されている。 • SVM が、Light Agent がインストールされた仮想マシンと同一のゾーンに導入されている。 • SVM が、Light Agent がインストールされた仮想マシンと同一のデータセンターに導入されている。
Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer、および Basis Dynamix Standard	

標準アルゴリズム	拡張アルゴリズム
Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer、または Basis Dynamix Standard ベースの仮想インフラストラクチャでは、Light Agent がインストールされている仮想マシンと同じハイパーバイザー上に導入されている SVM が、Light Agent に対してローカルと判断されます。	Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer、または Basis Dynamix Standard ベースの仮想インフラストラクチャでは、次のいずれかの場合に、Light Agent に対して SVM がローカルであると判断されることがあります： • SVM が、Light Agent がインストールされた仮想マシンと同一のハイパーバイザーに導入されている。 • SVM が、Light Agent がインストールされた仮想マシンと同一のハイパーバイザーのクラスタに導入されている。 • SVM が、Light Agent がインストールされた仮想マシンと同一のデータセンターに導入されている。
OpenStack および VK Private Cloud SVM	
OpenStack または VK Private Cloud プラットフォーム上で稼働する仮想インフラストラクチャでは、Integration Server 設定情報ファイル appsettings.json の［`HypervisorSpecificSettings:Openstack`］セクションにある［`StandardAlgorithmSvmLocality`］パラメータを使用して、SVM が Light Agent に対してローカルであるかどうかを判断する方法を指定できます。Integration Server のバージョンに応じて、ファイルは次のいずれかのパスにあります： • /var/opt/kaspersky/viis/common/：Linux ベースの Integration Server 用ファイル • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\：Windows ベースの Integration Server 用ファイル ［`StandardAlgorithmSvmLocality`］パラメータが取り得る値は、次のとおりです： • `ServerGroup` – この値を選択すると、SVM は Light Agent からローカルであると判断されます（Light Agent がインストールされた仮想マシンと同一のサーバーグループに配置されている場合）。この値は既定で使用されます。 • `Project` - この値を選択すると、SVM は Light Agent からローカルであると判断されます（Light Agent がインストールされた仮想マシンと同一の OpenStack プロジェクトに配置されている場合）。 • `AvailabilityZone` – この値を選択すると、SVM は Light Agent からローカルであると判断されます（Light Agent がインストールされた仮想マシンと同一のアベイラビリティゾーンに配置されている場合）。	OpenStack または VK Private Cloud プラットフォーム上で稼働する仮想インフラストラクチャでは、次のいずれかの場合に、Light Agent に対して SVM がローカルであると判断されることがあります： • SVM が、Light Agent がインストールされた仮想マシンと同一のサーバーグループに配置されている。 • SVM が、Light Agent がインストールされた仮想マシンと同一の OpenStack プロジェクトに導入されている。 • VM が、Light Agent がインストールされた仮想マシンと同一のアベイラビリティゾーンに配置されている。

SVM 接続アルゴリズムに加えて、タグを使用して複数の SVM に対する複数の Light Agent の接続を制限できます。

Web コンソールで Light Agent の SVM 選択アルゴリズムを設定する方法

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. ［**Light Agent モード**］→［**SVM 選択アルゴリズム**］に移動します。

5. アルゴリズムを選択します：

   - **標準の SVM 選択アルゴリズムを使用する**Light Agent は、同じハイパーバイザーに導入された SVM を選択します。

   - **拡張 SVM 選択アルゴリズムを使用する**Light Agent は、選択された種別の SVM パスに導入された SVM を選択します（既定では、［**ハイパーバイザー**］）。

6. 必要に応じて、拡張 SVM 選択アルゴリズムの SVM パスを選択します：

- **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、XenServer、 VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、 ALT Virtualization Server、 Astra Linux、Numa vServer、 または Basis Dynamix Standard ベース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た仮想マシンと同じサーバーグループに配置されます（OpenStack または VK Private Cloud プラットフォーム上で稼働する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た仮想マシンと同じノードに配置されます（Basis Dynamix Enterprise の仮想インフラストラクチャ内）。

  Light Agent を含む仮想マシンが配置されている同じハイパーバイザー上または同じサーバーグループ内に接続に使用可能な SVM がない場合、Light Agent は SVM に接続しません。

- **クラスター**Light Agent は、基準を満たす接続先の SVM を選択します（仮想インフラストラクチャの種別に応じて）：

  - SVM は、Light Agent がインストールされた仮想マシンと同じハイパーバイザーのクラスタ上に導入されます（Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、 ALT Virtualization Server、 Astra Linux、Numa vServer、 または Basis Dynamix Standard ベース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た仮想マシンと同じ OpenStack プロジェクトに導入されます（OpenStack または VK Private Cloud プラットフォーム上で稼働する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た仮想マシンと同じゾーン内に配置されます（Basis Dynamix Enterprise の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、XenServer、 VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、 ALT Virtualization Server、 Astra Linux、Numa vServer、 または Basis Dynamix Standard ベース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た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 または VK Private Cloud プラットフォーム上で稼働する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た仮想マシンと同じデータセンター内に配置されます（Basis Dynamix Enterprise の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**Light Agent は、Protection Server に接続するための SVM パスを無視します。Light Agent は、タグ、SVM に接続されている Light Agent の数など、他の条件を考慮します。

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。

Light Agent の接続を SVM 間で分散する方法

複数の Light Agent を 1 つの SVM に接続することができます。Light Agent の接続を分散するために、SVM の個別のリストを指定できます。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。

Web コンソールで Light Agent に SVM 接続タグを割り当てる方法

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. ［**Light Agent モード**］→［**SVM 接続タグ**］に移動します。
5. ［**接続タグを使用する**］をオンにして、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。
6. 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。

Light AgentとSVM間の接続の保護

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 のパフォーマンスが低下する可能性があります。

Web コンソールの Light Agent で接続保護を設定する方法

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. ［**Light Agent モード**］→［**接続の保護**］に移動します。
5. ［**Light Agent と Protection Server 間のデータチャネルを暗号化する**］チェックボックスをオンにします。
6. 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。

Light Agent のステータスを確認する方法

コマンドラインでは、Light Agent モードで使用されている本製品に関する次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 モードで本製品を使用する際の設定に関する情報の表示

```
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：

- 仮想環境保護用 Light Agent モード：オンまたはオフ。
  Light Agent モードが有効な場合、アプリケーションは Kaspersky Security for Virtualization Light Agent ソリューションの一部として使用されます。
- VDI 保護モード：オンまたはオフ。
  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。

- 仮想マシン種別：永続的または非永続的。
- 仮想マシンロール：サーバーまたはワークステーション。
- 仮想マシン ID：UUID。

Light Agent と Integration Server との接続に関する情報の表示

```
kesl-control [-V] --viis-info
```

コマンドは次の情報をコンソールに出力します：

- Light Agent が接続する Integration Server のアドレスとポート。
- Integration Server への接続のステータスです。
- Light Agent と Integration Server 間の最終接続日時。

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 Security for Virtualization Light Agent のヘルプを参照してください。

Light Agent と SVM との接続に関する情報の表示

```
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。

ベストプラクティス

Kaspersky Endpoint Security for Linux の導入時、本セクションに記載されている推奨事項を使用して、コンピューターの保護を設定し、パフォーマンスを最適化できます。コンピューターのパフォーマンスの問題の対処方法については、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。

製品によるリソース消費の最適化

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。

本製品によるシステムリソースの消費を最適化するための推奨設定シナリオ：

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、ネットワーク脅威対策、およびふるまい検知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、これらのコンポーネントのパフォーマンスを最適化します。

5. **すべてのデバイス上で本製品を設定します。**

   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。

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。

本製品によるリソース消費に関する情報の表示

```
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。

本製品のパフォーマンスに関する情報を取得するには、本製品が使用するオペレーティングシステムリソースのメトリックの収集を設定することもできます。

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、デバイスで次の実験を行います：

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、該当するタスクの推奨事項に従うことができます。

   ファイル脅威対策タスクのリソース消費を分析する方法

   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. 本製品のすべてのタスクの一覧を取得します：

      ```
      kesl-control --get-task-list
      ```

      b. 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 <task ID |name>
      ```

      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、スケジュールを変更します：

```
kesl-control --set-schedule <task ID |name> RuleType=Manual
```

3. 詳細度の高い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、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のと同じモードで、システムに負荷をかけます。数時間あれば十分です。

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 ContainerScan タイプのタスク）またはふるまい検知タスクである可能性が最も高くなります。スキャンタスクを最適化するか、ふるまい検知タスクのパフォーマンスを分析する必要があります。

7. アプリケーショントレースファイルの作成を無効にします：

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

2 ふるまい検知タスク（Behavior_Detection タイプのタスク）によるリソース使用状況を分析します。

このようにして、パフォーマンスの問題がふるまい検知タスクに関連しているのか、スキャンタスク（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、該当するタスクの推奨事項に従うことができます。

ふるまい検知タスクによるリソース使用状況を分析する方法

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. 本製品のすべてのタスクの一覧を取得します：

```
kesl-control --get-task-list
```

b. 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 <task ID|name>
```

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、スケジュールを変更します：

```
kesl-control --set-schedule <task ID|name> RuleType=Manual
```

3. 詳細度の高い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. ふるまい検知タスクが実行されていない場合は、開始します：

```
kesl-control --start-task 20
```

5. パフォーマンスの問題を引き起こしたのと同じモードで、システムに負荷をかけます。数時間あれば十分です。

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、ふるまい検知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 ContainerScan 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. アプリケーショントレースファイルの作成を無効にします：

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

3 最も頻繁にスキャンされるオブジェクトの特定

危険性のない、頻繁にスキャンされるオブジェクトやファイルを、ファイル脅威対策とスキャンタスクのパフォーマンスを最適化するためにスキャンから除外できます。

最も多くスキャンされたオブジェクトが危険かどうかを判断します。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。

最も頻繁にスキャンされるオブジェクトを特定する方法

1. 最も多くスキャンされたオブジェクトの一覧を取得します：

```
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 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` を追加できます。ここで、X はネストの深さです。例：

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

2. 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多くスキャンされたパスの一覧を取得します：

```
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` を追加できます。ここで、X はネストの深さです。例：

```
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
```

4 Kaspersky Endpoint Security による起動の検知頻度が最も高いプロセスの特定

危険性のない、頻繁に起動されるプロセスを、ふるまい検知のパフォーマンスを最適化するためにスキャンから除外できます。

最も頻繁に起動されるプロセスを特定する方法

次のコマンドを実行します：

```
kesl-control --get-statistic --processes
```

このコマンドは、Kaspersky Endpoint Security が最も頻繁に起動を検知するプロセスの一覧と、それらのプロセスの起動回数を出力します。

5 ファイル操作のインターセプトが最も多く発生するパスの特定

ディレクトリを、ファイル脅威対策とスキャンタスクのパフォーマンスを最適化するためにファイル操作のインターセプトから除外できます。

ファイル操作のインターセプトに関する情報を取得する方法

ファイル操作のインターセプトに関する情報は、以下の方法で取得できます：

- 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ファイルの統計情報を取得します：

  ```
  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。

- より詳細な分析には、アプリケーションのトレースファイルを使用します。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。

  既定では、本製品はトレースファイルを生成しません。

  トレースファイルの作成を有効にする

  ```
  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。

  トレースファイルの作成を無効にする

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

- インターセプトされたファイルの一覧を取得します：

  ```
  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インターセプト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` を追加できます。ここで、X はネストの深さです。例：

  ```
  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
  ```

コマンドラインでアプリケーション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、調査を実行する間、ローカルタスク管理を許可するようにします。

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

全般的な推奨事項

スキャン除外

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。

スキャンから次の項目を除外することを推奨します：

- 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。カスペルスキーのウイルス専門家によると、このようなファイルを介してウイルスが拡散する危険はありません。
- 最も頻繁にスキャンされるオブジェクトのリストに含まれる安全なオブジェクト。

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。ごくわずかな遅延も防止する必要がある場合は、ファイル操作のインターセプトからの除外を設定することを推奨します。

除外を設定する方法：

- 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できます。

  1つのスキャンタスクに設定された除外は、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。

コマンドラインで設定されたファイル脅威対策の除外の例

/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

```
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またはマスクで指定した複数のファイルを除外する

```
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

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

ファイル操作のインターセプトからの除外

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。

お使いのオペレーティングシステムが fanotify テクノロジーをサポートし、要件を満たしている場合は、アプリケーション用に更新可能なカーネルモジュールを設定します。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。更新可能なカーネルモジュールを使用すると、ファイル操作のインターセプトを最適化できます。

特定のディレクトリ内のファイルをスキャンだけでなくインターセプトからも除外するには、マウントポイントの除外（グローバル除外）を設定します。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。

デバイスで検出されたマウントポイントのリストは、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表示できます。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す情報がリストに表示されます。

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。

マウントポイントの種別（Local、AllRemoteMounted、Mounted:NFS、Mounted:SMB、または Mounted:Custom）または特定のマウントポイントを指定できます。アプリケーションは、除外された範囲を監視しません。

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。

システムイベントのインターセプトに更新可能なカーネルモジュールを使用する場合、マウントポイント全体だけでなく、デバイスにマウントされている個々のローカルディレクトリまたはリモートディレクトリもインターセプトから除外できます。

システムイベントのインターセプトに fanotify を使用する場合、グローバル除外はマウントポイントではないパスには適用されません。

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て /tmp ディレクトリに対して設定したグローバル除外の例

/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. システムイベントのインターセプトに fanotify を使用する場合は、/tmp ディレクトリがマウントポイントかどうかを確認します：

```
mount
```

mount コマンドの出力にこのディレクトリが含まれていない場合：

a. マウントポイントを作成します：

```
mount --bind /tmp/ /tmp
```

b. 新しく作成したマウントポイントが再起動後もシステムに保持されるように、/etc/fstab ファイルに次の行を追加します：

```
/tmp /tmp none defaults,bind 0 0
```

システムイベントのインターセプトに更新可能なカーネルモジュールを使用している場合は、この手順をスキップします。

2. /tmp ディレクトリをグローバル除外に追加します：

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
```

3. グローバル除外を適用するには、アプリケーションを再起動します：

```
systemctl restart kesl
```

アプリケーションによる RAM 使用量の制限

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` 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。

ファイル脅威対策に関する追加の推奨事項

ファイルを開く時のみスキャンする

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。
- デバイス上でローカルに：

```
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。

アーカイブのスキャン

アーカイブのスキャンが無効になっていることを確認します（既定の設定）。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。

ネットワークディレクトリからコピーされたファイルのスキャン

ネットワークディレクトリからコピーされたファイルに対するスキャンの除外を設定します。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。

スキャンタスクに関する追加の推奨事項

タスクの開始 スケジュール

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。

サーバー負荷が最小である時間にスキャンを実行します。

リモートディレクトリのスキャン

スキャンタスクの範囲に、SMB または 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。

グローバル除外およびファイル脅威対策の除外の使用

マルウェアのスキャンタスクで以下の設定が有効になっていることを確認してください：

- グローバル除外で指定されたマウントポイントをスキャン対象から除外するには、**グローバル除外を使用する**（`UseGlobalExclusions`）を有効にします。
- スキャン中に設定済みのファイル脅威対策の除外を使用するには、**ファイル脅威対策の除外を使用する**（`UseOASExclusions`）を有効にします。

既定では、両方の設定が有効になっています。

> 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/`

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

全般的な推奨事項

オペレーティングシステムの Firewall

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、アプリケーションを正しく動作させるには、ローカルデバイス（ループバック）からの受信接続を許可する accept ルールを追加します：

iptables のコマンド例

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

監視対象ネットワークポートのリスト

アプリケーションが監視す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。

アプリケーションと HAProxy の併用

アプリケーションを HAProxy ロードバランサーと併用する場合：

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
```

本製品と Kubernetes の併用

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と、Calico および Cilium ネットワークプラグインを使用する Kubernetes クラスターを連携させるには、kesl.ini 設定情報ファイルで `WtpFwMark`、 `NtpFwMark`、 `BypassFwMark`、 `BypassNflogMark` の設定を管理します。

「アプリケーションモジュールの整合性チェックに失敗しました」エラーが表示された場合の対処方法

ウェブ脅威対策に関する推奨事項

証明書検証ポリシー

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。

デバイスがインターネットに直接アクセスできない場合は、次のいずれかの操作を行ってください：

- 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します：

  - 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。

  - 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する場合：

    ```
    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。

- プロキシサーバー経由のインターネットアクセスを設定します：
  - ポリシーで、Web コンソールまたは管理コンソールを使用して、プロキシ設定を構成します。
  - 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する場合：

    認証付きプロキシサーバーの使用を有効にする

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<user name>:<password>@<IP address of the proxy server>:<port number>
    ```

    認証なしのプロキシサーバーの使用を有効にする

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<IP address of the proxy server>:<port number>
    ```

ネットワーク脅威対策に関する推奨事項

REDIRECT ルールとの互換性

ネットワーク脅威対策コンポーネントのインターセプトルールと REDIRECT ルール（たとえば、ポート 443 から 8443 へのリダイレクト）との互換性を確保するには：

1. 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
   ```

2. 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
   ```

ふるまい検知に関する推奨事項

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プロセスのアクティビティは、スキャン対象から除外することをお勧めします。

最も頻繁に開始されるプロセスを確認するには、次のコマンドを実行します：

```
kesl-control --get-statistic --processes
```

このコマンドは、Kaspersky Endpoint Security が最も頻繁に起動を検知するプロセスの一覧と、それらのプロセスの起動回数を出力します。

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除外リストを設定することも、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。

既定では、スキャンから除外されるのは指定したプロセスのみです。除外されたプロセスの子プロセスに対しては、ふるまい検知によるスキャンが継続されます。

コマンドラインでの除外リストの設定例

my_program1 と my_program2 のアクティビティをスキャン対象から除外する

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0001.ProgramPath=/bin/my_program2
```

my_program1 とその子プロセスのアクティビティをスキャン対象から除外する

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0000.ApplyToDescendants=Yes
```

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	–
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	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	–
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	–
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	–

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（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/apttmp/*` • `/tmp/suricata/*` • `/tmp/traffic/*` • `/tmp/apt_certs/*` tmp/apttmp/*、/tmp/suricata/*、/tmp/traffic/*、/tmp/apt_certs/* マウントポイントの除外は、バージョン 8.0 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/apttmp/*` • `/tmp/suricata/*` • `/tmp/traffic/*` • `/tmp/apt_certs/*` tmp/apttmp/*、/tmp/suricata/*、/tmp/traffic/*、/tmp/apt_certs/* マウントポイントの除外は、バージョン 8.0 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	–

アプリケーションコンポーネントのリファレンス

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 <prefix of command group>
```

ここで、`<prefix of command group>` 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ためのコマンド
- `-B`：バックアップを管理するためのコマンド
- `-C`：コンテナスキャンの全般設定を管理するためのコマンド
- `-D`：デバイスコントロールを管理するためのコマンド
- `-E`：現在の製品イベントを表示するためのコマンド
- `-F`：Firewall 管理用のコマンド
- `-H`：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
- `-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ためのコマンド
- `-M`：Kaspersky Endpoint Security と Kaspersky Unified Monitoring and Analysis Platform との連携の設定を管理するためのコマンド
- `-N`：暗号化された接続のスキャン設定を管理するためのコマンド
- `-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（クラウド）、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ためのコマンド
- `-U`：ユーザーとロールを管理するためのコマンド

- `-V`：Light Agent モードでの製品コマンド
- `-W`：製品イベントログのイベントを表示するためのコマンド
- `-X`：Kaspersky Endpoint Security と 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

bash シェルでは、kesl-control コマンドのオートコンプリートを有効にすることができます。

現在の bash セッションで kesl-control コマンドのオートコンプリートを有効にする

```
source /opt/kaspersky/kesl/shared/bash_completion.sh
```

すべての新しい bash セッションでオートコンプリートを有効にする

```
echo "source /opt/kaspersky/kesl/shared/bash_completion.sh" >> ~/.bashrc
```

ライセンスを管理するコマンド

`-L` 接頭辞は、そのコマンドがライセンスを管理するために使用されるコマンドの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、本製品が標準モードまたは EDR Agent モードで実行されている場合に使用できます。本製品を Light Agent モードで使用している場合、ライセンス管理コマンドはエラーを返します。

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、本製品のアクティベーション用のライセンスや、ライセンスに含まれていないコンポーネントのアクティベーション用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。

ライセンス情報ファイルを使用したライセンスの追加

```
kesl-control [-L] --add-active-key <key file path>
```

アクティベーションコードを使用したライセンスの追加

```
kesl-control [-L] --add-active-key <activation code>
```

説明：

`<key file path>` 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。

`<activation code>`は、アクティベーションコードです。

ライセンス情報ファイル（/home/test/00000001.key）を使用してライセンスを現在のライセンスとして追加する例

```
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、本製品のアクティベーション用のライセンスや、ライセンスに含まれていないコンポーネントのアクティベーション用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。

ライセンス情報ファイルを使用した予備のライセンスの追加

```
kesl-control [-L] --add-reserve-key <key file path>
```

アクティベーションコードを使用した予備のライセンスの追加

```
kesl-control [-L] --add-reserve-key <activation code>
```

説明：

`<key file path>`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。

`<activation code>`は、アクティベーションコードです。

ライセンス情報ファイル（/home/test/00000002.key）を使用して予備のライセンスを追加する例

```
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。

現在の EDR Optimum ライセンスの削除

```
kesl-control [-L] --remove-active-key [--edr-optimum]
```

現在の KUMA ライセンスの削除

```
kesl-control [-L] --remove-active-key [--kuma]
```

現在の MDR ライセンスの削除

```
kesl-control [-L] --remove-active-key [--mdr]
```

現在の EDR Expert（オンプレミス）ライセンスの削除

```
kesl-control [-L] --remove-active-key [--edr-kata]
```

現在の EDR Expert（クラウド）ライセンスの削除

```
kesl-control [-L] --remove-active-key [--cxdr]
```

現在の KWSM ライセンスの削除

```
kesl-control [-L] --remove-active-key [--khcs]
```

説明：

`--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。

`--cxdr` – 現在の EDR Expert（クラウド）ライセンスを削除します。

`--khcs` – 現在の KWSM ライセンスを削除します。

コマンドラインで `--edr-optimum`、`--kuma`、`--mdr`、`--edr-kata`、`--cxdr`、または `--khcs` オプションを指定しない場合、コマンドは本製品のアクティベーションに使用されている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。

予備の EDR Optimum ライセンスの削除

```
kesl-control [-L] --remove-reserve-key [--edr-optimum]
```

予備の KUMA ライセンスの削除

```
kesl-control [-L] --remove-reserve-key [--kuma]
```

予備の MDR ライセンスの削除

```
kesl-control [-L] --remove-reserve-key [--mdr]
```

予備の EDR Expert（オンプレミス）ライセンスの削除

```
kesl-control [-L] --remove-reserve-key [--edr-kata]
```

予備の EDR Expert（クラウド）ライセンスの削除

```
kesl-control [-L] --remove-reserve-key [--cxdr]
```

予備の KWSM ライセンスの削除

```
kesl-control [-L] --remove-reserve-key [--khcs]
```

説明：

`--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。

`--cxdr` – 予備の EDR Expert（クラウド）ライセンスを削除します。

`--khcs` – 予備の KWSM ライセンスを削除します。

コマンドラインで `--edr-optimum`、`--kuma`、`--mdr`、`--edr-kata`、`--cxdr`、または `--` オプションを指定しない場合、コマンドは本製品から予備のライセンスを削除します。

kesl-control -L --query

このコマンドは、本製品のアクティベーションに使用されたライセンスと、現在使用中のライセンスに関する情報を出力します。

```
kesl-control -L --query [--json]
```

説明：

`--json` – データを JSON 形式で出力します。

kesl-control --load-mdr-blob

この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。

```
kesl-control [-L] --load-mdr-blob <path to MDR BLOB file>
```

kesl-control --remove-mdr-blob

この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。

```
kesl-control [-L] --remove-mdr-blob
```

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。

ユーザーロールの管理

ユーザーとロールのリストを表示する

```
kesl-control [-U] --get-user-list
```

指定したユーザーにロールを割り当てる

```
kesl-control [-U] --grant-role <role> <user>
```

ユーザーロールを取り消す

```
kesl-control [-U] --revoke-role <role> <user>
```

説明：

`<user>` は、ユーザー名またはユーザーグループ名です。

`<role>` は、ユーザーまたはユーザーグループのロールです。

パスワードによる保護の設定

コマンドを使用してパスワードによる保護を管理できます。

パスワードによる保護を有効または無効にする

```
kesl-control --set-permission-manager-settings Enabled=<Yes|No>
```

現在のパスワードによる保護設定を表示する

```
kesl-control --get-permission-manager-settings
```

ユーザーまたはグループの権限を編集する

```
kesl-control --set-permissions <user> [--group] <permissions>=<Yes|No> [--file <file name>] [--json]
```

ユーザーまたはグループの現在の権限を表示する

```
kesl-control --get-permissions <user> [--group] [--file <file name>] [--json]
```

権限が設定されているユーザーまたはユーザーグループを削除する

```
kesl-control --remove-permissions <user> [--group]
```

説明：

`<user>` は、ユーザー名またはユーザーグループ名です。

`<permissions>` には、カスタム権限を指定します。

`--group` は、設定をユーザーグループに適用します。このオプションを指定しない場合、設定は個々のユーザーに適用されます。

`--file <path to file>`は、設定を設定情報ファイルに保存またはエクスポートします。このオプションを指定しない場合、コマンドの結果は標準出力に書き込まれます。

`--json` を指定すると、設定は JSON 形式で出力されます。

デバイスでのポリシーの管理

> デバイスでポリシーを無効にするには、ユーザーにKaspersky Security Center ポリシーの無効化権限が必要です。

ユーザーがデバイスでポリシーを無効にしている場合、デバイスまたはKaspersky Endpoint Securityを再起動すると、ポリシーは再び有効になります。

デバイスでポリシーを無効にする

```
kesl-control --disable-policy
```

デバイスにポリシーを適用する

```
kesl-control --enable-policy
```

アプリケーションのタスクと設定の管理

接頭辞 `-T` は、そのコマンドがアプリケーション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。

`-C` プレフィックスは、そのコマンドがコンテナスキャン設定を管理するコマンドのグループに属していることを示します。

「`-N`」は、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のグループに、そのコマンドが属することを示す接頭辞です。

kesl-control --export-settings

このコマンドは、すべてのアプリケーション設定をコンソールに出力するか、設定情報ファイルにエクスポートします。これらには、コンテナ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。

```
kesl-control [-T] --export-settings [--file <path to file>] [--json]
```

説明：

`--file <path to file>` 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。

kesl-control --import-settings

設定情報ファイルへのアクセス権限は、信頼できるユーザーのみに付与してください。本製品に設定をインポートする前に、ディレクトリ、設定情報ファイル、実行可能ファイル、隔離領域へのパスを確認してください。信頼できないソースから設定情報ファイルをインポートしないでください。設定情報ファイルが侵害されると、組織のインフラストラクチャやユーザーデータのセキュリティ、整合性、機能に影響が及ぶ可能性があります。

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。

```
kesl-control [-T] --import-settings --file <path to configuration file> [--json]
```

説明：

`--file <path to file>` は、アプリケーション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。

```
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

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。

```
kesl-control [-T] --get-app-settings [--file <path to file>] [--json]
```

説明：

`--file <path to file>` は、アプリケーションの全般設定の出力先とな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。

kesl-control --set-app-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、本製品の全般設定を構成します。

コマンドラインオプションを使用して設定を指定します：

```
kesl-control [-T] --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

設定情報ファイルを使用して設定を指定します：

```
kesl-control [-T] --set-app-settings --file <path to file> [--json]
```

説明：

`<setting name>=<setting value>` は、アプリケーションの全般設定の名前と値です。

`--file <path to file>` は、アプリケーション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。

```
kesl-control [-T] --get-settings <task ID|name> [--file <path to file>] [--json]
```

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。

`--file <path to file>` は、タスク設定の出力先とな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。

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。

コマンドラインオプションを使用して設定を指定します：

```
kesl-control [-T] --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>] [--add-path <path>] [--del-path <path>] [--add-exclusion <path>] [--del-exclusion <path>]
```

設定情報ファイルを使用して設定を指定します：

```
kesl-control [-T] --set-settings <task ID/name> --file <path to file> [--json]
```

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。

`<setting name>=<setting value>` は、1つのタスク設定の名前と値です。

`--add-path <path>` は、スキャンするオブジェクトが含まれるディレクトリへのパスを追加します。

`--del-path <path>` は、スキャンするオブジェクトが含まれるディレクトリへのパスを削除します。

`--add-exclusion <path>` 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 <path>` 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 <path to file>` は、タスク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 --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。

```
kesl-control [-T] --set-settings <task ID|name> --set-to-default
```

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。

kesl-control --get-schedule

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。

```
kesl-control [-T] --get-schedule <task ID|name> [--file <path to file>] [--json]
```

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。

`--file <path to file>` は、タスクスケジュール設定の出力先とな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。

kesl-control --set-schedule

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。

コマンドラインオプションを使用して設定を指定します：

```
kesl-control [-T] --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

設定情報ファイルを使用して設定を指定します：

```
kesl-control [-T] --set-schedule <task ID|name> --file <path to file> [--json]
```

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。

`<setting name>=<setting value>` は、1つのタスクスケジュール設定の名前と値です。

`--file <path to file>` 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。

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。

```
kesl-control [-T] --get-task-list [--json]
```

説明：

`--json` を指定すると、設定は JSON 形式で出力されます。

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 のポリシーで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、およびRollbackの各タスクに関する情報は利用できません。

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。

```
kesl-control [-T] --get-task-state <task ID|name> [--json]
```

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。

--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次の状態を示します：

- Started – タスクは実行中です。
- Starting – タスクは起動中です。
- Stopped – タスクは停止済みです。
- Stopping – タスクは停止中です。

ODS、ODFIM、InventoryScanタイプのタスクは、次のいずれかの状態を示す場合もあります：

- Pausing – タスクは一時停止処理中です。
- Suspended – タスクは中断されています。
- Resuming – タスクは再開中です。

kesl-control --create-task

このコマンドは、既定の設定または設定情報ファイルで指定された設定を使用して、指定されたタイプのタスクを作成します。

作成できるのはユーザータスクのみです。事前定義済みタスクは作成できません。

製品のモードに応じて、次の種類のユーザータスクを作成できます：

- 標準モード：ODS、Update、Rollback、ODFIM、ContainerScan、InventoryScan。
- Light Agent モード：ODS、ODFIM、ContainerScan、InventoryScan。

既定の設定でタスクを作成します

```
kesl-control [-T] --create-task <task name> --type <task type>
```

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 <task name> --type <task type> [--file <path to file>] [--json]
```

説明：

`<task name>` は、新しいタスクに指定した名前です。

`<task type>` には、作成するタスクの種別を指定します。

`--file <path to file>` 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。

削除できるのはユーザータスクのみです。事前設定済みのタスクは削除できません。

```
kesl-control [-T] --delete-task <task ID|name>
```

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。

kesl-control --start-task

このコマンドはタスクを開始します。

`License` タイプのタスクを除き、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できます。

```
kesl-control [-T] --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`：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。

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。

kesl-control --stop-task

このコマンドはタスクを停止します。

`License` タイプのタスクを除き、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できます。

```
kesl-control [-T] --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`：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。

一時停止できるのは、`ODS`、`ODFIM`、`InventoryScan` タイプのタスクのみです。

```
kesl-control [-T] --suspend-task <task ID|name>
```

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。

kesl-control --resume-task

このコマンドはタスクを再開します。

再開できるのは、ODS、ODFIM、InventoryScanタイプのタスクのみです。

```
kesl-control [-T] --resume-task <task ID|name>
```

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。

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。

```
kesl-control [-T] --scan-file <path> [--action <action>]
```

説明：

<path> 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 <action> には、感染したオブジェクトに対してアプリケーションに実行させる処理を指定します。--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。

```
kesl-control [-T] --scan-container <ID|name[:tag]>
```

説明：

<ID|name[:tag]> 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。

役立つ記事

マスクを指定する方法

アスタリスク記号「*」を使用して、ファイル名またはディレクトリ名のマスクを作成できます。

ファイル名またはディレクトリ名の「/」記号の前にある任意の文字数の文字列（0 文字の場合を含む）を表す「*」記号を 1 つ指定することができます。例：/dir/*/file または /dir/*/*/file。

2 つの連続する「*」記号は、ファイル名またはディレクトリ名における「/」記号を含む任意の文字数の文字列（0 文字の場合も含む）を示します。例：/dir/**/file*/ または /dir/file**/。

アスタリスク記号を 2 文字連続させた「**」というマスク表現は、ディレクトリ名で1回のみ使用できます。たとえば、「/dir/**/**/file」は不適切なマスク表現となります。

ファイル名またはディレクトリ名には、? 文字を使用して任意の文字を表示できます。

コンテナスキャンの全般設定を管理するコマンド

kesl-control --get-container-settings

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。

```
kesl-control [-C] --get-container-settings [--file <path to file>] [--json]
```

説明：

--file <path to file> は、コンテナスキャンの全般設定の出力先とな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。

kesl-control --set-container-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、コンテナスキャンの全般設定を構成します。

コマンドラインオプションを使用して設定を指定します：

```
kesl-control [-C] --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

設定情報ファイルを使用して設定を指定します：

```
kesl-control [-C] --set-container-settings --file <path to file> [--json]
```

説明：

<setting name>=<setting value> は、コンテナスキャンの全般設定の名前と値です。

--file <path to file> は、コンテナスキャンの全般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。

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

「-N」は、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のグループに、そのコマンドが属することを示す接頭辞です。

kesl-control -N --query

このコマンドは、暗号化された接続のスキャンからの除外リストを出力します。

- ユーザーが追加した除外項目のリスト
- 本製品によって追加された除外項目のリスト
- 本製品のデータベースから受信した除外項目のリスト

ユーザーが追加した除外項目のリストを表示します

```
kesl-control -N --query user
```

本製品によって追加された除外項目のリストを表示します

```
kesl-control -N --query auto
```

本製品のデータベースから受信した除外項目のリストを表示します

```
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。

```
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。

```
kesl-control [-N] --get-net-settings [--file <path to file>] [--json]
```

説明：

`--file <path to file>` は、ネットワークトラフィックのスキャン設定の出力先とな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。

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。

コマンドラインオプションを使用して設定を指定します：

```
kesl-control [-N] --set-net-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

設定情報ファイルを使用して設定を指定します：

```
kesl-control [-N] --set-net-settings --file <path to file> [--json]
```

説明：

`<setting name>=<setting value>` は、ネットワークトラフィックのスキャン設定の名前と値です。

`--file <path to file>` は、ネットワークトラフィックのスキャン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。

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。

```
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。

```
kesl-control [-N] --add-certificate <path to certificate>
```

説明：

`<path to certificate>` 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。

```
kesl-control [-N] --remove-certificate <certificate subject>
```

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。

```
kesl-control [-N] --add-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

説明：

`<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。

`<remote IP address>` 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。

`<destination port>` 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。

```
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。

```
kesl-control [-N] --remove-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

説明：

`<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。

`<remote IP address>` は、トラフィックの方向に応じて、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。

`<destination port>` 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。

ステータスと保護の監視

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。

```
kesl-control [-S] --app-info [--json] [--check-permissions]
```

説明：

`--json` を指定すると、設定は JSON 形式で出力されます。

`--check-permissions` は、権限が正しく設定されていないアプリケーションディレクトリへのパスを表示します。

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 [-S] --supported-tech-info [--json]
```

説明：

`--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。

```
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。

```
kesl-control [-S] --omsinfo --file <path to file>
```

イベントを表示するコマンド

`-W` プレフィックスは、製品イベントログのイベントを表示するコマンドを示します。

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。

```
kesl-control -W [--query "<filter conditions>"]
```

説明：

`<filter conditions>`は、特定の現在のイベントを出力するために、論理演算子`and`を使用して結合された、`<field> <comparison operation> '<value>'`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 接頭辞は、そのコマンドがアプリケーションイベントの管理に使用されるコマンドのグループに属することを示します。

kesl-control -E

このコマンドは、アプリケーションイベントログ内のすべてのイベントに関する情報を出力します。`less` コマンドを使用して、表示されたイベントのリストを操作できます。

```
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。

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--file <path to file>] [--
json] [--reverse]
```

説明：

`<database file>` 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。

`<filter conditions>` は、クエリの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 `<field> <comparison operator> '<value>'` 形式の 1 つ以上の 論理式を指定します。

`<number>` は、出力する、選択範囲内の最新イベントの数（つまり、選択範囲の末尾から数えたレコード数）です。

`--file <path to file>` 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）。

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。

```
kesl-control [-J] --export-metrics [--period <interval in seconds between exports>|--interactive]
```

説明：

`--period` は結果の定期的な出力を有効にします。

`<interval in seconds between exports>`は、コマンドの結果をコマンドラインコンソールに出力する頻度（秒単位）を指定します。

`--interactive` は、対話型出力を有効にします（**Enter** キーが押されたとき）。

セキュリティコントロール

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。

デバイスコントロール設定の管理

現在のデバイスコントロール設定を表示する

```
kesl-control --get-settings 15 [--file <path to file>] [--json]
```

アプリケーションコントロール設定を変更する

```
kesl-control --set-settings 15 [<setting>=<value>] [--file <path to file>] [--json]
```

説明：

`<setting>=<value>`は、デバイスコントロールの設定とその値を指定します。

--file <ファイルのパス> は、設定を設定情報ファイルに保存またはエクスポートします。このオプションを指定しない場合、コマンドの結果は標準出力に書き込まれます。

`--json` – データを JSON 形式で出力します。

デバイスの管理

接続されているデバイスのリストを表示する

```
kesl-control [-D] --get-device-list [--all] [--json] [--export <file>]
```

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。

`--export <file>`は、接続されているデバイスのリストを JSON ファイルにエクスポートします。接続されているデバイスのリストがエクスポートされます。

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。

信頼するデバイス

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。

```
kesl-control [-D] --trusted-devices [--list] [--add <ID>] [--delete <ID>] [--merge|--add|--replace --file <file>]
```

説明：

`--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 <file>`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。

ブロックされたデバイスへの一時アクセス

これらのコマンドを使用すると、アクセス要求ファイルを作成し、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アクセスを取得できます：

アクセス要求ファイルを作成する

```
kesl-control [-D] --request-temporary-device-access --device-id <device ID> --access-duration <access duration> --
path <path to access request file>
```

アクセスキーをアップロードする

```
kesl-control [-D] --upload-temporary-device-access-key --path <access key>
```

説明：

`--device-id <device ID>` は、アクセスする対象のブロックされたデバイスの ID です。

`--access-duration <access duration>` は、デバイスにアクセスする期間（時間単位）です。可能な値：1 ～ 100

`--path <path to access request file>` 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です。

`--path <access key>` は、デバイス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。

インベントリタスクの管理

クライアントデバイスで検出されたアプリケーションの一覧を表示します

```
kesl-control [-A] --get-app-list [--json]
```

説明：

`--json` – データを JSON 形式で出力します。

アプリケーションカテゴリの表示

作成済みのアプリケーションコントロールカテゴリの一覧を表示します

```
kesl-control [-A] --get-categories [--names <name of category 1> <name of category 2> ... <name of category N>] [--file <path to file>] [--json]
```

説明：

`<category name 1> <category name 2> ... <category name N>` はカテゴリ名です。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 <path to file>` は、設定を設定情報ファイルに保存またはエクスポートします。このオプションを指定しない場合、コマンドの結果は標準出力に書き込まれます。

`--json` – データを JSON 形式で出力します。

アプリケーションカテゴリの管理

アプリケーションカテゴリを作成するには：

1. アプリケーションカテゴリの一覧を設定情報ファイルに書き込みます：

```
kesl-control --set-categories --file <path to file>
```

2. アプリケーションカテゴリを次のように追加します：

```
[
   {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 2>"
   }
]
```

［Exclude］フィールドと［Include］フィールドでファイルパスを指定するには、マスクを使用できます。

3. カテゴリの一覧をアプリケーションにインポートします：

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --
file <path to file>
```

アプリケーションコントロールカテゴリの一覧を編集します

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --file
<path to file>
```

説明：

`FilePath like <application>`は、アプリケーションの実行ファイルへの完全パスです。

`FileHash == <hash>`は、アプリケーションの実行ファイルの SHA256 ハッシュです。

`<category ID>`は、一意のカテゴリ ID です。必須の設定。ハイフンを含めずに`GUID`を入力してください。

`<category name 1> <category name 2> ... <category name N>`はカテゴリ名です。必須の設定。

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、そのカテゴリは作成されないか、既存のカテゴリのリストから削除されます。

`--file <path to file>`は、設定を JSON 設定情報ファイルに保存またはエクスポートします。

アプリケーションコントロール設定の管理

現在のアプリケーションコントロール設定を表示します

```
kesl-control --get-settings 21 [--file <path to file>] [--json]
```

アプリケーションコントロール設定を変更する

```
kesl-control --set-settings 21 [<setting>=<value>] [--file <path to file>] [--json]
```

説明：

`<setting>=<value>`は、アプリケーションコントロールの設定とその値を指定します。

`--file <path to file>`は、設定を設定情報ファイルに保存またはエクスポートします。このオプションを指定しない場合、コマンドの結果は標準出力に書き込まれます。

`--json` – データを JSON 形式で出力します。

設定を既定値に戻す

アプリケーションカテゴリの一覧とアプリケーションコントロールルールを削除し、既定の設定に復元します

```
kesl-control --set-settings 21 --set-to-default
```

役立つ記事

マスクを指定する方法

* 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。

ウェブコントロール管理コマンド

ウェブコントロール設定の管理

現在のウェブコントロール設定の表示

```
kesl-control --get-settings 26 [--file <path to file>] [--json]
```

ウェブコントロール設定の変更

```
kesl-control --set-settings 26 [<setting>=<value>] [--file <path to file>] [--json]
```

説明：

`<setting>=<value>` は、ウェブコントロールの設定とその値です。任意の数の設定を変更できます。

`--file <path to file>`は、設定を設定情報ファイルに保存またはエクスポートします。このオプションを指定しない場合、コマンドの結果は標準出力に書き込まれます。

`--json` – データを JSON 形式で出力します。

設定を既定値に戻す

構成済みの設定を削除し、ウェブコントロールの既定の設定を復元

```
kesl-control --set-settings 26 --set-to-default
```

ネットワーク接続の保護

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。

kesl-control --get-blocked-hosts

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。

```
kesl-control [-H] --get-blocked-hosts
```

kesl-control --allow-hosts

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。

```
kesl-control [-H] --allow-hosts <address>
```

説明：

`<address>` は、デバイスまたはサブネットの IP アドレス（IPv4 / IPv6、短縮形式のアドレスを含む）です。デバイスまたはサブネットの IP アドレスをスペースで区切って複数指定できます。

ファイアウォールを管理するコマンド

-F接頭辞は、コマンドがファイアウォール管理コマンドに属することを示します。

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。

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

説明：

`--name <rule name>` は、ネットワークパケットルールの名前です。

`--action <Allow|Block>` は、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です。

`--protocol <protocol>` は、監視するネットワークアクティビティのプロトコルです。

`--direction <direction>` 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 <remote address>:<port>` は、リモートデバイスのネットワークアドレスです。

`--local <local address>:<port>` 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 <index>` 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。

ルール名によるネットワークパケットルールの削除

```
kesl-control [-F] --del-rule --name <rule name>
```

ルール番号によるネットワークパケットルールの削除

```
kesl-control [-F] --del-rule --index <index>
```

説明：

`--name <rule name>` は、ネットワークパケットルールの名前です。

`--index <index>` 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。

ルール名によるネットワークパケットルールの優先度の変更

```
kesl-control [-F] --move-rule --name <rule name> --at <index>
```

ルール番号によるネットワークパケットルールの優先度の変更

```
kesl-control [-F] --move-rule --index <index> --at <index>
```

説明：

`--name <rule name>` は、ネットワークパケットルールの名前です。

`--index <index>` 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 <index>` 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。

```
kesl-control [-F] --add-zone --zone <zone> --address <address>
```

説明：

`--zone <zone>`は、ネットワークゾーンの事前定義済みの名前です。

`--address <address>` は、ネットワークアドレスまたはサブネットです。

kesl-control --del-zone

このコマンドは、ネットワークゾーンからアドレスを削除します。

アドレスまたはサブネットによるネットワークゾーンからのアドレスの削除

```
kesl-control [-F] --del-zone --zone <zone> --address <address>
```

ルール番号によるネットワークゾーンからのアドレスの削除

```
kesl-control [-F] --del-zone --zone <zone> --index <address index>
```

説明：

`--zone <zone>`は、ネットワークゾーンの事前定義済みの名前です。

`--address <address>` は、ネットワークアドレスまたはサブネットです。

`--index <address index>` 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。

```
kesl-control -F --query
```

高度な脅威と標的型攻撃からの保護

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。

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 "<filter conditions>"
```

説明：

`<filter conditions>` は、クエリの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 `<field> <comparison operator> '<value>'` 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。

```
kesl-control [-Q] --put <file path> [--md5] [--sha256] [--save-original-file]
```

説明：

`<file path>` 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。

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 <number>] [--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 ["<filter conditions>"] [-n <number>]
```

説明：

`<filter conditions>` は、クエリの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 `<field> <comparison operator> '<value>'` 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。

`<number>` は、表示する最新の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。

```
kesl-control -Q --restore <file ID> [--file <file path>]
```

説明：

`<file ID>` は、隔離されたファイルの ID です。

`--file <file path>` は、ファイルの新しい名前と、その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。

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」接頭辞は、カスペルスキー Detection and Response ソリューションとの連携設定を管理するためのコマンドのグループに、そのコマンドが属することを示します。

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。

```
kesl-control [-R] --add-kataedr-server-certificate <file> [--server-type <response|telemetry>]
```

説明：

`<file>` は、サーバー証明書を含むファイルのパスです。

`--server-type <response|telemetry>` を使用すると、EDR Expert（オンプレミス）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。

```
kesl-control [-R] --remove-kataedr-server-certificate [--server-type <response|telemetry>]
```

説明：

`--server-type <response|telemetry>` を使用すると、EDR Expert（オンプレミス）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。

```
kesl-control [-R] --query-kataedr-server-certificate [--server-type <response|telemetry>]
```

説明：

`--server-type <response|telemetry>` を使用すると、EDR Expert（オンプレミス）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。

```
kesl-control [-R] --add-kataedr-client-certificate <file>  [--server-type <response|telemetry>]
```

説明：

`<file>` は、クライアント証明書と秘密鍵を含む暗号コンテナ（PFX アーカイブ）のパスです。

> 暗号化されたコンテナのパスワードを指定する必要があります。指定しない場合、**Enter** キーを押すと、`Certificate password is required and cannot be empty` エラーが表示されます。

`--server-type <response|telemetry>` を使用すると、EDR Expert（オンプレミス）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。

```
kesl-control [-R] --remove-kataedr-client-certificate [--server-type <response|telemetry>]
```

説明：

`--server-type <response|telemetry>` を使用すると、EDR Expert（オンプレミス）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。

```
kesl-control [-R] --query-kataedr-client-certificate [--server-type <response|telemetry>]
```

説明：

`--server-type <response|telemetry>` を使用すると、EDR Expert（オンプレミス）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。

EDR Expert（クラウド）コンポーネントを管理するためのコマンド

「-R」接頭辞は、カスペルスキー Detection and Response ソリューションとの連携設定を管理するためのコマンドのグループに、そのコマンドが属することを示します。

kesl-control --query-cloudxdr-server-certificate

このコマンドを使用すると、OSMP 脅威対応サーバーまたは OSMP テレメトリ収集サーバーの証明書の情報を表示できます。

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type <response|telemetry>
```

説明：

`--server-type <response|telemetry>` を使用すると、EDR Expert（クラウド）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

kesl-control --query-cloudxdr-client-certificate

このコマンドを使用すると、OSMP 脅威対応サーバーまたは OSMP 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、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。

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type <response|telemetry>
```

説明：

`--server-type <response|telemetry>` を使用すると、EDR Expert（クラウド）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

NDR (KATA) コンポーネントを管理するためのコマンド

「-R」接頭辞は、カスペルスキー Detection and Response ソリューションとの連携設定を管理するためのコマンドのグループに、そのコマンドが属することを示します。

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。

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

説明：

`<file>` は、サーバー証明書を含むファイルのパスです。

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。

```
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。

```
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。

```
kesl-control [-R] --add-katandr-client-certificate <file>
```

説明：

`<file>` は、クライアント証明書と秘密鍵を含む暗号コンテナ（PFX アーカイブ）のパスです。

> 暗号化されたコンテナのパスワードを指定する必要があります。指定しない場合、**Enter** キーを押すと、`Certificate password is required and cannot be empty` エラーが表示されます。

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。

```
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。

```
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」接頭辞は、カスペルスキー Detection and Response ソリューションとの連携設定を管理するためのコマンドのグループに、そのコマンドが属することを示します。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。

```
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。

```
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。

```
kesl-control [-M] --add-kuma-server-certificate <path to file>
```

説明：

`<path to file>` は、DER または PEM 形式の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。

```
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。

```
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。

```
kesl-control [-M] --add-kuma-client-certificate <path to file>
```

説明：

`<path to file>` は、クライアント証明書と秘密鍵を含む暗号コンテナ（PFX アーカイブ）のパスです。

> 暗号化されたコンテナのパスワードを指定する必要があります。指定しない場合、**`Enter`** キーを押すと、`Certificate password is required and cannot be empty` エラーが表示されます。

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。

```
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。

```
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。

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

説明：

`<file>` は、DER または PEM 形式の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。

```
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。

```
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。

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

説明：

`<file>` は、クライアント証明書と秘密鍵を含む暗号コンテナ（PFX アーカイブ）のパスです。

> 暗号化されたコンテナのパスワードを指定する必要があります。指定しない場合、**Enter** キーを押すと、`Certificate password is required and cannot be empty` エラーが表示されます。

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。

```
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。

```
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。

```
kesl-control [-X] --sandbox <path 1> <path 2>
```

説明：

`<path>` 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、そのコマンドがアプリケーション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。

```
kesl-control [-T] --scan-ioc --path <path to directory or file> [--process on|off] [--hint <regular expression>]
[--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--
excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

説明：

`--path <path to directory or file>` は、スキャンの実行に使用する .IOC または .XML 拡張子の 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 <regular expression>` 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：`digit`、`alpha`、`lower`、`upper`、`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 <list of exclusions>` 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 <list of directories>` 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` – アプリケーションは簡易スキャンを実行します。

Kaspersky Endpoint Security がスキャンする重要な領域

- /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。

kesl-control --get-response-task-list

このコマンドは、デバイスで実行中の *IOC* スキャンタスクに関する情報を表示します。

```
kesl-control [-T] --get-response-task-list
```

その結果、アプリケーションは実行中のタスクに関する情報を次の形式で表示します：

タスク ID：<タスク ID>

応答処理：locScan

作成日：<タスクの作成日時>

タスクの開始：<タスクの開始スケジュール>

ステータス：<タスクのステータス>

Kaspersky Endpoint Security は、サーバーとの同期のたびに、実行中の *IOC* スキャンタスクに関する情報を更新します。カスペルスキー Detection and Response ソリューションとの統合設定で、同期間隔を設定できます（`SynchronizationPeriod`）。既定では、アプリケーションは 5 分ごとにサーバーと同期します。

kesl-control --delete-response-task <タスク ID>

このコマンドは、ID を指定して *IOC* スキャンタスクを削除します。アプリケーションは、コンピューター上でローカルにタスクを削除します。Web コンソールまたは OSMP コンソールでタスクを削除していない場合、アプリケーションは次回サーバーと同期するときにこのタスクを復元します。

```
kesl-control [-T] --delete-response-task-list <task ID>
```

Light Agent モードでの製品コマンド

-V プレフィックスは、このコマンドが Light Agent モードで使用される Kaspersky Endpoint Security のコマンドグループに属することを示します。

> これらのコマンドは、Kaspersky Endpoint Security が Light Agent モードで使用されている場合にのみ実行できます。

kesl-control --ksvla-info

このコマンドは、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。

```
kesl-control --ksvla-info
```

kesl-control --viis-info

このコマンドは、Light Agent モードで本製品を Integration Server に接続することに関する情報を出力します。

```
kesl-control --viis-info
```

kesl-control --svm-info

このコマンドは、Light Agent モードで本製品を SVM に接続することに関する情報を出力します。

```
kesl-control --svm-info
```

アプリケーションのコマンドラインオプション

アップデートタスク

次の表では、`Update` タスクで指定できるすべての設定について、使用可能なすべての値と既定値を説明します。

アップデートタスクの設定

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。

設定	説明	値
SourceType	製品がアップデートを受信するアップデート元。	KLServers（既定値）– カスペルスキーのアップデートサーバーのいずれかからアップデートを受信します。アップデートは HTTPS プロトコルを使用してダウンロードされます。 SCServer ローカルネットワーク上にインストールされている管理サーバーからアップデートを保護対象のデバイスにダウンロードします。組織のデバイス保護の集中管理に Kaspersky Security Center を使用する場合は、このアップデート元を選択できます。 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。

ホスト脅威対策

ファイル脅威対策タスク

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。

次の表では、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。

設定	説明	値
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
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。

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
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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	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。
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_<item number>=*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。	<path to local folder> – 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す。パスの指定にマスクおよびタグを使用できます。 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）
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 folder> – 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。 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> – 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。
[ExcludedForProgram.item_#] セクションには、次の設定が含まれています：		

設定	説明	値
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。	<path to process> — 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。
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）
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。	<path to local folder> — 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す。パスの指定にマスクを使用できます。 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。

役立つ記事

マスクを指定する方法

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。

タグの使用方法

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。

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 <full path to the configuration file> [--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 <full path to the configuration file> [--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。

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カスタムタスク（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。

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
```

マルウェアのスキャンタスク

この表では、マルウェアのスキャンタスク（Scan_My_Computer）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。

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。 既定値です：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。 既定値です：0.
QueueScanTasks	以前に開始されたスケジュール済みスキャンがまだ実行中の場合、スケジュール済みスキャンタスクの実行を延期します。現在のスキャンが続行されている場合、Kaspersky Endpoint Security はスケジュール済みスキャンタスクをキューに追加します。これは、コンピューターの負荷の最適化に役立ちます。例えば、スキャンタスクが 18:00 と 20:00 に実行されるようにスケジュールされているとします。18:00 のスキャンがまだ実行中の場合、20:00 に実行されるようにスケジュールされているスキャンタスクは延期されます。延期されたタスクは、18:00 のタスクが完了した後に実行されます。	Yes：現在のスキャンがまだ実行中の場合、スケジュール済みスキャンタスクをキューに追加します。 No（既定値）：現在のスキャンがまだ実行中の場合でも、スケジュール済みスキャンタスクを実行します。
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。 既定値です：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。

設定	説明	値
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。
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。 <device name mask> – 指定され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。 既定値です：/** – 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。	既定値です：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_0000=*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。	<path to local directory> – 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。	既定値です：*（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。 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。

役立つ記事

マスクを指定する方法

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。

オブジェクトスキャン タスク

この表では、オブジェクトスキャンタスク（Scan_File）で指定できるすべての設定について、使用可能なすべての値と既定値を説明します。

オブジェクト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 – 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。
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。 既定値です：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。 既定値です：0.

設定	説明	値
QueueScanTasks	以前に開始されたスケジュール済みスキャンがまだ実行中の場合、スケジュール済みスキャンタスクの実行を延期します。現在のスキャンが続行されている場合、Kaspersky Endpoint Security はスケジュール済みスキャンタスクをキューに追加します。これは、コンピューターの負荷の最適化に役立ちます。例えば、スキャンタスクが 18:00 と 20:00 に実行されるようにスケジュールされているとします。18:00 のスキャンがまだ実行中の場合、20:00 に実行されるようにスケジュールされているスキャンタスクは延期されます。延期されたタスクは、18:00 のタスクが完了した後に実行されます。	Yes：現在のスキャンがまだ実行中の場合、スケジュール済みスキャンタスクをキューに追加します。 No（既定値）：現在のスキャンがまだ実行中の場合でも、スケジュール済みスキャンタスクを実行します。
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。 既定値です：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
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）– 推奨値です。
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。 <device name mask> – 指定され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。 既定値です：/** – デバイス名にあるすべての文字。「/」も含まれます。

簡易スキャンタスク

次の表では、簡易スキャンタスク（Critical_Areas_Scan）で指定できるすべての設定について、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
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。 既定値です：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。 既定値です：0.
QueueScanTasks	以前に開始されたスケジュール済みスキャンがまだ実行中の場合、スケジュール済みスキャンタスクの実行を延期します。現在のスキャンが続行されている場合、Kaspersky Endpoint Security はスケジュール済みスキャンタスクをキューに追加します。これは、コンピューターの負荷の最適化に役立ちます。例えば、スキャンタスクが 18:00 と 20:00 に実行されるようにスケジュールされているとします。18:00 のスキャンがまだ実行中の場合、20:00 に実行されるようにスケジュールされているスキャンタスクは延期されます。延期されたタスクは、18:00 のタスクが完了した後に実行されます。	Yes：現在のスキャンがまだ実行中の場合、スケジュール済みスキャンタスクをキューに追加します。 No（既定値）：現在のスキャンがまだ実行中の場合でも、スケジュール済みスキャンタスクを実行します。

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。 既定値です：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。 <device name mask> – 指定され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。 既定値です：/** – 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。	既定値です：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。

設定	説明	値
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_0000=*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。	<path to local directory> – 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。	既定値です：*（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。 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。

役立つ記事

マスクを指定する方法

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。

リムーバブルドライブスキャンタスク

コマンドラインでは、リムーバブルドライブのスキャンの事前定義済みタスク（Removable_Drives_Scan）を使用して、リムーバブルドライブのスキャンを管理できます。

既定では、*リムーバブルドライブのスキャン*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 および Blu-ray ディスクを除く）上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 および Blu-ray ディスクを除く）上の**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 ドライブおよび Blu-ray ディスク上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 ドライブおよび Blu-ray ディスク上の**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 ドライブおよび Blu-ray ディスクが接続されたときにスキャンしません。
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、タスクのスケジュールを設定できます。
- 次の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：

```
kesl-control --scan-container
```

コンテナスキャン設定

次の表では、ネームスペースとコンテナをリアルタイムでスキャンするときに使用されるコンテナスキャン設定について説明します。

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。
UseDocker	Docker コンテナ管理システムの使用。	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

コンテナのスキャンタスク

この表では、コンテナスキャンタスク（Container_Scan）で指定できるすべての設定について、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
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。	既定値です：*（すべてのコンテナーをスキャン）。 **my_container という名前のコンテナに対して実行されたコンテナスキャンの例** 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例** 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、任意の文字列で終わるすべてのコンテナに対して実行されたコンテナスキャンの例** 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。	既定値です：*（すべてのイメージをスキャン）。 **「my_image」という名前で、「latest」タグを持つイメージに対して実行されたイメージスキャンの例** ImageNameMask=my_image:latest **名前が my_image_ で始まり、任意のタグを持つすべてのイメージに対して実行されたイメージスキャンの例** ImageNameMask=my_image*
DeepScan	すべてのイメージレイヤーを確認し、コンテナを実行します。	Yes – 全レイヤーをスキャンします。 No（既定値）– どのレイヤーもスキャンしません。
ContainerScanAction	感染したオブジェクトの検知時に、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。

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。 既定値です：0.
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。 既定値です：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。 既定値です：DisinfectDeleteIfNotPossible

設定	説明	値
UseExcludeMasks	ExcludeMasks.item_# 設定で指定されたオブジェクトのスキャン除外を使用します。	Yes – 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
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。

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。
QueueScanTasks	以前に開始されたスケジュール済みスキャンがまだ実行中の場合、スケジュール済みスキャンタスクの実行を延期します。現在のスキャンが続行されている場合、Kaspersky Endpoint Security はスケジュール済みスキャンタスクをキューに追加します。これは、コンピューターの負荷の最適化に役立ちます。例えば、スキャンタスクが 18:00 と 20:00 に実行されるようにスケジュールされているとします。18:00 のスキャンがまだ実行中の場合、20:00 に実行されるようにスケジュールされているスキャンタスクは延期されます。延期されたタスクは、18:00 のタスクが完了した後に実行されます。	Yes：現在のスキャンがまだ実行中の場合、スケジュール済みスキャンタスクをキューに追加します。 No（既定値）：現在のスキャンがまだ実行中の場合でも、スケジュール済みスキャンタスクを実行します。

Jenkins との連携

Kaspersky Endpoint Security は、Jenkins との連携をサポートしています。Jenkins Pipeline プラグインを使用して、様々な段階で Docker イメージをスキャンできます。たとえば、開発プロセス中や公開前に、リポジトリ内の Docker イメージをスキャンできます。

Kaspersky Endpoint Security を Jenkins と連携するには：

1. Jenkins ノードに Kaspersky Endpoint Security をインストールします。
2. Jenkins ノードに Docker Engine をインストールします。
   詳細は、Docker Engine のガイドを参照してください。
3. Kaspersky Endpoint Security の管理者権限を Jenkins ユーザーに付与します：

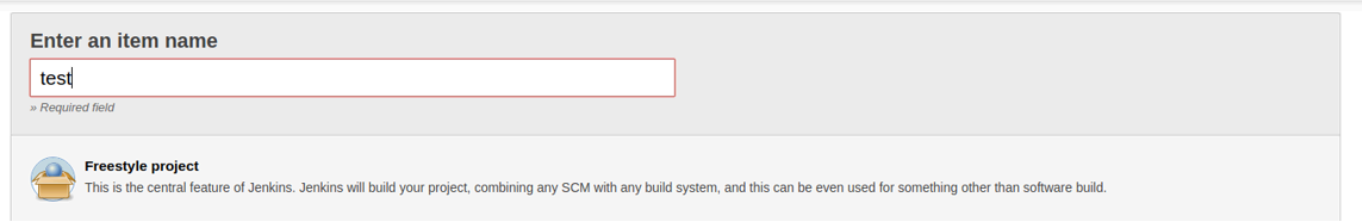
   ```
   kesl-control --grant-role admin <Jenkins user name>
   ```

4. Jenkins ユーザーを docker グループに追加します：

   ```
   sudo usermod -aG docker <Jenkins user name>
   ```

   通常、名前には jenkins が使用されます。

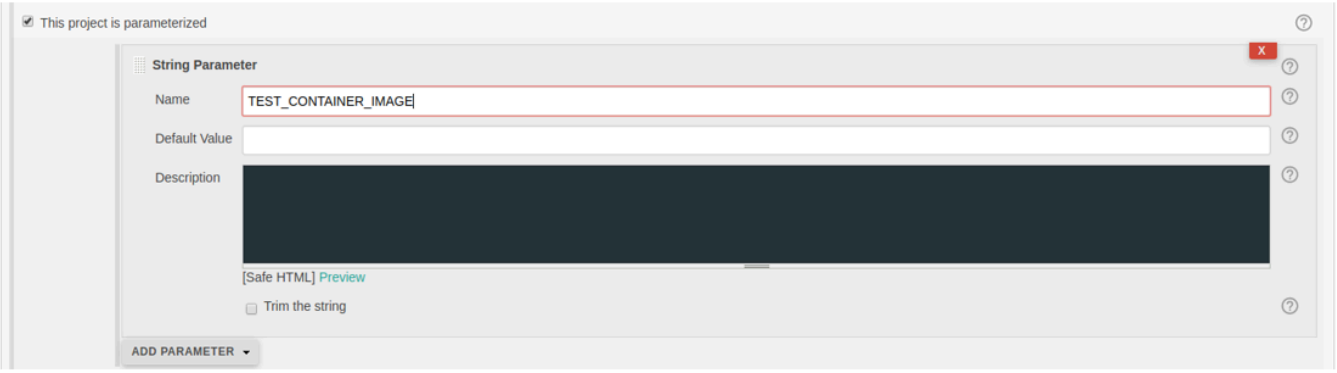
5. Jenkins で、名前に `test` を使用して新しいビルドジョブを作成します（[**新しいアイテム**] → [**アイテム名を入力**]）。



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 プラグインまたはその他の方法で Docker コンテナを起動する場合は、後でスキャンするため、実行中の Docker コンテナの ID を /tmp/kesl_cs_info ファイルに保存します：

```
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。

アンチクリプタータスク

コマンドラインで、アンチクリプタータスク（`Anti_Cryptor`）を使用してアンチクリプターを管理できます。

既定では、アンチクリプターのタスクは実行されません。このタスクは、手動で開始および停止できます。

アンチクリプターの事前定義済みタスクの設定を編集することで、アンチクリプターの設定を構成できます。

設定	説明	値
ActionOnDetect	［信頼されていないホストのブロック］をオンにする。	Block （既定値）– 信頼されていないホストのブロックを有効にします。 Notify：信頼されていないホストのブロックを無効にします。
BlockTime	信頼できないデバイスがブロックされる時間（分単位）。 侵入されたホストがブロックされてから BlockTime の設定値を変更しても、このホストのブロック時間は変更されません。ブロックの時間は動的な値ではなく、ブロックの瞬間に計算されます。	1 - 4294967295 の整数。 既定値：30
UseExcludeMasks	ExcludeMasks.item_# 設定で指定されたオブジェクト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。
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。 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。
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）

設定	説明	値
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。 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。

役立つ記事

マスクを指定する方法

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。

ふるまい検知タスク

ふるまい検知の事前定義済みタスク（Behavior_Detection）を使用して、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のふるまい検知を管理できます。

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。

設定	説明	値
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	この設定は、Elbrus CPUを搭載したデバイスには適用されません。	`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。
[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。		
`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。
`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のプロセスの除外。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	`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。

役立つ記事

マスクを指定する方法

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。

脆弱性攻撃ブロック

コマンドラインでは、ふるまい検知事前定義済みタスク（Behavior_Detection）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 ― MD5 ハッシュ Sha256 ― 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。
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） 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

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 設定の値は、コマンドラインオプション、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 <path to the configuration file> [--json] [--accept-ksn]
```

説明：

--file <path to the configuration file> は、必要な UseKSN 値 が設定されている一般的なアプリケーション設定を含む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。

--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。

Kaspersky Security Network への接続

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*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、ナレッジベースから情報を取得でき、脅威の種別や発生源に関する統計情報および情報が匿名で送信されます。
- *基本 KSN モード*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、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情報および情報は匿名で送信されません。
- *KSN が使用されていません*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（*KSN* または *KPSN*）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。

クラウドモードの有効化または無効化

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 を仮想環境保護用 Light Agent モードで使用する場合、軽量のマルウェアデータベースの使用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、コマンドラインオプションを使用して、`CloudMode` 設定を変更できます。

> Kaspersky Security Network の使用が有効になっている場合、クラウドモードを使用できます。

有害 USB 攻撃ブロックタスク

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。
`ProhibitBarcodeScanner`	認証コードを入力できない USB デバイスを認証するために、認証コードをバーコードとして表示する機能を有効または無効にします。	`Yes`（既定値）では、認証コードをバーコードとして表示することが禁止されます。 `No` では、認証コードをバーコードとして表示することが許可されます。

通信と危険サイト対策

ウェブ脅威対策タスク

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 のデータベースとの照合によるリンクのチェック。	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 のデータベースとの照合によるリンクのチェック。	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でのヒューリスティック分析の使用。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	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	広告 URL のデータベースとの照合によるリンクのチェック。	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	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含む URL のデータベースとの照合によるリンクのチェック。	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。
UseTrustedAddresses	信頼する URL のリストの使用。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。 IP アドレスの指定は、マスクをサポートしていません。

役立つ記事

マスクを指定する方法

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）。

ネットワークトラフィックのスキャン

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 <path to configuration file> [--json]
```

説明：

- `--file <path to the configuration file>` は、ネットワークトラフィックのスキャン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 <path to the configuration file> [--json]
```

説明：

- `--file <path to the configuration file>` 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 <parameter name>=<parameter value> [<parameter name>=<parameter value>]
```

ここで、`<parameter name>=<parameter value>`は、ネットワークトラフィックのスキャン設定の名前と値です。

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 <path to the certificate>
```

説明：

`<path to the certificate>` 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 <subject of the certificate>
```

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 <remote IP address> --dst-port <destination port>
```

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。
- `<remote IP address>` 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。
- `<destination port>` は、トラフィックの方向に応じて次のいずれかです：
  - 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 <remote IP address> --dst-port
<destination port>
```

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。
- `<remote IP address` は、トラフィックの方向に応じて、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。
- `<destination port>` 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。

ネットワーク脅威対策タスク

コマンドラインでは、ネットワーク脅威対策の事前定義済みタスク（`Network_Threat_Protection`）を使用してネットワーク脅威対策を管理できます。

既定では、ネットワーク脅威対策タスクは実行されません。タスクは手動で開始および停止できます。

ネットワーク脅威対策の設定は、ネットワーク脅威対策の事前定義済みタスクの設定を編集することで構成できます。

ネットワーク脅威対策タスクの設定

設定	説明	値
`ActionOnDetect`	ネットワーク攻撃に典型的なネットワーク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。

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Firewall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
```

ファイアウォール管理タスクの設定

設定	説明	値
DefaultIncomingAction	この接続種別に適用するネットワークルールがない場合、受信接続に対して実行する既定の処理。	Allow（既定値）– 受信接続を許可します。 Block – 受信接続をブロックします。
DefaultIncomingPacketAction	この接続種別に適用するネットワークパケットルールがない場合、受信パケットに対して実行する既定の処理。	Allow（既定値）– 受信パケットを許可します。 Block – 受信パケットをブロックします。
OpenNagentPorts	ネットワークエージェントの動的ルールをネットワークパケットルールに追加するかどうかを指定します。	Yes（既定値）– ネットワークエージェントの動的ルールをネットワークパケットルールに追加します。 No – ネットワークエージェントの動的ルールをネットワークパケットルールに追加しません。
[PacketRules.item_#] セクションには、ファイアウォール管理タスクのネットワークパケットルールが含まれます。複数の [PacketRules.item_#] セクションを、任意の順序で指定できます。範囲はインデックスの昇順で処理されます。 [PacketRules.item_#] の各セクションには、次の設定が含まれています：		
Name	ネットワークパケットルールの名前。	既定値：Packet rule #<n>（n はインデックス）
FirewallAction	このネットワークパケットルールで指定される接続に対して実行する処理。	Allow（既定値）– ネットワーク接続を許可します。 Block – ネットワーク接続をブロックします。
Protocol	監視するネットワーク活動のデータ転送プロトコルの種別。	Any（既定値）– ファイアウォール管理タスクはすべてのネットワーク活動を監視します。 TCP UDP ICMP ICMPv6 IGMP GRE

設定	説明	値
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。
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。

設定	説明	値
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）
[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）

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 [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
```

```
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

説明：

- `--name <rule name>` は、ネットワークパケットルールの名前です。
- `--action <Allow|Block>` は、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です。
- `--protocol <protocol>` は、監視するネットワークアクティビティのプロトコルです。
- `--direction <direction>` 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 <remote address>:<port>` 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 <local address>:<port>` 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 <index>` は、ネットワークパケットルールのリストにおける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。

TCP ポート 23 へのすべての受信接続および確立済み接続をブロックするルールの作成例

```
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、TCP ポート 23 経由の受信接続および確立済み接続をブロックするルールの作成例

```
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 <rule name>
```

または

```
kesl-control --del-rule --index <current index>
```

説明：

- `--name <rule name>` は、ネットワークパケットルールの名前です。
- `--index <current index>` 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 <rule name> --at < new index>
```

または

```
kesl-control --move-rule --index <current index> --at <new index>
```

説明：

- `--name <rule name>` は、ネットワークパケットルールの名前です。
- `--index <current index>` 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 <new index>` 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。

ネットワークゾーンの設定

ネットワークアドレスをゾーンに追加するには、次のコマンドを実行します：

```
kesl-control --add-zone <zone> --address <address>
```

説明：

- `<zone>`は、ネットワークゾーンの事前定義済みの名前です。可能な値：`Public`、`Local`、`Trusted`。
- `<address>` は、ネットワークアドレスまたはサブネットです。

ネットワークアドレスをゾーンから削除するには、次のいずれかのコマンドを実行します：

```
kesl-control --del-zone <zone> --address <address>
```

または

```
kesl-control --del-zone <zone> --index <address index in the zone>
```

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。

セキュリティコントロール

デバイスコントロールタスク

この表では、デバイスコントロールタスク（Device_Control）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。
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。

設定	説明	値
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。
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。

設定	説明	値
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。
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。

設定	説明	値
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=<device 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。 <user name> 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>\<user name> または <user name>@<ドメイン名> の形式で指定します）。 @<group name> 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。		
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。	既定値です：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。

設定	説明	値
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）。 <weekday> – 曜日。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。 <hour> – 時間 [0:24]。時間の場合は、間隔による指定のみ可能です。 **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 時まで有効な schedule_1 の例です。** [Schedules.item_0001] ScheduleName=schedule_1 DaysHours=Su-Sa:0..11,12..15,16..24 **次の時間帯に対して有効な schedule_2 の例です：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** [Schedules.item_0002] ScheduleName=schedule_2 DaysHours=Th:12..14;Fr:2..15,16..24 **週 7 日 24 時間有効な schedule_3 の例です。** [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。 <user name> は、アクセスルールが適用されるローカルユーザーの名前です。 @<group name> は、アクセスルールが適用される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。	既定値です：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。		
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。 <user name> は、アクセスルールが適用されるローカルユーザーの名前です。 @<group name> は、アクセスルールが適用される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。	既定値です：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。

設定	説明	値
[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。 <user name> は、アクセスルールが適用されるローカルユーザーの名前です。 @<group name> は、アクセスルールが適用される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。	既定値です：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。 <user name> は、アクセスルールが適用されるローカルユーザーの名前です。 @<group name> は、アクセスルールが適用される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。		
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。	既定値です：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。

ウェブコントロール

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

次の表では、ウェブコントロールタスク（Web_Control）で指定できるすべての設定について、使用可能なすべての値と既定値を説明します。

ウェブコントロールタスクの設定

設定	説明	値
WebControlDefaultAction	既定のルール、つまり、他のルールの対象でない Web リソースへのアクセス試行を検出したときにウェブコントロールが実行する処理です。	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, AITools
[Rules.item_#.FormatCategories.item_#]	データ種別カテゴリを指定するセクション。	–
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。	<username> は、ルールを適用するユーザーの名前です。 @<groupname> 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。	<weekday> – 曜日。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。 <hour> – 時間 [0:24]。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 <path to the configuration file>] [--json]
```

説明：

`--file <path to the 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。

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 <path to the configuration file>] [--json]
```

説明：

`--file <path to the 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。

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
```

アプリケーションコントロール

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、設定情報ファイルまたはコマンドラインオプションを使用してタスクの設定を変更するときは、次のコマンドを実行します：

```
kesl-control --set-settings --accept
```

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

この表では、アプリケーションコントロールタスク（`Application_Control`）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。
`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。
`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。
`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。
`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。

設定	説明	値
[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。
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。

役立つ記事

マスクを指定する方法

* 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。

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」コマンドとアプリケーションコントロール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 <path to the configuration file>
```

説明：

`--file <path to the configuration file>` は、カテゴリ設定を含む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 <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "Name" : "<category name 2>"
   }
]
```

［`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。

`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 <category name 1> <category name 2> ... <category name N>] --file <path to the configuration file>
```

説明：

- `<category name 1> <category name 2> ... <category name N>` は、情報を編集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 <path to the configuration file>` は、カテゴリ設定を含む設定情報ファイルへのパスです。

役立つ記事

マスクを指定する方法

* 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。

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 <path to the configuration file>] [--json]
```

説明：

- `--file <path to the 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` を指定すると、設定は JSON 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 <category name 1> <category name 2> ... <category name N>] [--file <path to the configuration file>] [--json]
```

説明：

- `<category name 1> <category name 2> ... <category name 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 <path to the configuration file>` – カテゴリリストがエクスポートされる JSON 設定情報ファイルへの完全パス。
- `--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 the configuration file>] [--json]
```

説明：

- `--file <path to the 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 the configuration file>] [--json]
```

説明：

- `--file <path to the 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
```

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：

- インベントリ事前定義済みタスク（`Inventory_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。
- インベントリのユーザータスク（`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

この表では、インベントリタスク（`Inventory_Scan`）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に対して実行する処理： 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（既定値）– 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 – 「ゴールデンイメージ」アプリケーションカテゴリをクリアします。タスクが開始されるとすぐにカテゴリがクリアされ、デバイス上のファイルのインベントリは実行されません。
[ScanScope.item_#] セクションには、次の設定が含まれています：		
AreaDesc	インベントリの範囲の説明。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。

役立つ記事

マスクを指定する方法

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を表示するには、次のコマンドを使用します：

    ```
    kesl-control --get-categories
    ```

> 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。

システム変更監視タスク

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。`OAFIM` タイプのタスク。

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。

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。
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。 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。 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）。

役立つ記事

マスクを指定する方法

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。

システム変更チェックタスク

カスタムのシステム変更チェックタスク（System_Integrity_Monitoring）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。ODFIM タイプのタスク。

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、*システム変更チェック*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。 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。 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）。

役立つ記事

マスクを指定する方法

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。

高度な脅威と標的型攻撃からの保護

Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携

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、コマンドラインで*Kaspersky Endpoint Detection and Response Expert（オンプレミス）（KATAEDR）*事前定義済みタスクを使用して管理できます。

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（オンプレミス）連携モード。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 Expert（オンプレミス）との連携設定を管理できます。

*Kaspersky Endpoint Detection and Response Expert（オンプレミス）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する証明書を管理できます。

Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携設定

次の表は、Kaspersky Endpoint Detection and Response Expert（オンプレミス）（KATAEDR）と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）との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（オンプレミス）*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）との連携設定

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 アプリケーションは OSMP プラットフォーム上のサーバーと通信します。 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（オンプレミス）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 Expert（オンプレミス）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。

設定	説明	値
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	デバイス上のイベントに関するデータ（テレメトリ）を OSMP テレメトリ収集サーバーに送信します。	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。		
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 Expert（オンプレミス）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	IOA があるテレメトリ のみを送信します。*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。	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	リクエスト数を制限します。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。	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。

設定	説明	値
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 EDR Expert（オンプレミス）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コンテナ（PFX アーカイブ）へのパスです。

2. 暗号コンテナのパスワードを入力してください

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` の設定値が `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` の設定値が `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 Endpoint Detection and Response Expert（クラウド）との連携

Kaspersky Endpoint Security と Kaspersky Endpoint Detection and Response Expert（クラウド）ソリューションの連携は、コマンドラインで *Kaspersky Endpoint Detection and Response Expert（クラウド）との連携* 事前定義済みタスクを使用して管理できます。

事前定義済みタスクの設定を編集することで、Kaspersky Endpoint Detection and Response Expert（クラウド）の連携設定を管理できます。

*Kaspersky Endpoint Detection and Response Expert（クラウド）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。

カスペルスキー Endpoint Detection and Response Expert（クラウド）連携設定

以下の表では、Kaspersky Endpoint Detection and Response Expert（クラウド）連携の事前定義済みタスク（`EDRExpertCloud`）の設定について説明します。

タスク設定の現在の値を取得する方法

```
kesl-control --get-settings 39
```

タスク設定を構成する方法

```
kesl-control --set-settings 39 <parameter>=<value>
```

カスペルスキー Endpoint Detection and Response Expert（クラウド）連携設定

設定	説明
レスポンスサーバー連携設定	
`UseTunnel`	レスポンスサーバーへの接続に TCP トンネルを使用します。インフラストラクチャのセキュリティポリシーでサーバーへの直接接続が許可されていない場合、サーバーへの接続に TCP トンネルを使用します。 既定では、TCP トンネルの使用は無効になっています（`No`）。
`TunnelAddress`	トンネルへの接続に使用するサーバーアドレス（IPv4 または IPv6）。
`TunnelPort`	トンネルへの接続に使用するサーバーポート。
`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`。
テレメトリ収集サーバー連携設定 `[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。	
`EnableTelemetry`	デバイス上のイベントに関するデータ（テレメトリ）を OSMP テレメトリ収集サーバーに送信します。 既定で、テレメトリの送信は有効です（`Yes`）。

設定	説明
`OnlyTaggedEvents`	IOA があるテレメトリ のみを送信します。*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。 既定では、IOA があるテレメトリのみの送信は無効です（No）。
`UseTunnel`	テレメトリ収集サーバーへの接続に TCP トンネルを使用します。インフラストラクチャのセキュリティポリシーでサーバーへの直接接続が許可されていない場合、サーバーへの接続に TCP トンネルを使用します。 既定では、TCP トンネルの使用は無効になっています（No）。
`TunnelAddress`	トンネルへの接続に使用するサーバーアドレス（IPv4 または IPv6）。
`TunnelPort`	トンネルへの接続に使用するサーバーポート。
`[TelemetrySettings.EventTransferSettings]` 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。	
`UseRequestCountLimits`	リクエスト数を制限します。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。 既定で、このオプションはオンです。
`MaximumDataTransferTime`	イベント送信時の最大遅延時間。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。既定値は 30 秒です。
`MaximumNumberOfEventsInHour`	1 時間あたりの最大イベント数。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 1 時間あたりのイベント数の上限を超えた場合は、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。1 時間あたりの既定値は 3000 イベントです。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。
`MaximumNumberOfEventsInPackage`	1 パッケージあたりの最大イベント数。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。既定値は 1024 イベントです。
`EventLimitExceededPercentage`	イベントスロットルの閾値（パーセント）。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。既定値は 15 % です。

OSMP EDR Expert サーバー（クラウド）の接続証明書の管理

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。

Kaspersky Endpoint Detection and Response Expert（クラウド）のデータ処理に関する契約の利用条件に同意すると、アプリケーションは信頼済み接続の確立に使用するサーバーアドレスと証明書を自動的に受信します。そのため、コマンドを使用して証明書を追加または削除することはできません。証明書に関する情報は、コマンドラインでのみ表示できます。

OSMP 脅威対応サーバーへの接続用証明書の管理

脅威対応サーバー証明書に関する情報を表示するには

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type response
```

脅威対応サーバー接続用のクライアント証明書に関する情報を表示するには

```
kesl-control [-R] --query-cloudxdr-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

OSMP テレメトリサーバーに接続するための証明書の管理

テレメトリ収集サーバー証明書に関する情報の表示

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type telemetry
```

テレメトリサーバー接続用のクライアント証明書に関する情報を表示するには

```
kesl-control [-R] --query-cloudxdr-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

Kaspersky Endpoint Detection and Response（KATA）統合

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 Expert（オンプレミス）との連携（KATAEDR）*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 Expert（オンプレミス）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する証明書を管理できます。

Kaspersky Endpoint Detection and Response（KATA）連携設定

次の表では、Kaspersky Endpoint Detection and Response Expert（オンプレミス）（`KATAEDR`）との連携の事前定義済みタスクの設定について説明します。このタスクは、Kaspersky Endpoint Detection and Response (KATA) との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 アプリケーションは OSMP プラットフォーム上のサーバーと通信します。 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（オンプレミス）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 Expert（オンプレミス）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`。
`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`	イベントデータ（テレメトリ）の KATA への送信。	`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。		

設定	説明	値
`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コンテナ（PFX アーカイブ）へのパスです。

2. 暗号コンテナのパスワードを入力してください

KATA サーバーの設定と、*Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携*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
```

Kaspersky Endpoint Detection and Response (KATA) 連携

Kaspersky Network Security と Kaspersky Endpoint Detection and Response (KATA) の連携は、*Kaspersky Network Detection and Response (KATA) との連携*（`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（`KATANDR`）で指定できるすべての設定と、すべての設定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`。
［**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コンテナ（PFX アーカイブ）へのパスです。

2. 暗号コンテナのパスワードを入力してください

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

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。

Sandbox との連携タスクを開始するには、次のコマンドを実行します：

```
kesl-control --start-task 29
```

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。

*Sandbox との連携*タスクが開始されており、選択されているモードでスキャン対象ファイルの手動送信が許可されている場合（`Manual` または `AutoAndManual`）、コマンドラインから Sandbox でスキャンするファイルを送信できます。

スキャン対象ファイルを Sandbox に送信する方法

```
kesl-control [-X] --sandbox <path>
```

`<path>` 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

次の表では、Sandbox との連携タスク（Standalone_Sandbox）で指定できるすべての設定と、すべての設定の既定値について説明します。

Sandbox との連携の設定を構成する方法

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port> [<setting name>=
<setting value>]
```

サンドボックスの連携タスクの設定

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。

設定	説明	値
`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` – 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`。
[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コンテナ（PFX アーカイブ）へのパスです。

2. 暗号コンテナのパスワードを入力してください

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 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。

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 Managed Detection and Response 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。

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。

［`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 <path to the 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。

デバイスのネットワーク分離の管理

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。*

隔離設定の管理

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。

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
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 4000 0 は隔離のサイズが無制限でないことを意味します。 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の既定値は 200 で、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 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 <path to the file> [--md5] [--sha256] [--save-original-file]
```

説明：

- `<path to the file>` 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 ["<filter conditions>"] [-n <number of files>] [--json]
```

説明：

- `<filter conditions>`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。
- `<number of files>` は、表示する最新の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 <object identifier>
```

ここで、`<object identifier>` 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 <object identifier> --file <path to the file>
```

ここで、`--file <path to the file>` 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。ファイルを復元する際、アプリケーションは MAC ラベルが 3（cnnr フラグ）のディレクトリを作成します。

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 "<filter conditions>"
```

ここで、`<filter conditions>` 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。

名前またはパスに「test」を含むファイルの削除例

```
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
```

侵害の兆候の調査

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) と連携している場合、IOC スキャンは対応する Detection and Response ソリューション側で実行されます。

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 <path to the directory or file> [--process on|off] [--hint <regular
expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives
```

```
all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

説明：

- `--path <path to the directory or file>` は、スキャンの実行に使用する .IOC または .XML 拡張子の 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 <regular expression>` 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 <list of exclusions>` 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 <list of directories>` 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` – アプリケーションは簡易スキャンを実行します。

    Kaspersky Endpoint Security がスキャンする重要な領域

    - /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。

実行防止の管理

実行防止により、実行可能ファイルやスクリプトの実行の管理や、Office 形式のファイルを開くことの管理が可能です。実行防止は、実行防止ルールを使用してファイルへのユーザーアクセスを管理します。

オブジェクトの実行防止には、次のタスクが含まれます：

- *オブジェクトの実行防止（EDR（オンプレミス））*（`KATAEDR_Prevention`）
- *オブジェクトの実行防止 (EDR Expert（クラウド))*（`EDRExpertCloud_Prevention`）
- *オブジェクトの実行防止（EDR Optimum）*（`EDRO_Prevention`）

デフォルトでは、*オブジェクトの実行防止*タスクは開始されません。実行防止ルールを1つ以上追加している場合、アプリケーションはタスクを開始します。

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|cxdr|edro]
```

説明：

`--kata`：EDR Expert（オンプレミス）コンポーネントの実行防止ルールのリスト
`--cxdr`：EDR Expert（クラウド）コンポーネントの実行防止ルールのリスト
`--edro`：EDR Optimum コンポーネントの実行防止ルールのリスト

KUMA 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 との連携タスク

この表では、Kaspersky Unified Monitoring and Analysis Platform（KUMA）との連携タスクで指定できるすべての設定と、すべての設定の既定値について説明します。

Kaspersky Unified Monitoring and Analysis Platform 統合タスク設定

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。

設定	説明	値
`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。 `HTTPWithCompression` — イベント圧縮を使用する HTTP 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。
[KumaTransferSettings] 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 <path to the file>
```

ここで、`<path to the file>` は、DER または PEM 形式の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 [-M] --add-kuma-client-certificate <path to the file>
```

   `<path to the file>`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. 暗号コンテナのパスワードを入力してください

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
```

全般設定

管理コンソールでは、ポリシーのプロパティ（[**全般設定**]）で、アプリケーション全体の動作および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を管理できます。

全般的な製品設定

下の表では、アプリケーション全体の動作および個々の機能の動作を制御するアプリケーションの全般設定について説明します。

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 ディレクトリが指定されています。 既定値です：/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 レクトリが指定されています。 既定値です：/etc/exports。
`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。	既定値です：/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 は、root 権限が必要です。別の ディレクトリを指 は、このディレクトリに対する読み取りおよび書 を root ユーザーのみが持っていることを確認して （`700` または `rwx--------` の権限）。
`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。 この設定では、アプリケーションのトレースファイルの生成のみが有効になります。グラフィカルインターフェイスと kesl-control コマンドラインユーティリティのトレースファイルを生成するには、LFS_ENABLE_ALL_COMPONENTS_LOGGING 環境変数を設定する必要があります。	`Detailed` – 詳細なアプリケーションのトレース 生成します。 `MediumDetailed` – 情報メッセージとエラーメッ むアプリケーションのトレースファイルを生成し `NotDetailed` – エラーメッセージを含むアプリケ のトレースファイルを生成します。 `None`（既定値）– アプリケーションのトレースフ 成しません。
`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 既定値です：10.

設定	説明	値
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 既定値です：500.
WdTraceLevel	Watchdog サーバー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 Watchdog サーバーのトレー を生成します。 MediumDetailed – 情報メッセージとエラーメッ む Watchdog サーバーのトレースファイルを生成 NotDetailed – エラーメッセージを含む Watchd ーのトレースファイルを生成します。 None – Watchdog サーバーのトレースファイルを せん。 Product（既定値）– 値を TraceLevel の値と同 ます。
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 既定値です：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 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 用できる正規のアプリケーションの検出を無効に
NamespaceMonitoring	名前空間とコンテナスキャンを有効にします。 コンテナと名前空間を操作するためのコンポーネントがオペレーティングシステムにインストールされていない限り、アプリケーションは名前空間とコンテナをスキャンしません。	Yes（既定値）– 名前空間とコンテナのスキャン ます。 No – 名前空間とコンテナのスキャンを無効にし
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。ファイル操作インターセプトモードは、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、オブジェクトの実行防止処理、およびリムーバブルドライブスキャンタスクに影響します。	Yes（既定値）：スキャン中はファイルへのアクセ ックします。 スキャン中にファイルにアクセスする場合は No を す。すべてのファイルへのリクエストを許可し、 非同期に行われます。このファイル操作インター ドでは、スキャン中のシステムパフォーマンスへ さくなりますが、ファイル内の脅威が駆除または いリスクがあります。これは、スキャン中に、こ に関連付けられたプロセスが、アプリケーション イルのステータスを判定する前にファイル名を変 に発生する可能性があります。ただし、選択した に関係なく、ファイル脅威対策、デバイスコント 行防止コンポーネント、およびリムーバブルドラ ンタスクは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 Networ 有効にします。 Extended – 拡張モードで Kaspersky Security Net 用を有効にします。 No（既定値）– Kaspersky Security Network を使用 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（既定値）：Kaspersky Endpoint Security がマ ータベースの軽量版を使用する動作モードを有効 No（既定値）– マルウェアデータベースの完全版 す。 KSN の使用が無効になっている場合、クラウト 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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	Yes – Managed Detection and Response コンポー 効にします。 No（既定値）– Managed Detection and Response ネントを無効にします。
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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	Yes – EDR Optimum コンポーネントを有効にしま No（既定）– EDR Optimum コンポーネントを無効 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

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 • [<connection protocol>://]<address o proxy server>:<port> - プロキシサーバー 認証が不要な場合。 • [<connection protocol>://][<user name [<password>]@]<address of the proxy s <port> - プロキシサーバーへの接続に認証が 合。IPv6 アドレスを指定する場合は、角括弧 力してください。 HTTPS 経由のプロキシサーバーへの接続には対 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、<address>[:<port>]の形式で指定 ドレスを指定する際は、マスク（*記号）および に記述するコメントを使用できます。
ProxyBypassEdr	Kaspersky Endpoint Detection and Response Expert（オンプレミス）Integration Server に接続するときにプロキシサーバーを使用するかどうか。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	Yes：Kaspersky Endpoint Detection and Response （オンプレミス）Integration Server に接続すると キシサーバーを使用しません。 No（既定値）：Kaspersky Endpoint Detection and Expert（オンプレミス）Integration Server に接続 は、プロキシサーバーを使用します。
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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	Yes – Kaspersky Network Detection and Response Integration Server に接続する時は、プロキシサー ません。 No（既定値）– Kaspersky Network Detection and (KATA) Integration Server に接続する時は、プロキ 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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	Yes の場合、サンドボックスとの対話を提供する 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 サーバーに接続するときにプロキシサーバーを使
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。	既定値です：500000. 値が 0 の場合、新しいイベントは保存されず、古 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または kesladmin ロール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 開始できないことを意味します。 既定値です：100.
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

設定	説明	値
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/
ExcludedMountPoint.item_#	スキャン範囲から除外するマウントポイント。除外は、ファイル脅威対策、アンチクリプター、およびコンテナ監視コンポーネントの操作とリムーバブルドライブスキャンタスクに適用され、ODS および ContainerScan スキャンタスクの操作でも設定されます。 複数のマウントポイントを選択して、スキャンから除外することも可能です。 マウントポイントは、 mount コマンドを実行して出力されるのと同じものを指定する必要があります。 既定では、 ExcludedMountPoint.item_# 設定は指定されていません。	AllRemoteMounted — SMB プロトコルと NFS プ 使用してデバイスにマウントされるすべてのリモ 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 ントされるすべてのリモートディレクトリをファ 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 ントされるすべてのリモートディレクトリをファ 読み取りから除外します。 Mounted:<file system type>：指定したファ ム種別でマウントされているすべてのディレクト 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 内のオブジェクトをファイル操作の読み取りから す。このディレクトリは、リムーバブルドライブ マウントポイントとして使用されます。 <path that contains the /mnt/user*|/mnt/**/user_share>：名前に指 クが含まれるマウントポイント内のオブジェクト 操作のインターセプトから除外します。
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。	<full path to process> — 指定されたディレ オブジェクトをスキャンから除外します。パスの クを使用できます。
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 いるときにスケジュールされたタスクをスキップ No は、デバイスがバッテリー電源で動作している に関係なく、スケジュールされたタスクを実行し
UseOnDemandCPULimit	*ODS*、*ContainerScan*、および *InventoryScan* タイプのタスクの CPU 使用量制限を有効にします。	Yes：*ODS*、*ContainerScan*、および *InventorySc* 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
OnDemandCPULimit	*ODS*、*ContainerScan*、および *InventoryScan* タイプのタスクを実行する時の、すべてのプロセッサコアにおける最大使用率（パーセンテージ）。	10 から 100 までの整数値。 既定値です：100.
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 4000 0–無制限のサイズ。 既定値です：0.
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。 既定値です：30.
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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	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 アプリケーションを標準モードで使用している場 は 200、Light Agent モードで使用している場合の 100 です。

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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	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 です。 既定値です：90.
`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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。 `BackupFolder` 設定が使用されます。	既定値： `/var/opt/kaspersky/kesl/common/objects-b` 既定のディレクトリにアクセスするには、root 必要です。
`BackupFolder`	バックアップ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/ob` `backup/` 既定のバックアップの保管領域のディレクトリ セスするには、root 権限が必要です。
`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 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 プ通知を表示しません。
`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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	`UseFanotify`（既定）– fanotify テクノロジーを使 ステムイベントを遮断します。 `UseUpdatableKernelModule` – 更新可能なカーネ ールを使用してシステムイベントを遮断します。
`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 ために fanotify に切り替えます。 `FallbackToLimitedMode` – システムイベントの しません。本製品がシステムイベントインターセ 用しない場合、リアルタイムスキャンは実行され スの保護レベルが低下します。

設定	説明	値
`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 カーネルモジュールを起動するために本製品を自 動します。この設定の使用を推奨します。 `RestartServiceManually`（既定）は、ユーザー を手動で再起動した後に、アップデート可能なカ ュールを起動します。
`SystemEventsTransmission`	サードパーティ製アプリケーション（カスペルスキー製品ではないアプリケーション）からのイベントに関する情報の送信を有効にする。この設定を有効にすると、Kaspersky Endpoint Security は自身のイベントに加えて、サードパーティ製アプリケーションの systemd-journald イベントもアプリケーションイベントログに送信します。 systemd-journald へのアクセスには root 権限が必要です。	`Yes` を選択すると、サードパーティ製アプリケー systemd-journald イベントに関する情報のアプリ イベントログへの送信が有効になります。 `No`（既定値）を選択すると、サードパーティ製ア ションの systemd-journald イベントに関する情報 ーションイベントログへの送信が無効になります。
`UrgentUpdateRestartEnabled`	アプリケーションのインストール後の最初の 24 時間が経過した後に重要なアップデートを受信した場合、アプリケーションを自動的に再起動します。	`Yes` を選択すると、重要なアップデートを受信し プリケーションを自動的に再起動します。 `No`（既定値）：重要なアップデートを受信した場 ケーションを再起動しません。
`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。	`Yes`：アプリケーションがクラッシュした場合に イルを作成します。 `No`（既定値）：アプリケーションがクラッシュし 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 には、root 権限が必要です。

役立つ記事

マスクを指定する方法

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。

タスクスケジュール

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。

タスクの開始スケジュール設定

設定	説明
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。この設定の形式は、RuleType によって異なります。 可能な値： • <year>：1970 ～ 2099 • <month>：JAN、FEB、MAR、APR、MAY、JUN、JUL、AUG、SEP、OCT、NOV、DEC。 • <day of the month>：1 ～ 31 • <day of the week>：Mon、Tue、Wed、Thu、Fri、Sat、Sun。 • <hh>：0 ～ 23 • <mm>：0 ～ 59 • <ss>：0 ～ 59 • <interval between runs (in days)>：0 ～ 364 • <interval between runs (in hours)>：0 ～ 23 • <interval between runs (in minutes)>：0 ～ 59
RandomInterval	一定の時間間隔内（0 から指定値まで）で、コンピューター上のタスクをランダムに実行します。これにより、複数のタスクが同時に開始されることを回避できます。 既定値：99 分。 使用できる値：0 ～ 999。
RunMissedStartRules	本製品を起動後にミスタスクを実行します。 • Yes（既定値）は、未実行のタスクの実行が有効になっていることを意味します。スケジュールされたタスクの実行中に製品が停止した場合、またはコンピューターの電源がオフになった場合、Kaspersky Endpoint Security は製品の起動直後にそのタスクを開始します。これにより、重要なタスクの実行漏れを防ぐことができます。 • No は、未実行のタスクの実行が無効になっていることを意味します。スケジュールされたタスクの実行中に製品が停止した場合、またはコンピューターの電源がオフになった場合、製品はそのタスクをスキップします。これにより、製品の起動時に余分な負荷が発生することを回避できます。
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。 使用できる値：1 ～ 999。

プロキシサーバーの設定

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はプロキシサーバーの使用を有効にします。
- Noはプロキシサーバーを無効にします。

ProxyServer 設定では、プロキシサーバーの設定を <connection protocol>://[<user>[:<password>]@] <proxy server address>:<port number> 形式で指定できます。各項目は次のとおりです：

- <user> 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。
- <password> は、プロキシサーバーでの認証に使用するユーザーのパスワードです。
- <proxy server address> は、プロキシサーバーの IP アドレスまたはドメイン名です。
- <port number> 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、<address>[:<port number>] の形式で指定します。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でのプロキシサーバーの使用を設定できます：

- ProxyBypassEdr 設定では、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はプロキシサーバーの使用を有効にします。
- Noはプロキシサーバーを無効にします。

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 4000 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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。 `BackupFolder` 設定が使用されます。	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。
`BackupFolder`	バックアップ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/` 既定のバックアップの保管領域のディレクトリにアクセスするには、root 権限が必要です。

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。
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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	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。	

設定	説明	値
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。

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。

［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:<file system type>：指定したファイルシステム種別でマウントされているすべてのディレクトリをファイル操作のインターセプトから除外します。
- /mnt — /mnt マウントポイント（サブディレクトリを含む）内のオブジェクトをファイル操作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。
- <path containing the mask /mnt/user* or /mnt/**/user_share>：名前に指定したマスクが含まれる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。

> 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。

役立つ記事

マスクを指定する方法

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。

パスワードによる保護の設定

コマンドラインオプションを使用して設定を変更するか、設定情報ファイルを編集することで、アプリケーションを管理する権限を付与または取り消すことができます。

パスワードによる保護の設定

設定	説明	値
StopProtection	保護コンポーネントの停止。	Yes の場合、ユーザーは操作を実行できます。 No の場合、ユーザーは操作を実行できません。
StopSecurityControl	管理コンポーネントの停止	
StartProtection	保護コンポーネントの開始	
StartSecurityControl	管理コンポーネントの有効化	
ApplicationSettings	アプリケーションの設定	
ViewReports	レポートの表示	
RestoreFromBackup	バックアップからの復元	
RemoveLicenseKey	ライセンスの削除	
AddLicense	ライセンスの追加	
DisablePolicy	Kaspersky Security Center ポリシーの無効化	

管理コンソールでのアプリケーション設定

Kaspersky Endpoint Securityを設定するには、ポリシーを使用します。製品の各機能に関して詳しくは、それぞれの機能の該当セクションを参照してください。

定義データベースのアップデート

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をアップデートできます。

アップデートのユーザータスクを作成して実行できます。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。

アップデートタスクのプロパティの**アップデート元**セクションと**設定**セクションで、以下の表に記載されている設定を管理できます。

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。

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。

ホスト脅威対策

ファイル脅威対策

管理コンソールでは、ポリシーのプロパティ（**脅威対策 → ファイル脅威対策**）でファイル脅威対策を管理できます。

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
範囲名	スキャン範囲名。
パス	スキャンするディレクトリのパス。
ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：**追加**、**編集**、**削除**、**上に移動**、**下に移動**。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、範囲の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。
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。
	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。 「**/**」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。

役立つ記事

マスクを指定する方法

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。

タグの使用方法

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。

［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（**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設定できます。

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
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。 「**/**」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。
ファイルシステム名	除外範囲に追加するディレクトリがあるファイルシステムの名前を入力するためのフィールドです。 このフィールドは、ファイルシステムのドロップダウンリストで［**Mounted**］が選択され、右側のドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。
マスク	このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。マスクは、［パス］フィールドに指定されたディレクトリ内のオブジェクトにのみ適用されます。 既定では、すべてのオブジェクトを示すマスク「*****」がリストに含まれています。 マスクは、追加、編集、削除できます。

役立つ記事

マスクを指定する方法

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。

タグの使用方法

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。

［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。
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。

役立つ記事

マスクを指定する方法

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したりできます。タスクの設定を編集して、スキャン設定を管理できます。

*マルウェアの検索*タスクのプロパティの**設定**セクションでは、以下の表に示す設定を管理できます。

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、スキャン設定を指定できるウィンドウを開くボタンが含まれています。
脅威の検知時の処理	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**脅威の検知時の処理**］ウィンドウが表示され、検知された感染オブジェクトに対して実行する処理を設定できます。

マルウェアの検索タスクのプロパティの**除外**セクションでは、除外範囲、マスクによる除外、および脅威名による除外をカスタマイズできます。

［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
範囲名	スキャン範囲名。
パス	スキャンするディレクトリのパス。
ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：**追加**、**編集**、**削除**、**上に移動**、**下に移動**。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、範囲の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。

設定	説明
スキャン範囲名	スキャン範囲の名前を入力するフィールド。この名前は、［**スキャン範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品がこの範囲をスキャンするかどうかを選択します。 このチェックボックスをオンにすると、製品がこのスキャン範囲を処理します。 このチェックボックスをオフにすると、製品がこのスキャン範囲を処理しません。このチェックボックスをオンにすることにより、後からこの範囲をコンポーネント設定に含めることができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	これらの設定では、スキャン範囲を設定できます。 ファイルシステムのドロップダウンリストで、ファイルシステムの種別を選択できます： • **Local**（既定値）– ローカルディレクトリ。この項目を選択する場合は、ローカルディレクトリのパスを指定する必要があります。 • **Mounted** – マウントされたリモートまたはローカルのディレクトリ。この項目を選択する場合は、ファイルシステムのプロトコルまたは名前を指定する必要があります。 • **Shared** – Samba または NFS プロトコルでアクセス可能な保護されているサーバーファイルシステムリソースを表示します。 • **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。
	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。 「**/**」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。

役立つ記事

マスクを指定する方法

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。

タグの使用方法

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。

［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。

設定	説明
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。

スキャンの設定

設定	説明
アーカイブをスキャン	このチェックボックスでは、アーカイブをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、アーカイブがスキャンされます。 アーカイブをスキャンするには、アーカイブを解凍する必要があるためスキャン速度が遅くなる可能性があります。アーカイブのスキャンの所要時間を短縮するには、**全般スキャン設定**セクションで［**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）**］の設定を構成します。 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。

設定	説明
メールデータベースをスキャン	このチェックボックスでは、Microsoft Outlook、Outlook Express などのメールアプリケーションのメールデータベースをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、メールデータベースはスキャンされます。 このチェックボックスをオフにすると、メールデータベースはスキャンされません。 既定では、このチェックボックスはオフです。
メール形式のファイルをスキャン	このチェックボックスでは、プレーンテキストのメールメッセージのファイルをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、プレーンテキストのメッセージがスキャンされます。 このチェックボックスをオフにすると、プレーンテキストのメッセージはスキャンされません。 既定では、このチェックボックスはオフです。
スキャン時間が次を超えたらファイルをスキップする（秒）	このフィールドでは、ファイルをスキャンする最大時間を秒単位で指定できます。指定した時間が経過した後、ファイルのスキャンは停止されます。 使用できる値：0 ～ 9999。値が 0 に設定されると、スキャン時間は制限されません。 既定値：0
ファイルのサイズが次を超えたらスキップする（MB）	このフィールドでは、スキャンするファイルの最大サイズをメガバイト単位で指定できます。 使用できる値：0 ～ 999999。値が 0 に設定されると、サイズにかかわらず、すべてのファイルがスキャンされます。 既定値：0
感染していないオブジェクトを記録する	このチェックボックスでは、*ObjectProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、スキャンされたすべてのオブジェクトの *ObjectProcessed* タイプのイベントをログに記録します。 このチェックボックスをオフにすると、スキャンされたオブジェクトの *ObjectProcessed* タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
処理されていないオブジェクトを記録する	このチェックボックスでは、スキャン中にファイルを処理できない場合、*ObjectNotProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、［*ObjectNotProcessed*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*ObjectNotProcessed*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
圧縮されたオブジェクトを記録する	このチェックボックスでは、検出されたすべての圧縮されたオブジェクトに関する *PackedObjectDetected* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、［*PackedObjectDetected*］タイプのイベントをログに記録します。 このチェックボックスをオフにすると、［*PackedObjectDetected*］タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。
iChecker 技術を使用する	このチェックボックスでは、前回のファイルのスキャン以降の新しいファイルおよび変更されたファイルのみをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、前回のスキャン以降の新しいファイルおよび変更されたファイルのみがスキャンされます。 このチェックボックスをオフにすると、作成日または変更日に関係なくファイルがスキャンされます。 既定では、このチェックボックスはオンです。
ヒューリスティック分析を使用する	このチェックボックスでは、ファイルのスキャン中にヒューリスティック分析を使用するかどうかを選択します。 既定では、このチェックボックスはオンです。
ヒューリスティック分析のレベル	［**ヒューリスティック分析を使用する**］チェックボックスをオンにすると、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）：カスペルスキーのエキスパート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。
複数のスキャンタスクを同時に実行しない	スキャンが既に実行中の場合はスキャンタスクの開始を遅延します。現在のスキャンが続行される場合は Kaspersky Endpoint Security は新しいスキャンタスクをエンキューします。これは、コンピューターの負荷の最適化に役立ちます。たとえば、本製品がスケジュールに従って完全スキャンタスクを開始していたとします。ユーザーが製品インターフェイスから簡易スキャンを開始しようとすると、Kaspersky Endpoint Security はこの簡易キャンタスクをエンキューし、完全スキャンタスクの完了後にこのタスクが自動的に開始されます。 既定では、このチェックボックスはオフです。

［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
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。

設定	説明
除外範囲名	除外範囲の名前を入力するフィールド。この名前は、［**除外範囲**］ウィンドウの表で表示されます。 この入力フィールドを空白のままにすることはできません。
この範囲を使用する	このチェックボックスでは、製品の実行時にこの範囲をスキャンから除外するかどうかを選択します。 チェックボックスをオンにすると、スキャン中にこの範囲が除外されます。 このチェックボックスをオフにすると、この範囲がスキャン範囲に含まれます。このチェックボックスをオンにすることにより、後からこの範囲を除外することができます。 既定では、このチェックボックスはオンです。
ファイルシステム、アクセスプロトコル、パス	これらの設定では、除外範囲を設定できます。 ファイルシステムのドロップダウンリストで、スキャンから除外するディレクトリのファイルシステムの種別を選択できます： • **Local** – ローカルディレクトリ。 • **Mounted** – マウントされたディレクトリ。 • **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。 「**/**」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。
ファイルシステム名	除外範囲に追加するディレクトリがあるファイルシステムの名前を入力するためのフィールドです。 このフィールドは、ファイルシステムのドロップダウンリストで［**Mounted**］が選択され、右側のドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。
マスク	このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。マスクは、［パス］フィールドに指定されたディレクトリ内のオブジェクトにのみ適用されます。 既定では、すべてのオブジェクトを示すマスク「*****」がリストに含まれています。 マスクは、追加、編集、削除できます。

役立つ記事

マスクを指定する方法

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。

タグの使用方法

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。

［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）。

［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。

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。

カスタムの簡易スキャン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。

*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、以下の表に示す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
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、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、除外範囲、マスクによる除外、脅威名による除外をカスタマイズできます。

［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
範囲名	スキャン範囲名。
パス	スキャンするディレクトリのパス。
ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：**追加**、**編集**、**削除**、**上に移動**、**下に移動**。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、範囲の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。
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。
	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。 「**/**」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。

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。

役立つ記事

マスクを指定する方法

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。

タグの使用方法

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。

［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	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。アーカイブのスキャンの所要時間を短縮するには、**全般スキャン設定**セクションで［**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）**］の設定を構成します。 このチェックボックスをオフにすると、アーカイブはスキャンされません。 既定では、このチェックボックスはオンです。
SFX アーカイブをスキャン	このチェックボックスでは、*自己解凍アーカイブ*をスキャンするかどうかを選択します。自己解凍アーカイブとは、実行可能な展開モジュールを含むアーカイブです。 このチェックボックスをオンにすると、自己解凍アーカイブがスキャンされます。 このチェックボックスをオフにすると、自己解凍アーカイブはスキャンされません。 このチェックボックスは、［**アーカイブをスキャン**］がオフの場合に使用できます。 既定では、このチェックボックスはオンです。
メールデータベースをスキャン	このチェックボックスでは、Microsoft Outlook、Outlook Express などのメールアプリケーションのメールデータベースをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、メールデータベースはスキャンされます。 このチェックボックスをオフにすると、メールデータベースはスキャンされません。 既定では、このチェックボックスはオフです。
メール形式のファイルをスキャン	このチェックボックスでは、プレーンテキストのメールメッセージのファイルをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、プレーンテキストのメッセージがスキャンされます。 このチェックボックスをオフにすると、プレーンテキストのメッセージはスキャンされません。 既定では、このチェックボックスはオフです。
スキャン時間が次を超えたらファイルをスキップする（秒）	このフィールドでは、ファイルをスキャンする最大時間を秒単位で指定できます。指定した時間が経過した後、ファイルのスキャンは停止されます。 使用できる値：0 ～ 9999。値が 0 に設定されると、スキャン時間は制限されません。 既定値：0
ファイルのサイズが次を超えたらスキップする（MB）	このフィールドでは、スキャンするファイルの最大サイズをメガバイト単位で指定できます。 使用できる値：0 ～ 999999。値が 0 に設定されると、サイズにかかわらず、すべてのファイルがスキャンされます。 既定値：0
感染していないオブジェクトを記録する	このチェックボックスでは、*ObjectProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、スキャンされたすべてのオブジェクトの *ObjectProcessed* タイプのイベントをログに記録します。 このチェックボックスをオフにすると、スキャンされたオブジェクトの *ObjectProcessed* タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。

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**］チェックボックスをオンにすると、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）：カスペルスキーのエキスパート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。
複数のスキャンタスクを同時に実行しない	スキャンが既に実行中の場合はスキャンタスクの開始を遅延します。現在のスキャンが続行される場合は Kaspersky Endpoint Security は新しいスキャンタスクをエンキューします。これは、コンピューターの負荷の最適化に役立ちます。たとえば、本製品がスケジュールに従って完全スキャンタスクを開始していたとします。ユーザーが製品インターフェイスから簡易スキャンを開始しようとすると、Kaspersky Endpoint Security はこの簡易キャンタスクをエンキューし、完全スキャンタスクの完了後にこのタスクが自動的に開始されます。 既定では、このチェックボックスはオフです。

［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
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。 「**/**」パスは既定で指定されています。この指定により、ローカルファイルシステムのすべてのディレクトリがスキャンから除外されます。
ファイルシステム名	除外範囲に追加するディレクトリがあるファイルシステムの名前を入力するためのフィールドです。 このフィールドは、ファイルシステムのドロップダウンリストで［**Mounted**］が選択され、右側のドロップダウンリストで［**カスタム**］が選択されている場合に使用できます。
マスク	このリストには、スキャンから除外するオブジェクト名のマスクが含まれます。マスクは、［パス］フィールドに指定されたディレクトリ内のオブジェクトにのみ適用されます。 既定では、すべてのオブジェクトを示すマスク「*****」がリストに含まれています。 マスクは、追加、編集、削除できます。

役立つ記事

マスクを指定する方法

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。

タグの使用方法

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。

［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）。

［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。

コンテナの監視

管理コンソールでは、ポリシーのプロパティ（**全般設定 → コンテナスキャン設定**）でコンテナ監視コンポーネントを設定できます。

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 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。
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。

設定	説明
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

コンテナスキャン

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。

カスタムコンテナスキャン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。

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、以下の表に記載されている設定を管理できます。

コンテナのスキャンタスクの設定

設定	説明
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。

コンテナスキャンタスクのプロパティの**除外**セクションでは、マスクによる除外および脅威名による除外を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。

設定	説明
名前のマスク	スキャン対象に含めるイメージの名前または名前のマスクを入力するフィールド。 既定では、「*」というマスクが指定されています。これは、すべてのイメージがスキャン対象となります。
脅威の検知時の処理	ドロップダウンリストで、感染したオブジェクトの検知時にイメージに対して実行する処理を選択します： • **イメージをスキップ**（既定値）– 感染したオブジェクトが検知されても、イメージに対して何の処理も実行しません。 • **イメージを削除** – 感染したオブジェクトの検知時に、イメージを削除します（推奨しないオプションです）。すべての依存関係も削除されます。実行中のコンテナは停止され、それから削除されます。
各レイヤーをスキャン	このチェックボックスでは、イメージと実行中のコンテナのすべてのレイヤーのスキャンを行うかどうかを選択できます。 既定では、このチェックボックスはオフです。

［スキャンの設定］ウィンドウ

このウィンドウでは、タスクのファイルスキャンを設定します。

スキャンの設定

設定	説明
アーカイブをスキャン	このチェックボックスでは、アーカイブをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、アーカイブがスキャンされます。 アーカイブをスキャンするには、アーカイブを解凍する必要があるためスキャン速度が遅くなる可能性があります。アーカイブのスキャンの所要時間を短縮するには、**全般スキャン設定**セクションで［**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）**］の設定を構成します。 このチェックボックスをオフにすると、アーカイブはスキャンされません。 既定では、このチェックボックスはオンです。
SFX アーカイブをスキャン	このチェックボックスでは、*自己解凍アーカイブ*をスキャンするかどうかを選択します。自己解凍アーカイブとは、実行可能な展開モジュールを含むアーカイブです。 このチェックボックスをオンにすると、自己解凍アーカイブがスキャンされます。 このチェックボックスをオフにすると、自己解凍アーカイブはスキャンされません。 このチェックボックスは、［**アーカイブをスキャン**］がオフの場合に使用できます。 既定では、このチェックボックスはオンです。
メールデータベースをスキャン	このチェックボックスでは、Microsoft Outlook、Outlook Express などのメールアプリケーションのメールデータベースをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、メールデータベースはスキャンされます。 このチェックボックスをオフにすると、メールデータベースはスキャンされません。 既定では、このチェックボックスはオフです。
メール形式のファイルをスキャン	このチェックボックスでは、プレーンテキストのメールメッセージのファイルをスキャンするかどうかを選択します。 このチェックボックスをオンにすると、プレーンテキストのメッセージがスキャンされます。 このチェックボックスをオフにすると、プレーンテキストのメッセージはスキャンされません。 既定では、このチェックボックスはオフです。
スキャン時間が次を超えたらファイルをスキップする（秒）	このフィールドでは、ファイルをスキャンする最大時間を秒単位で指定できます。指定した時間が経過した後、ファイルのスキャンは停止されます。 使用できる値：0 ～ 9999。値が 0 に設定されると、スキャン時間は制限されません。 既定値：0
ファイルのサイズが次を超えたらスキップする（MB）	このフィールドでは、スキャンするファイルの最大サイズをメガバイト単位で指定できます。 使用できる値：0 ～ 999999。値が 0 に設定されると、サイズにかかわらず、すべてのファイルがスキャンされます。 既定値：0
感染していないオブジェクトを記録する	このチェックボックスでは、*ObjectProcessed* タイプのイベントをログに記録するかどうかを選択します。 このチェックボックスをオンにすると、スキャンされたすべてのオブジェクトの *ObjectProcessed* タイプのイベントをログに記録します。 このチェックボックスをオフにすると、スキャンされたオブジェクトの *ObjectProcessed* タイプのイベントを記録しません。 既定では、このチェックボックスはオフです。

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**］チェックボックスをオンにすると、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）：カスペルスキーのエキスパート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。
複数のスキャンタスクを同時に実行しない	スキャンが既に実行中の場合はスキャンタスクの開始を遅延します。現在のスキャンが続行される場合は Kaspersky Endpoint Security は新しいスキャンタスクをエンキューします。これは、コンピューターの負荷の最適化に役立ちます。たとえば、本製品がスケジュールに従って完全スキャンタスクを開始していたとします。ユーザーが製品インターフェイスから簡易スキャンを開始しようとすると、Kaspersky Endpoint Security はこの簡易キャンタスクをエンキューし、完全スキャンタスクの完了後にこのタスクが自動的に開始されます。 既定では、このチェックボックスはオフです。

［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。
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）。

［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。

リムーバブルドライブのスキャン

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構成できます（**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、複合オブジェクト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。 • **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。
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。 • **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。

役立つ記事

簡易スキャンのファイル種別

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。

ふるまい検知

管理コンソールでは、ポリシーのプロパティ（**先進の脅威対策 → ふるまい検知**）で、ふるまい検知の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。 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）のテレメトリからプロセスを除外	このチェックボックスでは、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る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。

役立つ記事

マスクを指定する方法

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。

脆弱性攻撃ブロック

管理コンソールでは、ポリシーのプロパティ（**先進の脅威対策 → ふるまい検知**）で脆弱性攻撃ブロックを設定できます。

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	［**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。
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。
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。

アンチクリプター

管理コンソールでは、ポリシーのプロパティ（**先進の脅威対策 → アンチクリプター**）でアンチクリプター設定を管理できます。

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
範囲名	スキャン範囲名。
パス	スキャンするディレクトリのパス。
ステータス	製品がこの範囲をスキャンするかどうかをステータスに示します。

表内の項目に対して可能な操作は次の通りです：**追加**、**編集**、**削除**、**上に移動**、**下に移動**。

［**下へ**］をクリックすると、表内で選択した項目が下に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**上へ**］をクリックすると、表内で選択した項目が上に移動します。

指定された範囲にあるオブジェクトは、スキャン範囲の表の並び順でスキャンされます。親ディレクトリとは異なるセキュリティ設定をサブディレクトリに指定する場合は、サブディレクトリをその親ディレクトリよりも表内で上に配置する必要があります。

このボタンは、1つの範囲を表から選択している場合に使用できます。

［**削除**］をクリックすると、選択した範囲がスキャンから除外されます。

このボタンは、少なくとも1つのスキャン範囲を表から選択している場合に使用できます。

選択した要素の設定が、別のウィンドウで変更されます。

［**追加**］をクリックすると、新しい項目を設定できるウィンドウが表示されます。

指定された範囲にあるオブジェクトは、範囲の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。
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。 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。

役立つ記事

マスクを指定する方法

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。

［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）。

設定	説明
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
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。
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： • **ローカル**：ローカルディレクトリ。 • **Mounted**：マウントされたディレクトリ。 • **リモートでマウント済みのすべての場所**：Samba プロトコルおよび NFS プロトコルを使用してデバイスにマウントされた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た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た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の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 **ローカル** 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。 「/」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** タイプが選択され、右側のドロップダウンリストで **カスタム** 項目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。

役立つ記事

マスクを指定する方法

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。

タグの使用方法

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。

［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。

Kaspersky Security Network

管理コンソールでは、ポリシーのプロパティ（［**先進の脅威対策**］ → ［**Kaspersky Security Network**］）で、Kaspersky Endpoint Security における 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	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	クラウドモードでは、Kaspersky Endpoint Security は軽量版の定義データベースを使用するため、コンピューターの RAM への負荷が約半分になります。 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。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。

有害 USB 攻撃ブロック

管理コンソールでは、ポリシーのプロパティ（**脅威対策 → 有害 USB 攻撃ブロック**）でウェブ脅威対策の設定を管理できます。

有害 USB 攻撃ブロックの設定

設定	説明
有害 USB 攻撃ブロックを有効にする	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 デバイス認証の最大試行回数	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。
USB デバイスの最大認証試行回数に達した場合にブロックする期間（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）
USB デバイスの承認時にセキュリティキーボードの使用を許可しない	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 デバイスの認証におけるバーコードの使用を禁止する	この切り替えボタンを有効にすると、本製品では、承認コードの入力に使用できない USB デバイスの承認にバーコードを使用することは許可されません。

通信と危険サイト対策

メール脅威対策

管理コンソールでは、ポリシーのプロパティ（**脅威対策 → メール脅威対策**）でウェブ脅威対策の設定を管理できます。

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。
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。 この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。

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、**送受信メッセージ**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。
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。

ウェブ脅威対策

管理コンソールでは、ポリシーのプロパティ（**脅威対策 → ウェブ脅威対策**）でウェブ脅威対策の設定を行うことができます。

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。

役立つ記事

マスクを指定する方法

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。

ネットワーク脅威対策

管理コンソールでは、ポリシーのプロパティ（**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。

ファイアウォール管理

管理コンソールでは、ポリシーのプロパティ（**脅威対策 → ファイアウォール管理**）でファイアウォール管理設定を構成できます。

ファイアウォール管理の設定

設定	説明
ファイアウォール管理を有効にする	このチェックボックスでは、ファイアウォール管理を有効にするかどうかを選択します。 既定では、このチェックボックスはオフです。
ネットワークパケットルール	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**ネットワークパケットルール**］ウィンドウが表示されます。このウィンドウでは、ネットワーク接続の試行を検知した場合にファイアウォール管理が適用するネットワークパケットルールを編集できます。
使用可能なネットワーク	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**使用可能なネットワーク**］ウィンドウが表示されます。このウィンドウでは、ファイアウォール管理が監視するネットワークのリストを設定します。
受信接続	このドロップダウンリストでは、ネットワークの受信接続に対して実行する処理を選択します： • 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。
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。

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
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**

セキュリティコントロール

デバイスコントロール

管理コンソールでは、ポリシーのプロパティ（**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の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。

設定	説明
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。 • **バスに依存**（既定値）– 接続バスのアクセスモードに応じて、デバイスへのアクセスを許可またはブロックします。 • **ルール別** – デバイスへのアクセスを、アクセスルールとスケジュールに従って許可またはブロックします。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。

設定	説明
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： • **アクススケジュール** – 既存のアク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**のアクススケジュールが含まれています。**接続バス**を介したアクセスがこのデバイス種別で許可されている場合、既定のアク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	アクセスルールが適用されるローカルユーザー名またはユーザーグループ名。

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、デバイスのアクススケジュールを設定できます。

デバイスへのアクススケジュール

設定	説明
名前	アク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。

ウェブコントロール

管理コンソールでは、ポリシーのプロパティ（**セキュリティコントロール → ウェブコントロール**）でウェブコントロールの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。
	また、［**詳細設定**］->［**インポート**］の順にクリックしてファイルからルールのリストをインポートしたり、［**追加**］->［**選択項目をエクスポート**］または［**追加**］->［**すべてエクスポート**］の順にクリックして追加したルールのリストをファイルにエクスポートすることもできます。インポート時に、ルールのリストを置き換えるか、既存のリストにルールのリストを追加するかを尋ねるメッセージが表示されます。

デフォルトのルール	ドロップダウンリストで、他のルールの対象でない Web リソースへのアクセスを本製品がどのように制御するかを制御する既定のルールを選択できます。 • **許可**（既定値）– Web リソースへのアクセスを許可します。 • **ブロック** – Web リソースへのアクセスをブロックします。
メッセージテンプレート	この設定グループには、**設定**が含まれています。このボタンをクリックすると、［**メッセージテンプレート**］ウィンドウが表示されます。

［ウェブコントロールルール］ウィンドウ

このウィンドウでは、Web リソースアクセスルールの設定を行うことができます。

ウェブコントロールルールの追加

設定	説明
ルール名	Web リソースアクセスルールの名前を入力するフィールド。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。

設定	説明
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。

アプリケーションコントロール

管理コンソールでは、ポリシーのプロパティ（[**セキュリティコントロール**] → [**アプリケーションコントロール**]）でアプリケーションコントロール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。
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**］。

インベントリ

Kaspersky Security Center 管理コンソールでは、インベントリタスクを使用して、保護されたデバイスのアプリケーションのインベントリを実行できます。

インベントリのユーザータスクを作成して実行できます。タスクの設定を編集して、スキャン設定を管理できます。

> 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に対して実行す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。 • **削除** – ゴールデンイメージカテゴリからアプリケーションを削除します。タスクが開始されるとすぐにカテゴリがクリアされ、デバイス上のファイルのインベントリは実行されません。 ゴールデンイメージカテゴリをアプリケーションコントロールルールで使用できます。
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。 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。

役立つ記事

マスクを指定する方法

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。

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
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。
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。
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。

役立つ記事

マスクを指定する方法

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。

システム変更監視

管理コンソールでは、ポリシーのプロパティ（**セキュリティコントロール → システム変更監視**）でシステム変更監視設定を構成できます。

システム変更監視設定の設定

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。

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］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。
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。

設定	説明
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。

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。

カスタムのシステム変更チェック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。

システム変更チェックのプロパティの［**除外範囲**］セクションで、監視の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。
ファイルシステム、アクセスプロトコル、パス	監視範囲に含めるローカルディレクトリのパスを入力するフィールド。パスの指定にマスクを使用できます。 このフィールドを空白のままにすることはできません。 既定のパスは、/opt/kaspersky/kesl です。

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。

役立つ記事

マスクを指定する方法

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。

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
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。 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）。

役立つ記事

マスクを指定する方法

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）。

ローカルタスク

タスクの管理

管理コンソールでは、ポリシーのプロパティ（**ローカルタスク → タスク管理**）でタスクを表示および管理する権限を設定できます。

タスク管理の設定

設定	説明
ローカルタスクを許可する	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。

高度な脅威と標的型攻撃からの保護

Kaspersky Managed Detection and Response との連携

管理コンソールでは、ポリシーのプロパティ（**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、MDR BLOB ファイルをアップロードできます。

MDR 連携の設定

設定	説明
Managed Detection and Response を有効にする	このチェックボックスは、Kaspersky Endpoint Security と Kaspersky Managed Detection and Response ソリューションを連携するために必要な 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。 テナントが存在する場合、または MDR BLOB ファイルを使用して MDR コンポーネントを有効化している場合は、この操作が必須です。

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。

Kaspersky Endpoint Detection and Response（オンプレミス）との連携

管理コンソールでは、ポリシーのプロパティ（**Detection and Response → EDR 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 アプリケーションと Kaspersky Endpoint Detection and Response (KATA) コンポーネントを連携するための設定を管理できます。

EDR Expert（オンプレミス）コンポーネントについて、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（オンプレミス）連携モードが選択されている場合、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できません。連携モードは、Web コンソールで変更できます。

Kaspersky Endpoint Detection and Response（オンプレミス）との連携設定

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では、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では、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。

設定	説明
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）。 既定値です：`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）。 既定値です：`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）。 既定値です：`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。次に、**暗号化されたコンテナのパスワード**フィールドにクライアント証明書のパスワードを入力します。
	  このフィールドは必須です。パスワードを入力せずに設定を保存しようとすると、エラーメッセージが表示されます。
	パスワードが正しい場合、**OK**ボタンが有効になります。設定を保存できます。
	• ［**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`。

Kaspersky Endpoint Detection and Response (KATA) 連携

管理コンソールでは、ポリシーのプロパティ（［**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。次に、**暗号化されたコンテナのパスワード**フィールドにクライアント証明書のパスワードを入力します。
	  このフィールドは必須です。パスワードを入力せずに設定を保存しようとすると、エラーメッセージが表示されます。
	パスワードが正しい場合、**OK**ボタンが有効になります。設定を保存できます。
	• ［**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`。

設定	説明
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`。

KUMA との連携

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、ポリシープロパティ（**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 サーバーへの接続に使用するプロトコル：TCP、UDP、または圧縮を使用する HTTP/HTTPS。 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。

設定	説明
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。

［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。次に、**暗号化されたコンテナのパスワード**フィールドにクライアント証明書のパスワードを入力します。

このフィールドは必須です。パスワードを入力せずに設定を保存しようとすると、エラーメッセージが表示されます。

パスワードが正しい場合、**OK**ボタンが有効になります。設定を保存できます。

隔離

管理コンソールでは、ポリシーのプロパティ（［**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。 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の既定値は 200 で、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 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

オブジェクトの実行防止

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できます。

ポリシーのプロパティ（[**製品設定**] → [**Detection and Response**] → [**EDR 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。

オブジェクトの実行防止 の **オブジェクトの実行防止を有効にする** チェックボックスでは、オブジェクトの実行防止用の EDR Expert（オンプレミス）ルールを有効または無効にします。

全般設定

管理コンソールでは、ポリシーのプロパティ（[**全般設定**]）で、アプリケーション全体の動作および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を管理できます。

プロキシサーバー

管理コンソールでは、ポリシーのプロパティ（**全般設定 → プロキシサーバー設定**）でプロキシサーバー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。

設定	説明
プロキシサーバー認証を使用する	このチェックボックスでは、ユーザー名とパスワードを使用したプロキシサーバー認証を使用するかどうかを選択します。 このチェックボックスは、［**指定したプロキシサーバー設定を使用する**］をオンにすると使用できます。 既定では、このチェックボックスはオフです。 HTTP プロキシ経由で接続する場合は、他のシステムへのログインに使用しない別のアカウントを使用することを推奨します。HTTP プロキシがセキュアでない接続を使用しているため、アカウントが危険にさらされている可能性があります。
ユーザー名	プロキシサーバー認証のために使用されるユーザー名の入力フィールド。 この入力フィールドは、**プロキシサーバー認証を使用する**のチェックボックスがオンの場合に使用できます。
パスワード	プロキシサーバー認証のためのユーザーパスワードの入力フィールド。 パスワードの複雑性とブルートフォース攻撃防止メカニズムにより、6か月以内にパスワードが推測できないようにすることを推奨します。 ［**表示**］をクリックすると、［**パスワード**］フィールドでユーザーパスワードが見えるように表示されます。既定では、ユーザーパスワードは非表示で、アスタリスクで示されます。 **プロキシサーバー認証を使用する**のチェック ボックスがオンの場合、テキストボックスとボタンが利用可能になります。
Kaspersky Security Center を製品のアクティベーションのプロキシサーバーとして使用する	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。本製品を Light Agent モードで使用している場合、ライセンスの情報は 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）** – 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。

設定	説明
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。

スキャンタスクによる CPU 使用率

管理コンソールでは、ポリシーのプロパティ（［**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、スキャンタスクの CPU 使用率制限を有効または無効にし、メモリ使用量制限を設定できます。

パフォーマンス の **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** ウィンドウが開きます。このウィンドウの **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）。

CPU とメモリの使用状況の設定

設定	説明
スキャンタスクの CPU 使用率を制限する（%）	このチェックボックスは、*マルウェアのスキャン*、*簡易スキャン*、*インベントリ*、および*コンテナのスキャン*タスクの CPU 使用率制限を有効または無効にします。 チェックボックスをオンにすると、すべてのプロセッサコアの最大使用率が右のフィールドでで指定した率を超えなくなります。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

バッテリー電源でのタスクの実行

管理コンソールでは、ポリシーのプロパティ（［**全般設定**］ → ［**製品設定**］の［**パフォーマンス**］セクション）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。

バッテリー駆動時のタスクの設定

設定	説明
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	このチェックボックスでは、スケジュールされたタスクをキャンセル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。 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。

アプリケーションの起動

管理コンソールでは、ポリシーのプロパティ（［**全般設定**］ → ［**製品設定**］の［**アプリケーションの起動設定**］セクション）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

重要なアップデートを受信したときに自動的に再起動

管理コンソールでは、ポリシーのプロパティ（[**全般設定**] → [**アプリケーション設定**]）で、重要なアップデートのインストール時にアプリケーションを自動的に再起動するように設定できます。

[**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、重要なアップデートの受信時にアプリケーションを再起動するように設定できます（次の表を参照）。

重要なアップデートを適用するための設定

設定	説明
重要なアップデートの受信時にアプリケーションを自動的に再起動する	このチェックボックスでは、アプリケーションのインストール後最初の24時間が経過した後に重要なアップデートを受信した場合に、アプリケーションを自動的に再起動するかどうかをオンまたはオフにします。 既定では、このチェックボックスはオフです。 このチェックボックスをオンにすると、インストール後24 時間が経過している場合、重要なアップデートの適用後にアプリケーションが再起動します。

パスワードによる保護

管理コンソールでは、ポリシーのプロパティ（**全般設定** → **インターフェイス**、**パスワードによる保護**セクション）で、パスワードによる保護設定を構成できます。

パスワードによる保護で、**設定**ボタンをクリックすると、**パスワードによる保護の設定**ウィンドウが開きます。このウィンドウで、パスワードによる保護設定を編集できます（下の表を参照）。

アプリケーションの起動設定

設定	説明
パスワードによる保護を有効にする	このチェックボックスをオンまたはオフにして、アプリケーション設定のパスワードによる保護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。
権限	この表には、アプリケーション設定の変更権限を設定できるユーザーとグループが含まれています。表には次の列があります： • **ユーザーまたはグループ**は、権限が設定されているローカルユーザーまたはドメインユーザーの名前、またはユーザーグループの名前です。 • **種別** は、権限が設定されている **ユーザー** または **グループ** です。 • **権限**は、ユーザーまたはグループに実行が許可されている操作のリストです。 ユーザーまたはユーザーグループを追加、編集、削除できます。 **追加**ボタンをクリックすると、**ユーザーまたはグループの権**ウィンドウが開きます。このウィンドウで、ユーザーまたはグループを追加し、アプリケーション設定の変更権限を設定できます。

トレースおよびダンプの設定

管理コンソールでは、ポリシーのプロパティ（**全般設定 → アプリケーション設定**、**トレースとダンプの設定**セクション）で、トレースとダンプの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、トレースとダンプの設定を編集できる［**トレースとダンプの設定**］ウィンドウが開きます（次の表を参照）。

トレースおよびダンプの設定

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
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。

アプリケーションが使用する常駐メモリ

管理コンソールでは、ポリシーのプロパティ（**全般設定 → 製品設定**）で、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。

アプリケーションによる常駐メモリ使用量の設定

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。

設定	説明
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。 既定値です：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。 既定値です：2000.

暗号化された接続のスキャン

管理コンソールでは、ポリシーのプロパティ（**全般設定 → 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。
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。

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。

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。

グローバル除外リスト

管理コンソールでは、ポリシーのプロパティ（**全般設定 → グローバル除外**）でグローバル除外を設定できます。

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。 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。

役立つ記事

マスクを指定する方法

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。

プロセスメモリのスキャンからの除外

管理コンソールでは、ポリシーのプロパティ（**全般設定 → プロセスメモリを除外**）で、プロセスメモリをスキャンから除外するように設定できます。

プロセスメモリをスキャンから除外で**設定**をクリックすると、除外リストを作成できるウィンドウが開きます。

プロセスメモリをスキャンから除外ウィンドウのリストには、アプリケーションがプロセスメモリのスキャンから除外するプロセスへのパスが含まれています。パスの指定にマスクを使用できます。既定では、このリストは空です。

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。

役立つ記事

マスクを指定する方法

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。

バックアップ

管理コンソールでは、ポリシーのプロパティ（[**全般設定**] → [**ストレージ設定**]）および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 → [アプリケーションプロパティ] ウィンドウ → [**ストレージ設定**]）でバックアップ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 ～ 4000。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。

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

管理コンソールでは、ポリシーのプロパティ（**全般設定 → 製品設定**、**スキャン設定**セクション）で、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設定できます。

デバイスまたはデータを侵害するために侵入者が使用できるアプリケーションの検知設定

設定	説明
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、ユーザーのコンピューターまたはデータに損害を与える目的でハッカーが悪用す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。

ファイル操作のインターセプト

管理コンソールでは、ポリシーのプロパティ（**全般設定 → 製品設定**、**ファイル操作のインターセプトモード**セクション）で、ファイル操作のインターセプトモードを設定できます。

ファイル操作のインターセプト設定

設定	説明
スキャン中にファイルへのアクセスをブロック	このチェックボックスでは、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、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に、ファイルへのアクセス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。 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。

Kaspersky Security Center 保管領域への情報の送信

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全体リストは、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**]）でも利用できます。

クライアントデバイス上のカスペルスキーアプリケーションによってバックアップに配置されたファイルの全体リストは、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**]）で利用できます。

未処理ファイルに関する情報は、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。

クライアントデバイスにインストールされている、または接続されているデバイスに関する情報は、管理コンソール（[**詳細設定**] → [**リポジトリ**] → [**ハードウェア**]）の機器の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で検出されたアプリケーションに関する情報は、管理コンソール（[**詳細設定**] → [**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のリストにも表示されます。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。

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（[**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。

管理サーバーへのデータ転送設定

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。

設定	説明
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。

システムイベントインターセプター

管理コンソールでは、ポリシーのプロパティ（［**全般設定**］ → ［**OS 対話設定**］、［**システムイベント遮断設定**］セクション）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。

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。

テレメトリの詳細設定

管理コンソールでは、ポリシーのプロパティ（［**全般設定**］ → ［**OS 対話設定**］の［**テレメトリの詳細設定**］セクション）で、テレメトリの詳細設定を管理できます。

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。

Light Agent モード

管理コンソールでは、ポリシーのプロパティ（**Light Agent モード**）で、Light Agent を SVM に接続するための設定を管理できます。

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。

Integration Server 接続設定

設定	説明
アドレス	Integration Server がインストールされているデバイスの IPv4 形式による 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。

設定	説明
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。

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、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た仮想マシンと同じサーバーグループに配置されます（OpenStack または VK Private Cloud プラットフォーム上で稼働する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た仮想マシンと同じノードに配置されます（Basis Dynamix Enterprise の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、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た仮想マシンと同じ OpenStack プロジェクトに導入されます（OpenStack プラットフォームまたは VK Private Cloud 上で実行されている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た仮想マシンと同じゾーン内に配置されます（Basis Dynamix Enterprise の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、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た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 プラットフォームまたは VK Private Cloud 上で実行されている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た仮想マシンと同じデータセンター内に配置されます（Basis Dynamix Enterprise の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。

既知の問題と制限事項

アプリケーションの制限事項

Kaspersky Endpoint Security は、次の場合にサポートされません：

- OSnova オペレーティングシステムで、クローズドソフトウェア環境モードおよび強化カーネルモードを使用している場合。
- Red Hat Enterprise Linux ベースのオペレーティングシステムで、IMA サブシステムを使用している場合。
- Red Hat Enterprise Linux ベースのオペレーティングシステムで、FIPS モードを使用している場合。
- Ubuntu オペレーティングシステムおよび SUSE Linux Enterprise Server ベースのオペレーティングシステムで、AppArmor 強制アクセス制御システムを使用している場合。
- Grsecurity セキュリティシステムを使用している場合（すべてのオペレーティングシステム）。
- seccomp メカニズムを使用している場合（すべてのオペレーティングシステム）。
- WSL1 および WSL2 テクノロジーを使用している場合（すべてのオペレーティングシステム）。
- ファイルシステムの特定のマウントオプション（noexec、nosuid など）を使用している場合。
- Kaspersky Endpoint Security がコンテナ内にインストールされている場合。

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。

特定のアーキテクチャにおける本製品の制限事項

本製品を次のプロセッサアーキテクチャで実行する場合、制限事項があります：

Elbrus

- Light Agent モード：サポートされていません。
- EDR エージェントモード：サポートされていません。
- 有害 USB 攻撃ブロック：機能しません。
- ぜい弱性攻撃ブロック：機能しません。

- ウェブ脅威対策：フィッシングリンクを検知するためにウェブページをスキャンする際、ヒューリスティック分析は利用できません。
- Kaspersky Endpoint Detection and Response Optimum との連携：機能しません。
- Kaspersky Endpoint Detection and Response Expert（クラウド）との連携：機能しません。
- Kaspersky Endpoint Detection and Response (KATA) との連携：機能しません。
- Kaspersky Managed Detection and Response との連携：機能しません。
- サンドボックス：機能しません。
- KUMA 連携：機能しません。
- コンテナスキャン：機能しません。
- 更新可能なカーネルモジュール：サポートされていません。
- 管理グラフィカルユーザーインターフェイス：Sandbox コンポーネントがサポートされていないため、ユーザーは Sandbox でのスキャン用にファイルを送信できません。

一部の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制限事項

このアプリケーションは、次のオペレーティングシステムで実行する場合に制限事項があります：

Astra Linux Special Edition RUSB.10015-01 (operational update 1.5)

- 有害 USB 攻撃ブロック：オペレーティングシステムに systemd-logind サービスがないため、機能しません。
- 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各タスクにおける CPU リソース使用量の制限は、「4.2.0-23-generic」カーネルでは機能しません。

CentOS 5.2 および 5.4

- ふるまい検知：プロセス起動の同期インターセプトを利用できないため、このコンポーネントが正しく動作することは保証されません。
- メール脅威対策：機能しません。
- ウェブ脅威対策：TProxy メカニズムがサポートされていないため、機能しません。
- ネットワーク脅威対策：TProxy メカニズムがサポートされていないため、機能しません。
- アンチクリプター：TProxy メカニズムがサポートされていないため、機能しません。
- 有害 USB 攻撃ブロック：オペレーティングシステムに systemd-logind サービスがないため、機能しません。
- コンテナスキャン：オペレーティングシステムがコンテナをサポートしていないため、機能しません。

- デバイスコントロール：デバイスの読み取り専用モードは、アプリケーションでこのモードを有効にした後にデバイスが接続された場合にのみ機能します。このモードが有効になる前に接続されていたデバイスについては、アクセスモードは変更されません。
- アプリケーションコントロール：プロセス開始の同期インターセプトに必要な fanotify テクノロジーがサポートされていないため、機能しません。
- Firewall 管理：iptables へのチェーンの追加がサポートされていないため、機能しません。
- ウェブコントロール：TProxy メカニズムがサポートされていないため、機能しません。
- 更新可能なカーネルモジュール：サポートされていません。
- ネットワーク分離：TProxy メカニズムがサポートされていないため、機能しません。
- オブジェクトの実行防止は、プロセス開始の同期インターセプトがないため、機能しません。
- Kaspersky Endpoint Detection and Response Optimum との連携：機能しません。
- Kaspersky Endpoint Detection and Response Expert（クラウド）との連携：機能しません。
- Kaspersky Endpoint Detection and Response (KATA) 連携：eBPF テレメトリソースを利用できません。
- Kaspersky Managed Detection and Response 連携：auditd テレメトリソースを利用できません。
- グラフィカルユーザーインターフェイス：オペレーティングシステムに libxcb ライブラリがないため、機能しません。
- Kaspersky Security Center ネットワークエージェント：追加のデバイス設定が必要です。Kaspersky Security Center のヘルプを参照してください。
- インストール / 削除：このバージョンのオペレーティングシステムでは、このアプリケーションは SELinux と互換性がありません。考えられる解決策：SELinux を非ブロッキングモード（permissive モード）に設定する、SELinux を無効にする、または SELinux を手動で設定する。
- マルウェアのスキャン：glibc バージョン 2.11 より前のオペレーティングシステムでは、パス長が 4096 文字を超えるディレクトリにあるファイルは駆除または削除されません。
- 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各タスクに対する CPU リソース使用量の制限が機能しません。
- Light Agent モードはサポートされていないため、アプリケーションのインストール時に KSVLA_MODE、SERVER_MODE、VDI_MODE の設定は適用されません。
- EDR エージェントモードでの本製品の動作はサポートされていません。
- 本製品は、Kaspersky Security Center Cloud コンソールではサポートされていません。
- 本製品は、FUSE テクノロジーに基づくファイルシステムをサポートしていません。
- 最も頻繁にスキャンされるファイルの統計情報は収集されません。
- 場合によっては、Kaspersky Endpoint Detection and Response (KATA) との連携の一環として送信されるテレメトリには、システムイベントログのイベントに関する情報が不完全な形で含まれることがあります。

CentOS 6.4 および 6.6

- ふるまい検知：プロセス起動の同期インターセプトを利用できないため、このコンポーネントが正しく動作することは保証されません。
- ウェブ脅威対策：IPv6 トラフィックのインターセプトが機能しません。
- ネットワーク脅威対策：IPv6 トラフィックのインターセプトが機能しません。
- アンチクリプター：IPv6 トラフィックのインターセプトが機能しません。
- 有害 USB 攻撃ブロック：オペレーティングシステムに systemd-logind サービスがないため、機能しません。
- コンテナスキャン：オペレーティングシステムがコンテナをサポートしていないため、機能しません。
- アプリケーションコントロール：プロセス開始の同期インターセプトに必要な fanotify テクノロジーがサポートされていないため、機能しません。
- Firewall 管理：Firewall の IPv6 ルールが機能しません。
- ウェブコントロール：IPv6 トラフィックのインターセプトが機能しません。
- 更新可能なカーネルモジュール：サポートされていません。
- オブジェクトの実行防止は、プロセス開始の同期インターセプトがないため、機能しません。
- Kaspersky Endpoint Detection and Response Optimum：TProxy がサポートされていないため、脅威の展開チェーンにネットワークアクティビティが表示されません。ファイル操作に関するテレメトリイベントのみを利用できます。オブジェクト実行防止は、プロセス開始の同期インターセプトを利用できないため、機能しません。
- Kaspersky Endpoint Detection and Response Expert（クラウド）との連携：機能しません。
- Kaspersky Endpoint Detection and Response (KATA) 連携：eBPF テレメトリソースを利用できません。
- Kaspersky Managed Detection and Response 連携：auditd テレメトリソースを利用できません。
- Kaspersky Security Center ネットワークエージェント：追加のデバイス設定が必要です。Kaspersky Security Center のヘルプを参照してください。
- インストール / 削除：このバージョンのオペレーティングシステムでは、このアプリケーションは SELinux と互換性がありません。考えられる解決策：SELinux を非ブロッキングモード（permissive モード）に設定する、SELinux を無効にする、または SELinux を手動で設定する。
- マルウェアのスキャン：glibc バージョン 2.11 より前のオペレーティングシステムでは、パス長が 4096 文字を超えるディレクトリにあるファイルは駆除または削除されません。
- Light Agent モードおよび EDR エージェントモードでの本製品の動作はサポートされていません。
- 本製品は、Kaspersky Security Center Cloud コンソールではサポートされていません。
- 最も頻繁にスキャンされるファイルの統計情報は収集されません。
- 場合によっては、Kaspersky Endpoint Detection and Response (KATA) との連携の一環として送信されるテレメトリには、システムイベントログのイベントに関する情報が不完全な形で含まれることがあります。

ptrace 設定値に関連する制限事項

オペレーティングシステムの `kernel.yama.ptrace_scope` 設定の値は、Kaspersky Endpoint Security に影響を与える可能性があります：

- 1（制限付き ptrace）。プロセスは、自身が開始したプロセスにのみ接続できます。他のプロセスに接続するには、特別な権限が必要です。アプリケーションの機能は次のように制限されます：
  - ふるまい検知コンポーネントは、プロセスの環境パラメータを取得できません。
  - カーネルバージョンが 5.7 より後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プロセスのコマンドライン引数および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。
  - /proc/<pid>/mem の読み取りが許可されていないため、プロセスメモリの YARA スキャンは保証されません。
- 2（管理者用 ptrace）。CAP_SYS_PTRACE 権限を持つプロセス（通常は root）のみが、ptrace を使用したり、/proc 内のプロセス（/proc/<pid>/mem）にアクセスしたりできます。トラブルシューティングには制限があり、kesl プロセス自体のダンプは機能しますが、ユーザープロセス（kesl-control や kesl-gui など）のクラッシュダンプは機能しません。
- 3（ptrace 禁止）：オペレーティングシステムレベルで ptrace が完全に禁止されています。アプリケーションの機能は次のように制限されます：
  - クラッシュダンプは、kesl プロセスまたはユーザープロセス（kesl-control や kesl-gui など）では機能しません。
  - ふるまい検知コンポーネントは、プロセスの環境パラメータを取得できません。
  - アプリケーションコントロールコンポーネントはサポートされていません。
  - /proc/<pid>/mem ディレクトリを読み取ることができないため：
    - スキャンタスクでは、プロセスメモリおよびカーネルメモリのスキャンが機能しません。
    - Detection and Response ソリューションと連携している場合、［メモリダンプの取得］タスクおよび［プロセスメモリダンプの取得］タスクは機能しません。
    - Kaspersky Endpoint Detection and Response Expert（オンプレミス）と連携している場合、強制アクセス制御モードでプロセスメモリの YARA スキャンが機能することは保証されません。

更新可能なカーネルモジュールの制限事項

更新可能なカーネルモジュールは、次の種類およびバージョンのカーネルをサポートしていません：

Ubuntu

- `*-kvm`
- `*-gkeop 5.15.0-100[1234] (bionic/jammy)`
- `focal 5.10.0-1002-oem`
- `noble 6.8.0-1014-ibm`
- `*-realtime`
- `*-uc-*`
- `kinetic 5.18.0-100(1|2)-(ibm|gcp|oracle)`

Astra

- `6.1.90-1-generic-*, 6.6.28-1-generic-*`
- `*-hardened`

Debian

- `*-rt`
- `5.14.0-1-(cloud-amd64|amd64)-5.14.6-2`
- `6.1.0-36-(cloud-amd64|amd64)-6.1.139-1`
- `6.5.0-5-*amd64-6.5.13-1`
- `6.6.*`

RED OS 7.3

- `kernel-ml-5.14.9-1.el7`

RED OS 8.0

- `6.6.26-1.red80`
- `6.6.34-1.red80`
- `6.6.51-1.red80`
- `6.6.76-1.red80`
- `6.6.6-1.red80`

eBPF 技術の使用に関する制限

ネットワークトラフィックの傍受に eBPF 技術を使用するには、次のオプションでコンパイルされた Linux カーネル 4.18 以降が必要です：

- `CONFIG_DEBUG_INFO_BTF=y` または `m`（BTF を使用した eBPF のサポート）
- `CONFIG_KPROBES= y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_FSNOTIFY=y`

Detection and Response ソリューションとの統合時に、テレメトリの送信に eBPF を使用するには、次のオプションでコンパイルされた Linux カーネル 4.18 以降が必要です：

- `CONFIG_BPF=y`
- `CONFIG_BPF_SYSCALL=y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_KPROBES=y`
- `CONFIG_KPROBES_ON_FTRACE=y`
- `CONFIG_KRETPROBES=y`
- `CONFIG_HAVE_SYSCALL_TRACEPOINTS=y`
- `CONFIG_FTRACE=y`
- `CONFIG_FUNCTION_TRACER=y`
- `CONFIG_DYNAMIC_FTRACE=y`
- `CONFIG_DYNAMIC_FTRACE_WITH_REGS=y`
- `CONFIG_FTRACE_SYSCALLS=y`
- `CONFIG_KPROBE_EVENTS=y`
- `CONFIG_FSNOTIFY=y`

特記事項

- 本製品では、Light Agent モードと EDR Agent モードを同時に使用することはできません。
- auditd 3.0.7 および Linux カーネル 4.18 を搭載したオペレーティングシステムでは、ふるまい検知コンポーネントを使用すると、アプリケーションおよび ssh 接続がフリーズする可能性があります。
- Kylin Desktop V10 SP1 2303 オペレーティングシステムでは、ふるまい検知コンポーネントによってオペレーティングシステムがフリーズする可能性があります。この問題を解決するには、オペレーティングシステムのカーネルをアップデートすることを推奨します。

Light Agent モードに関する特別な考慮事項

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。

EDR Agent モードに関する特記事項

Kaspersky Endpoint Security が EDR 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は限定されたサブセットのみです。インストール後の製品設定は次の通りです：

- Kaspersky Endpoint Detection and Response Expert（クラウド）との連携はサポートされていません。
- 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 EDR 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すが、保護対象デバイスには適用されません。

- 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）。次の設定は、保護対象デバイスには適用されません：

  - 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。

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の各バージョンのライフサイクル期間中に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ページを参照してください）。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では、カスペルスキーのアプリケーションを利用している組織が、メールによるリクエストを通じてカスペルスキーのテクニカルサポートに問い合わせることができます。このポータルでは、新規リクエストの作成、進捗状況の確認、リクエスト処理履歴の保存を行うことができます。

組織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単一のアカウントに登録します。これにより、カスペルスキーへの電子リクエストを一元管理し、ユーザーによるカスペルスキーカンパニーアカウントへのアクセスを制御できるようになります。

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、カスペルスキーカンパニーアカウントの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。

トレースファイルの作成を有効にして設定する方法

*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。コマンドライン、全般的なアプリケーション設定、またはグラフィカルユーザーインターフェイスで、トレースファイルの作成を有効または無効にしたり、トレースレベルを選択したりできます。

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。

Web コンソールでトレース設定を管理する方法

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**］を選択します。

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. ［**全般設定 → テクニカルサポート**］セクションに移動し、［**トレース設定**］の下を確認します。

5. 本製品のトレースファイルの既定の保存先ディレクトリを変更する場合は、**トレースフォルダーのパス**フィールドでトレースファイルを保存するディレクトリを指定します。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）。

6. 必要に応じて、**トレースファイルの最大サイズ（MB）**フィールドに本製品のトレースファイルの最大サイズ（メガバイト単位）を指定します。既定値：500

7. 必要に応じて、**トレースファイルの最大数**フィールドに本製品のトレースファイルの最大数を指定します。既定値：10

8. 変更内容を保存します。

9. トレース設定を適用するには、本製品を再起動します。

管理コンソールでトレース設定を管理する方法

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. ［**全般設定**］ → ［**アプリケーション設定**］セクションに移動します。

5. ［**トレースとダンプ設定**］で、［**設定**］をクリックします。

6. ［**トレースとダンプ設定**］ウィンドウが開きます。

7. 本製品のトレースファイルの既定の保存先ディレクトリを変更する場合は、**トレースファイルディレクトリのパス**フィールドでトレースファイルを保存するディレクトリを指定します。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）。

8. 必要に応じて、**トレースファイルの最大サイズ（MB）**フィールドに本製品のトレースファイルの最大サイズ（メガバイト単位）を指定します。既定値：500

9. 必要に応じて、**トレースファイルの最大数**フィールドに本製品で作成できるトレースファイルの最大数を指定します。既定値：10

10. ［**OK**］をクリックして、［**トレースとダンプ設定**］ウィンドウを閉じます。

11. ［**適用**］をクリックします。

12. トレース設定を適用するには、本製品を再起動します。

コマンドラインでトレースを有効にしてトレース設定を管理する方法

コマンドラインでは、全般的なアプリケーション設定の `TraceLevel`、`TraceFolder`、`TraceMaxFileCount`、`TraceMaxFileSize` 設定を使用して、トレースを設定できます。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。

コマンドラインでトレースファイルを作成し、トレース設定を行うには：

1. トレースファイルの作成を有効にし、トレースレベルを選択します：

   ```
   kesl-control --set-app-settings TraceLevel=Detailed | MediumDetailed | NotDetailed
   ```

   説明：

   - `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。

2. 本製品のトレースファイルの既定の保存先ディレクトリを変更する場合は、トレースファイルを保存するディレクトリを指定します：

   ```
   kesl-control --set-app-settings TraceFolder=<path to trace files directory>
   ```

   ここで、`<path to trace files directory>`はトレースファイルが保存されるディレクトリへのパスです。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）。

3. 必要に応じて、トレースファイルの最大数を指定します：

   ```
   kesl-control --set-app-settings TraceMaxFileCount=<number of application trace files>
   ```

   ここで、`<number of application trace files>`は本製品のトレースファイルの最大数です。指定可能な値：1 ～ 10000。既定値： 10。

4. 必要に応じて、本製品のトレースファイルの最大サイズ（メガバイト単位）を指定します：

```
kesl-control --set-app-settings TraceMaxFileSize=<size of an application trace file>
```

ここで、`<size of an application trace file>`はトレースファイルの最大サイズ（メガバイト単位）です。指定可能な値：1～1000。既定値： 500。

`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。

トレースファイルの作成を無効にするには、次のコマンドを実行します：

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

グラフィカルインターフェイスでトレースを有効にしてトレース設定を管理する方法

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。

1. アプリケーションの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：
   - **診断（300）** – エラーメッセージのみ。
   - **情報（700）** – 情報メッセージおよびエラーメッセージ。
   - **デバッグ（800）** – 詳細なトレースファイル。

   必要な詳細レベルについて、カスペルスキーのテクニカルサポートの担当者に確認することを推奨します。既定の設定は **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。

Watchdog サーバーのトレースファイルの作成を有効にして設定することもできます。

コマンドラインでトレースを有効にしてウォッチドッグサーバーのトレース設定を管理する方法

コマンドラインでは、アプリケーションの全般設定の WdTraceLevel 設定を使用して、ウォッチドッグサーバーのトレースを設定できます。コマンドラインオプション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用して、設定の値を変更できます。

コマンドラインからウォッチドッグサーバーのトレースファイルを作成してトレース設定を構成します

```
kesl-control --set-app-settings WdTraceLevel=Detailed | MediumDetailed | NotDetailed | Product
```

説明：

- 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。
- Product - アプリケーションの全般設定の TraceLevel 設定の値と同じ値を設定します。TraceLevel=None の場合、トレースファイルは生成されません。

コマンドラインからウォッチドッグサーバーのトレースファイルの作成を無効にしてトレース設定を構成します

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

既定で、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。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）。

グラフィカルインターフェイスおよび kesl-control コマンドラインユーティリティのトレースファイルは、/var/log/kaspersky/kesl-user ディレクトリに保存されます。これらのトレースファイルの作成を有効にするには、LFS_ENABLE_ALL_COMPONENTS_LOGGING 環境変数を設定する必要があります。

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、追加の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。

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 コンソールのアクティビティのログ記録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。

アプリケーショ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。

管理プラグインのトレースファイルの内容

管理プラグインの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

管理プラグインの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。

ダンプを有効にして設定する方法

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プ作成を有効または無効にできます。

Kaspersky Security Center を通じて Kaspersky Endpoint Security アプリケーションを管理している場合は、Web コンソールまたは管理コンソールを使用して、Kaspersky Endpoint Security のポリシー設定でダンプ作成を有効または無効にし、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する場合は、アプリケーションの全般設定でダンプ作成を有効または無効にできます。

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 コンソールでダンプ作成を有効化および設定する方法

Web コンソールでダンプ作成を有効化および設定するには：

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**］を選択します。

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. ［**全般設定 → テクニカルサポート**］セクションの［**デバッグ情報**］に移動します。

5. アプリケーションがクラッシュしたときにダンプファイルを生成する場合は、［**ダンプへの書き込みは有効です**］トグルスイッチをオンにします。

6. kesl プロセスのダンプファイルを既定で保存するディレクトリを変更する場合は、［**コードダンプのパス**］フィールドでダンプファイルを保存するディレクトリを指定します。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。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）。

7. 変更内容を保存します。

管理コンソールでダンプ作成を有効化および設定する方法

管理コンソールでダンプ作成を有効化および設定するには：

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. ［**全般設定**］ → ［**アプリケーション設定**］セクションに移動します。

5. ［**トレースとダンプ設定**］で、［**設定**］をクリックします。

6. ［**トレースとダンプ設定**］ウィンドウが開きます。

7. アプリケーションがクラッシュしたときにダンプファイルを生成する場合は、［**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する**］チェックボックスをオンにします。

8. kesl プロセスのダンプファイルを既定で保存するディレクトリを変更する場合は、［**ダンプファイルディレクトリへのパス**］フィールドでダンプファイルを保存するディレクトリを指定します。既定値：/var/opt/kaspersky/kesl/common/dumps。既定のダンプファイルディレクトリにアクセスするには、root 権限が必要です（`700` または `rwx--------` の権限）。別の ディレクトリを指定する場合は、root ユーザーのみが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持っていることを確認してください。

9. ［**OK**］をクリックして、［**トレースとダンプ設定**］ウィンドウを閉じます。

10. ［**適用**］をクリックします。

コマンドラインでダンプ作成を有効化および設定する方法

コマンドラインでは、アプリケーションの全般設定の `CoreDumps` および `CoreDumpsPath` 設定を使用して、ダンプ作成を有効化、無効化、および設定できます。

ダンプ作成を有効化および設定するには：

1. ダンプ作成を有効にするには、次のコマンドを実行します：

   ```
   kesl --set-app-settings CoreDumps=Yes
   ```

2. ダンプファイルの保存先ディレクトリを変更する場合は、`CoreDumpsPath` 設定でディレクトリへのパスを指定します。

   ```
   kesl --set-app-settings CoreDumpsPath=<path to directory with dump files>
   ```

   ここで、`<path to directory with dump files>` はダンプファイルが保存されるディレクトリへのパスです。既定値：/var/opt/kaspersky/kesl/common/dumps。既定のダンプファイルディレクトリにアクセスするには、root 権限が必要です（`700` または `rwx--------` の権限）。別の ディレクトリを指定する場合は、root ユーザーのみが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持っていることを確認してください。

ダンプ作成を無効化するには、次のコマンドを実行します：

```
kesl --set-app-settings CoreDumps=No
```

ダンプ作成を有効化している場合、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。

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：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：
- 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。

初期設定ファイル

アプリケーションの初期設定は、設定情報ファイルを使用して指定できます：

- Kaspersky Security Center を使用してアプリケーションをインストールする場合、アプリケーションのリモートインストール用アーカイブに autoinstall.ini 設定情報ファイルがあります。インストールパッケージを作成する前に、このファイルで設定を指定できます。Kaspersky Security Center は、アプリケーションのインストール時にこれらの設定を適用します。
- コマンドラインを使用してアプリケーションをインストールする場合は、設定情報ファイルを作成し、初期セットアップウィザードの開始時にそのファイルへのパスを指定する必要があります。このファイルの構造は、autoinstall.ini 設定情報ファイルからコピーできます。

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。autoinstall.ini ファイルには既定値が指定されています。

一部の設定で有効な値は、Kaspersky Security Center を介してリモートでインストールするか、コマンドラインでインストールするかによって異なります。

設定情報ファイルの設定を変更するには、その値を <setting name>=<value> 形式で指定します。

例

```
UPDATER_SOURCE=KLServers
```

設定	説明	値

[CustomSettings] セクション	リモートインストール中にアプリケーションを詳細に設定します。kesl.ini ファイル内の一部の設定と、トレースレベルを変更できます。
	
	このセクションを使用してアプリケーションを設定できるのは、初回インストール時のみです。
	
	`[CustomSettings]` セクションに autoinstall.ini ファイルの設定と重複する設定がある場合、autoinstall.ini の設定がアプリケーションに適用されます。
		• kesl.ini 設定情報ファイル内の任意の設定（<setting section>.<setting name>=<value> 形式）
		例
		`[CustomSettings]`
		`General.Locale=ru_RU.utf8`
		`Network.ProxyRouteTable=202`
		`Watchdog.MaxMemory=20MB`
		• `TraceLevel`：アプリケーションのトレースファイルの詳細レベル：
		  • `Detailed` – 詳細なアプリケーションの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アプリケーションの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アプリケーションのトレースファイルを生成します。
		  • `None`（既定値）– アプリケーションのトレースファイルを生成しません。
		• `WdTraceLevel`：Watchdog サーバーのトレースファイルの詳細レベル：
		  • `Detailed`：詳細な Watchdog サーバーの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 Watchdog サーバーの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 Watchdog サーバーのトレースファイルを生成します。
		  • `None`：Watchdog サーバーのトレースファイルを生成しません。
		  • `Product`（既定値）：値を `TraceLevel` の値と同じに設定します。

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。
LOCALE	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（米国） • `es_MX.UTF-8` – スペイン語（メキシコ） • `fr_FR.UTF-8` – フランス語 • `ja_JP.UTF-8` – 日本語 • `pt_BR.UTF-8` – ポルトガル語（ブラジル） • `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	autoinstall.ini 設定情報ファイル内：アプリケーション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。 コマンドラインの設定情報ファイルでは、アプリケーションにライセンスを追加するために、ライセンス情報ファイルへのパスも指定できます。 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。	`<activation code>`：Kaspersky Security Center またはコマンドラインでインストールする際に、アクティベーションコードを使用してアプリケーションをアクティベートする場合。 `<full path to key file>`：コマンドラインでのインストール中に、ライセンス情報ファイルを使用してアプリケーション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。

設定	説明	値
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。 このパラメータは、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` （既定） – 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します。 `<update source address>` ：ローカルディレクトリ（例：/home/bases）またはリモートの HTTP サーバーまたは HTTPS サーバー（例：http://example.com/bases/）として指定します。
PROXY_SERVER	インターネットへの接続に使用するプロキシサーバーのアドレス。 このパラメータは、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>://] <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>]@]<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。IPv6 アドレスを指定する場合は、角括弧で囲んで入力してください。 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。 このパラメータは、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	ファイル脅威対策の開始時にカーネルモジュールを自動的にコンパイルします。 この設定は、fanotify に対応していない OS にのみ適用されます。	`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。 このパラメータは、アプリケーションが標準モードまたは EDR エージェントモードで使用され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。

設定	説明	値
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`（既定） – 特権グループからユーザーを削除しません。
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。
ENDPOINT_AGENT_MODE	Kaspersky Endpoint Security の EDR Agent モードでの使用。 この設定は、Elbrus CPU を搭載したデバイスには適用されません。	`Yes` – Kaspersky Endpoint Security は、保護対象デバイス上のサードパーティ製アンチウイルスソリューションと連携する Kaspersky Detection and Response ソリューションをサポートするために、EDR エージェント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）。
EDR_EXPERT_CLOUD_MODE	Endpoint Detection and Response Expert コンポーネントのモードを選択します。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。 この設定は、Elbrus CPU を搭載したデバイスには適用されません。	`Yes` は、アプリケーションが Kaspersky Endpoint Detection and Response Expert（クラウド）統合を使用することを意味します。 `No`（既定値）は、アプリケーションが Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携を使用することを意味します。

設定	説明	値
KSVLA_MODE	Kaspersky Endpoint Security の Light Agent モードでの使用。 この設定は、Elbrus CPU を搭載したデバイスには適用されません。	`Yes` - Kaspersky Endpoint Security は 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 EDR エージェント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。 この設定は、Elbrus CPU を搭載したデバイスには適用されません。	`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。 この設定は、Elbrus CPU を搭載したデバイスには適用されません。	`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。
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。 この設定は、Elbrus CPU を搭載したデバイスには適用されません。	`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
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。 この設定は、Elbrus CPU を搭載したデバイスには適用されません。	`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、Kaspersky Security Center 経由でインストールする場合にのみ適用されます。 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。 この設定は、Elbrus CPU を搭載したデバイスには適用されません。	`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`（既定値）– アプリケーションの初回起動時にトレースファイルを作成しません。

設定	説明	値
AK_FORCED_PACKAGE_MANAGER_OPERATIONS_AS_FALLBACK	パッケージマネージャーのエラーを無視するアプリケーションインストールモードを使用します。 アプリケーションを通常どおりにインストールできなかった場合は、このモードを使用できます。 この設定は、Kaspersky Security Center 経由でインストールする場合にのみ適用されます。 既定値の変更は、テクニカルサポートの担当者の監督の下、その指示に従う場合にのみ推奨されます。	No（既定値）を指定すると、アプリケーションが通常どおりインストールされます。 Yes を指定すると、システムエラーを無視してアプリケーションがインストールされます。
AK_REMOVE_PARTIALLY_INSTALLED_PACKAGE	アプリケーションのインストールパッケージが部分的にしかインストールされなかった場合、そのパッケージを自動的に削除します。 アプリケーションを正常にインストールできなかった場合は、この設定を無効にしてください。 この設定は、Kaspersky Security Center 経由でインストールする場合にのみ適用されます。 既定値の変更は、テクニカルサポートの担当者の監督の下、その指示に従う場合にのみ推奨されます。	Yes（既定値）を指定すると、部分的にインストールされたアプリケーションのインストールパッケージが削除されます。 No を指定すると、部分的にインストールされたパッケージを無視してアプリケーションがインストールされます。
AK_PACKAGE_MANAGER_DEBUG_LOG_OUTPUT	パッケージマネージャーのデバッグログを有効にします。 この設定は、アプリケーションを正常にインストールできなかった場合に使用できます。 この設定は、Kaspersky Security Center 経由でインストールする場合にのみ適用されます。 既定値の変更は、テクニカルサポートの担当者の監督の下、その指示に従う場合にのみ推奨されます。	Yes を指定すると、パッケージマネージャーのデバッグログが有効になります。 No（既定値）を指定すると、パッケージマネージャーのデバッグログが有効になりません。

インストールパッケージでの初期設定

Kaspersky Security Center を使用してアプリケーションをインストールする際に使用するインストールパッケージで、アプリケーションの初期設定を指定できます。

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**］。

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。

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。

Web コンソールでの初期設定

初期設定

設定	説明
使用モード	• **ワークステーションとサーバーを保護する標準モード**（既定値）：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。 • **仮想環境保護用 Light Agent**このオプションを選択すると、アプリケーションは Light Agent モードで使用されます（Kaspersky Security for Virtualization Light Agent の一部として）。 Elbrus CPU を搭載したデバイスでは、EDR Agent モードと Light Agent モードは使用できません。
Endpoint Detection and Response Expert（クラウド）を有効にする	Endpoint Detection and Response Expert（クラウド）との連携を使用するには、このチェックボックスをオンにします。 標準モードでは、アプリケーションは Endpoint Detection and Response Expert（クラウド）および Endpoint Detection and Response Expert（オンプレミス）との連携をサポートしています。このチェックボックスをオフにすると、Endpoint Detection and Response Expert（オンプレミス）との連携が使用されます。 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 この設定は、Elbrus CPUを搭載したデバイスには適用されません。

設定	説明
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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。
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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。
KSC のイベントの言語	Kaspersky Security Center に送信されるアプリケーションイベントのローカライズ言語： • **システム**（既定）を選択すると、OS のロケールが使用されます。 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、イベントの言語化に英語が使用されます。 • Kaspersky Endpoint Security がサポートする言語のいずれか：英語（米国）、スペイン語（メキシコ）、繁体字中国語、簡体字中国語、ドイツ語、ポルトガル語（ブラジル）、ロシア語、フランス語、日本語。 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。 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ソースをアップデートします。 • **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。 このパラメータは、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。 インストールパッケージに事前にダウンロードしたアプリケーションの定義データベースを追加している場合は、このチェックボックスをオフにします。 このパラメータは、アプリケーションが標準モードまたは EDR Agent モードで使用される場合にのみ適用されます。

設定	説明
プロキシサーバー設定を指定する	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>://]<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>]@]<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。IPv6 アドレスを指定する場合は、角括弧で囲んで入力してください。 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。 このパラメータは、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。 この設定は、fanotify に対応していない OS にのみ適用されます。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。
グラフィカルユーザーインターフェースを使用	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。 このパラメータは、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、アプリケーションの初期設定時に、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。
インストール後の製品の初回起動時に保護機能とスキャンタスクを無効にする	インストールプロセスの完了後、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。
インストール後の製品の初回起動時にトレースを有効にする	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
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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。
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	更新可能なカーネルモジュールの起動に失敗した場合にアプリケーションが実行する処理： • **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。 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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。
パッケージマネージャーのエラー無視モードを有効にする	アプリケーションのインストール時にパッケージマネージャーのエラーを無視するには、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。 この設定は、アプリケーションを正常にインストールできなかった場合に使用できます。 この設定は、テクニカルサポートからの指示がある場合にのみ有効にすることを推奨します。

管理コンソールでの初期設定

初期設定

設定	説明
KSC のイベントの言語	Kaspersky Security Center に送信されるアプリケーションイベントのローカライズ言語： • **システム**（既定）を選択すると、OS のロケールが使用されます。 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、イベントの言語化に英語が使用されます。 • Kaspersky Endpoint Security がサポートする言語のいずれか：英語（米国）、スペイン語（メキシコ）、繁体字中国語、簡体字中国語、ドイツ語、ポルトガル語（ブラジル）、ロシア語、フランス語、日本語。 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。

設定	説明
アクティベーションコード	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、アクティベーションコードを入力します。 この設定は、アプリケーションが標準モードで使用される場合にのみ適用されます。
アップデート元を選択してください	［**設定**］をクリックすると、定義データベースと機能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**（既定値）： • 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。 このパラメータは、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。 インストールパッケージに事前にダウンロードしたアプリケーションの定義データベースを追加している場合は、このチェックボックスをオフにします。 このパラメータは、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>://]<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>]@]<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。IPv6 アドレスを指定する場合は、角括弧で囲んで入力してください。 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。 このパラメータは、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。 この設定は、fanotify に対応していない OS にのみ適用されます。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。
グラフィカルユーザーインターフェースを使用	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。 このパラメータは、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の名前。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。

設定	説明
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、アプリケーションの初期設定時に、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。
アプリケーションをインストール後初めて起動する際に、保護機能とスキャンタスクを無効にする	インストールプロセスの完了後、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、アプリケーションの初回起動時にトレースを有効にする	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**ボタンが含まれています。このボタンをクリックすると、［**アプリケーションモード**］ウィンドウが表示されます。このウィンドウでは、アプリケーションの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**（既定値）：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。 • **仮想環境保護用 Light Agent**このオプションを選択すると、アプリケーションは Light Agent モードで使用されます（Kaspersky Security for Virtualization Light Agent の一部として）。 Elbrus CPU を搭載したデバイスでは、EDR Agent モードと Light Agent モードは使用できません。
Endpoint Detection and Response Expert（クラウド）を有効にしてください	Endpoint Detection and Response Expert（クラウド）との連携を使用するには、このチェックボックスをオンにします。 標準モードでは、アプリケーションは Endpoint Detection and Response Expert（クラウド）および Endpoint Detection and Response Expert（オンプレミス）との連携をサポートしています。このチェックボックスをオフにすると、Endpoint Detection and Response Expert（オンプレミス）との連携が使用されます。 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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。
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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。

設定	説明
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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。
システムイベントインターセプター	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、［**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、アプリケーション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 技術**（既定値）：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。 • **更新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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。
更新可能なカーネルモジュールが開始できなかった場合 （［**システムイベントインターセプターの設定**］ウィンドウ）。	更新可能なカーネルモジュールの起動に失敗した場合にアプリケーションが実行する処理： • **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。 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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。
パッケージマネージャーのエラー無視モードを有効にする	アプリケーションのインストール時にパッケージマネージャーのエラーを無視するには、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。 この設定は、アプリケーションを正常にインストールできなかった場合に使用できます。 この設定は、テクニカルサポートからの指示がある場合にのみ有効にすることを推奨します。

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、kesl.ini 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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	`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。
`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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	`true/yes` 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。 `false/no` – 本製品は標準モードで使用されます。

設定	説明	値
EndpointAgentMode	Kaspersky Endpoint Security の EDR Agent モードでの使用。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	true/yes は、本製品が EDR Agent モードで使用されていることを意味します。 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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	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 のいずれかのモード（標準モード、EDR Agent モード、または Light Agent モード）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。
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	本製品の RAM 使用量の上限（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：4047
`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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	既定値：3
`SafeMode`	更新可能なカーネルモジュールを使用する場合の「セーフ」モードの有効化。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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	`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。

設定	説明	値
`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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	`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。
`UseIncreasedXdrEventsCache`	Detection and Response ソリューションと連携する場合のイベントキャッシュの管理。高パフォーマンスと RAM 使用量の間にはトレードオフがあります。	`true/yes`（既定値）は、ディスク I/O を最小限に抑えますが、より多くの RAM（100 MB）を使用します。 `false/no` は、ディスクの読み取りおよび書き込み操作が増える代わりに、使用するメモリが少なくなります（約 5 MB）。
`FastShutdown`	本製品が停止または再起動されたときの kesl プロセスの高速シャットダウン。	`true/yes` は、本製品が停止されたときに kesl プロセスの高速シャットダウンを有効にします。 `false/no`（既定値）は、本製品が停止されたときに kesl プロセスの高速シャットダウンを無効にします。
[Network] セクションには、次の設定が含まれています：		
`WtpFwMark`	ウェブ脅威対策コンポーネントによる処理のために本製品に転送されるトラフィックの iptables ルール内のマーク。 本製品がインストールされたデバイスで、TCP パケットマスクの 9 番目のビットを使用する他のソフトウェアが実行され、競合が発生した場合は、このマークを変更する必要があります。	10 進数の値または先頭に 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）。

設定	説明	値
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	スキャン時に本製品が無視するパケットのマーク。	10 進数の値または先頭に 0x が付いた 16 進数。
		既定値：0x800。
		例：
		指定したデバイスとのすべての TCP トラフィックを無視します：
		`iptables -t mangle -A PREROUTING -s <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`
		`iptables -t mangle -A OUTPUT -d <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`
		HTTPS サーバーのトラフィックを無視します：
		`iptables -t mangle -A PREROUTING -p tcp -m tcp --dport 443 -j MARK --set-xmark 0x800/0x800`
		`iptables -t mangle -A OUTPUT -p tcp -m tcp --sport 443 -j MARK --set-xmark 0x800/0x800`
		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。
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：		

設定	説明	値
ServerMode	Kaspersky Endpoint Security が Light Agent モードで使用される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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	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	本製品を Light Agent モードで使用する場合に 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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	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。 <value>% – RAM の 1 ～ 100 パーセントの値。 <value>MB – メガバイト単位の値。 lowest/<value>%/<value>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/<value>%/<value>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。 <value>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。 <value>% – RAM の 0 ～ 100 パーセントの値。 <value>MB – メガバイト単位の値。 lowest/<value>%/<value>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/<value>%/<value>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。
`TimeoutMaxCleanPeriod`	オペレーティングシステムの Firewall ルールをクリアするプロセスに割り当てられる最大時間。プロセスがこの時間内に完了を通知しない場合、Watchdog サーバーはプロセスがフリーズしているとみなします。	既定値：10 秒。
`TimeoutAfterClean`	Watchdog サーバーがクリーンアッププロセスに SIGTERM シグナルを送信した後、オペレーティングシステムの Firewall ルールをクリアするプロセスが終了するまでに割り当てられる最大時間。	既定値：10 秒。
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`	コンテナ監視コンポーネントを実行するときに、containerd 環境のサポートを有効にします。 既定では、このセクションは設定情報ファイルに存在しません。コンテナ監視コンポーネントの実行中に containerd 環境を使用する場合は、設定情報ファイルとその中に `[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。 この設定は、Elbrus CPUを搭載したデバイスには適用されません。	`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

QueueScanTasks=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

QueueScanTasks=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

QueueScanTasks=No

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

QueueScanTasks=No
```

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

ProhibitBarcodeScanner=Yes
```

KATANDR タスク（ID:31）の既定

```
ConnectionTimeout=10

RequestTimeout=10

SynchronizationPeriod=5

UseTunnel=No

TunnelAddress=127.0.0.1

TunnelPort=443

[Endpoints.item_0000]

Address=127.0.0.1
```

```
Port=443
EnableTelemetry=Yes
[TelemetrySettings]

ConnectionTimeout=10
RequestTimeout=10
OnlyTaggedEvents=No
UseTunnel=No
TunnelAddress=127.0.0.1
TunnelPort=443
[TelemetrySettings.Endpoints.item_0000]

Address=127.0.0.1
Port=443
[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30
UseRequestCountLimits=Yes
MaximumNumberOfEventsInHour=3000
EventLimitExceededPercentage=15
MaximumNumberOfEventsInPackage=1024
```

補足資料 2：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 3：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。

補足資料 4：リムーバブルドライブの簡易スキャンのファイル拡張子

com – アプリケーションの実行ファイル（64 KB 以下）

exe – 実行ファイルまたは自己解凍型アーカイブ

sys – Microsoft Windows システムファイル

prg – dBase™、Clipper または Microsoft Visual FoxPro® のプログラムテキスト、または WAVmaker プログラム

bin – バイナリファイル

bat – バッチファイル

cmd – Microsoft Windows NT（DOS のバッチファイルに類似）、OS/2 のコマンドファイル

dpl – Borland Delphi の圧縮ライブラリ

dll – ダイナミックリンクライブラリ

scr – Microsoft Windows スプラッシュスクリーン

cpl – Microsoft Windows コントロールパネルモジュール

ocx – Microsoft OLE（オブジェクトのリンクと埋め込み）オブジェクト

tsp – スプリットタイムモードで実行されているプログラム

drv – デバイスドライバー

vxd – Microsoft Windows 仮想デバイスドライバー

pif – プログラム情報ファイル

lnk – Microsoft Windows リンクファイル

reg – Microsoft Windows システムレジストリキーファイル

ini – Microsoft Windows、Windows NT、および一部のアプリケーションの構成データを含む設定ファイル

cla – Java クラス

vbs – Visual Basic® スクリプト

vbe – BIOS Video Extension

js、jse – JavaScript ソーステキスト

htm – ハイパーテキストドキュメント

htt – Microsoft Windows ハイパーテキストヘッダー

hta – Microsoft Internet Explorer® のハイパーテキストプログラム

asp – Active Server Pages スクリプト

chm – コンパイル済み HTML ファイル

pht – 統合 PHP スクリプトを含む HTML ファイル

php – HTML ファイルに組み込まれたスクリプト

wsh – Microsoft Windows スクリプトホストファイル

wsf – Microsoft Windows スクリプト

the – Microsoft Windows 95 デスクトップ壁紙ファイル

hlp – Windows ヘルプファイル

msg – Microsoft Mail メール

plg – メール

mbx – 保存されている Microsoft Office Outlook メールメッセージ

doc* – Microsoft Office Word ドキュメント（doc – Microsoft Office Word ドキュメント、docx – XML のサポートを含む Microsoft Office Word 2007 ドキュメント、docm – マクロのサポートを含む Microsoft Office Word 2007 ドキュメント）

dot* – Microsoft Office Word ドキュメントテンプレート（dot – Microsoft Office Word ドキュメントテンプレート、dotx – Microsoft Office Word 2007 ドキュメントテンプレート、dotm – マクロのサポートを含む Microsoft Office Word 2007 ドキュメントテンプレート）

fpm – データベースプログラム、Microsoft Visual FoxPro 開始ファイル

rtf – リッチテキストフォーマットドキュメント

shs – Shell Scrap Object Handler フラグメント

dwg – AutoCAD® 図面データベース

msi – Microsoft Windows インストールパッケージ

otm – Microsoft Office Outlook 用 VBA プロジェクト

pdf – Adobe Acrobat ドキュメント

swf – Shockwave® Flash パッケージオブジェクト

jpg、jpeg – 圧縮イメージグラフィック形式

emf – Enhanced Metafile 形式のファイル

ico – オブジェクトアイコンファイル

ov? – Microsoft Office Word 実行ファイル

xl* – Microsoft Office Excel ドキュメントおよびファイル（xla – Microsoft Office Excel の拡張子、xlc – ダイアグラム、xlt – ドキュメントテンプレート、xlsx – Microsoft Office Excel 2007 ブック、xltm – マクロのサポートを含む Microsoft Office Excel 2007 ブック、xlsb – バイナリ（非 XML）形式の Microsoft Office Excel 2007 ブック、xltx – Microsoft Office Excel 2007 テンプレート、xlsm – マクロのサポートを含む Microsoft Office Excel 2007 テンプレート、xlam – マクロのサポートを含む Microsoft Office Excel 2007 プラグイン）

pp* – Microsoft Office PowerPoint® ドキュメントおよびファイル（pps – Microsoft Office PowerPoint スライド、ppt – プレゼンテーション、pptx – Microsoft Office PowerPoint 2007 プレゼンテーション、pptm – マクロのサポートを含む Microsoft Office PowerPoint 2007 プレゼンテーション、potx – Microsoft Office PowerPoint 2007 プレゼンテーションテンプレート、potm – マクロのサポートを含む Microsoft Office PowerPoint 2007 プレゼンテーションテンプレート、ppsx – Microsoft Office PowerPoint 2007 スライドショー、ppsm – マクロのサポートを含む Microsoft Office PowerPoint 2007 スライドショー、ppam – マクロのサポートを含む Microsoft Office PowerPoint 2007 プラグイン）

md* – Microsoft Office Access® ドキュメントおよびファイル（mda – Microsoft Office Access ワークグループ、mdb – データベース）

sldx – Microsoft PowerPoint 2007 スライド

sldm – マクロのサポートを含む Microsoft PowerPoint 2007 スライド

thmx – Microsoft Office 2007 テーマ

補足資料 5：メッセージテンプレートの変数

デバイスコントロールコンポーネントとウェブコントロールコンポーネントを使用すると、ブロックされたデバイス、アプリケーション、またはリソースにアクセスしようとしているユーザーや、潜在的に危険な操作を実行しようとしているユーザーに対して Kaspersky Endpoint Security が表示するメッセージのテンプレートを設定できます。

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。Kaspersky Endpoint Security は、メッセージを生成する際に、オペレーティングシステムの設定から変数の値を取得し、特定のコンピューター、ユーザー、およびイベントに一致するメッセージに挿入します。

デバイスコントロールのメッセージテンプレートの変数

ユーザーメッセージテンプレートまたは管理者メッセージテンプレートでは、次の変数を使用できます。

- **ユーザー**：`%USER_NAME%`

  メッセージが生成されたコンピュータ上の現在のユーザーアカウントの名前。形式：`<device name>\<user alias>`（例： `DESKTOP-123\John.Smith`）。

- **コンピューター名**：`%COMPUTER_NAME%`

  デバイスがブロックされたコンピューターの名前。

- **ルール名**：`%RULE%`

  デバイスをブロックしたルールの名前。

- **ルールの適用日**：`%DATE%`

  デバイスがブロックされた日付（形式：DD.MM.YYYY）。

- **ルールの適用時刻**：`%TIME%`

  デバイスがブロックされた時刻（形式：HH:MM）。

- **デバイス名**：`%DEVICE_NAME%`

  ブロックされたデバイスの名前。

- **デバイス種別**：`%DEVICE_TYPE%`

  ブロックされたデバイスの種別（プリンター、リムーバブルドライブ、CD/DVD ドライブなど）。

- **デバイスモデル**：`%DEVICE_VIDPID%`

  ブロックされたデバイスのモデル（例：VID_1234&PID_5678）。

- **デバイス ID**：`%DEVICE_ID%`

  ブロックされたデバイスの ID（例：`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`）。

- **デバイス操作**：`%OPERATION%`

  デバイスでの禁止操作の種別。

ウェブコントロールのメッセージテンプレートの変数

ユーザーメッセージテンプレートまたは管理者メッセージテンプレートでは、次の変数を使用できます。

- **ユーザー**：%USER_NAME%

  メッセージが生成されたコンピュータ上の現在のユーザーアカウントの名前。形式：<device name>\<user alias>（例： DESKTOP-123\John.Smith）。

- **Web リソースアドレス**：%CANONIC_REQUEST_URL%

  ブロックされた Web リソースのアドレス。

- **ルール名**：%RULE%

  Web リソースをブロックしたルールの名前。

- **メッセージを送信するメール**：%COMPLAIN_EMAIL%

  Web リソースのブロックに関する連絡用のメールアドレス。メールアドレスをクリックすると、ユーザーが管理者にメッセージを書き込むことができるウィンドウが開きます。

- **コンテンツカテゴリ名**：%CONTENT_CATEGORY_LIST%

  ブロックされたリソースが属する Web サイトのカテゴリ（例：*決済システム*）。

- **データ種別カテゴリ名**：%TYPE_CATEGORY_LIST%

  ブロックされた Web リソース上のデータ種別のカテゴリ（例：*グラフィックファイル*）。

- **要求された Web リソースへのリンク**：%CONTINUE_PAGE%

  要求された Web ページへのリンク（例：http://www.example.com/pagename.html）。

- **Web サイトへのリンク**：%CONTINUE_SITE%

  要求された Web ページを含む Web サイトへのリンク（例：http://www.example.com/）。

- **ドメインへのアクセス用リンク**：%CONTINUE_DOMAIN%

  クリックしてドメイン名の既存のすべての Web ページにアクセスできるリンク。たとえば、ブロックされた Web ページのアドレスが http://www.example.com だった場合、変数 %CONTINUE_DOMAIN% は http://*.example.com リンクに置換されます。このリンクをクリックすると、基本ドメイン名 http://www.example.com/ のすべての Web アドレス（サブドメインを含む）にアクセスできます。例えば、http://start.example.com/* や http://domain.domain.example.com/* などです。ここで、文字「*」は任意の文字列（空白の文字列を含む）を表します。

補足資料 6：アプリケーションイベント

Kaspersky Security Center イベントログおよびオペレーティングシステムのイベントログ（syslog）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、各マルウェアのスキャンタスク、アップデートタスクおよび整合性チェックタスクの完了状況、ならびに製品全体の動作に関する情報が記録されます。

緊急

システム整合性違反

ステータス	!
コンポーネント	システム変更監視
LinuxイベントID	0
Kaspersky Security Center イベント ID	GNRL_EV_FIM_ALARM
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションの起動が拒否されました

ステータス	!
コンポーネント	アプリケーションコントロール
LinuxイベントID	122
Kaspersky Security Center イベント ID	GNRL_EV_APPLICATION_LAUNCH_DENIED
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

悪意のあるオブジェクトが検知されました（ローカル定義データベース）

ステータス	!
コンポーネント	ファイル脅威対策 メール脅威対策 ふるまい検知 脆弱性攻撃ブロック Sandbox
LinuxイベントID	6
Kaspersky Security Center イベント ID	GNRL_EV_VIRUS_FOUND
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

システム変更監視イベントの上限を超過しました

ステータス	!
コンポーネント	システム変更監視
LinuxイベントID	70
Kaspersky Security Center イベント ID	GNRL_EV_FIM_ALARM_OVERFLOW
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

デバイスの操作が禁止されています

ステータス	!
コンポーネント	デバイスコントロール
LinuxイベントID	94
Kaspersky Security Center イベント ID	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

ネットワーク攻撃が検知されました

ステータス	ⓘ
コンポーネント	ネットワーク脅威対策
LinuxイベントID	102
Kaspersky Security Center イベント ID	`GNRL_EV_ATTACK_DETECTED`
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アクセスが拒否されました（ローカル定義データベース）

ステータス	ⓘ
コンポーネント	ウェブコントロール
LinuxイベントID	190
Kaspersky Security Center イベント ID	`GNRL_EV_WEB_URL_BLOCKED`
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

警告

駆除できません

ステータス	⚠
コンポーネント	ファイル脅威対策 メール脅威対策
LinuxイベントID	10
Kaspersky Security Center イベント ID	`GNRL_EV_OBJECT_NOTCURED`
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

望ましくないコンテンツに関する警告（ローカルデータベース）

ステータス	⚠
コンポーネント	ウェブコントロール
LinuxイベントID	192
Kaspersky Security Center イベント ID	`GNRL_EV_WEB_URL_WARNING`
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

Web ページへのアクセスのブロックに関する管理者へのメッセージ

ステータス	⚠
コンポーネント	ウェブコントロール
LinuxイベントID	196

Kaspersky Security Center イベント ID	GNRL_EV_WC_USER_REQUEST
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

情報メッセージ

オブジェクトが駆除されました

ステータス	ⓘ
コンポーネント	ファイル脅威対策 メール脅威対策
LinuxイベントID	9
Kaspersky Security Center イベント ID	GNRL_EV_OBJECT_CURED
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

オブジェクトが削除されました

ステータス	ⓘ
コンポーネント	ファイル脅威対策 メール脅威対策
LinuxイベントID	8
Kaspersky Security Center イベント ID	GNRL_EV_OBJECT_DELETED
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

アプリケーションの起動が許可されました

ステータス	ⓘ
コンポーネント	アプリケーションコントロール
LinuxイベントID	120
Kaspersky Security Center イベント ID	GNRL_EV_APPLICATION_LAUNCHED
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ	設定されていません

テストモードでアプリケーションの起動が許可されました

ステータス	ⓘ
コンポーネント	アプリケーションコントロール
LinuxイベントID	121
Kaspersky Security Center イベント ID	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

テストモードでアプリケーションの起動が拒否されました

ステータス	ⓘ
コンポーネント	アプリケーションコントロール
LinuxイベントID	123
Kaspersky Security Center イベント ID	GNRL_EV_APP_LAUNCH_TESTED_DENIED
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

デバイスが接続されました

ステータス	ⓘ
コンポーネント	デバイスコントロール
LinuxイベントID	90
Kaspersky Security Center イベント ID	GNRL_EV_DEVCTRL_DEV_PLUGGED
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

デバイスが切断されました

ステータス	ⓘ
コンポーネント	デバイスコントロール
LinuxイベントID	91
Kaspersky Security Center イベント ID	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
ログ（syslog）（既定）	–
Kaspersky Security Center イベントログ（既定）	✓

補足資料 7：リターンコード

初期セットアップウィザードのリターンコード

0 – インストールが正常に完了しました。

重大なエラー

1 – 不明なエラー（以下に示すエラーを除くその他すべての重大なエラー。例：システムエラー、メモリ不足、ファイルを開く際のエラーなど）。

2 – 初期設定情報ファイルに無効なパラメータが含まれています。

3 – アプリケーションのインストールまたはアップデートに失敗しました。

4 – アプリケーションを削除できません。

5 – アプリケーションを起動できません。考えられる原因：アクセス権限が正しく設定されていません。次のディレクトリへの書き込み権限が root アカウントのみに付与されていることを確認してください：/、/opt、/opt/kaspersky、/var、/var/opt、/var/opt/kaspersky、/usr、/usr/lib64。

6 – インストール前に必要な処理が実行されていません。

7 – アプリケーションのアップデートに失敗しました。以前のバージョンのアプリケーションのインストールはサポートされていません。

8 – 特権グループからのユーザーの削除に失敗しました。

9 – アプリケーションのインストール用に一意の MachineID を作成できませんでした。

10 – アプリケーションの起動または再起動に失敗しました。

11 – 使用許諾契約書（EULA）およびプライバシーポリシーの条項に同意していません。

12 – アプリケーションでは、Light Agent モードと EDR Agent モードを同時に使用することはできません。

13 – Astra Linux のクローズドソフトウェア環境モード用の astra-digsig-oldkeys パッケージが見つかりませんでした。

14 – 初期設定は既に開始されています。

15 – Kaspersky Security for Virtualization 5.2 Light Agent ソリューションの一部としてインストールされている Light Agent for Linux コンポーネントを削除する必要があります。

16 – 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。

17 – アプリケーションプロセスが既に実行されているため、初期セットアップウィザードを開始できませんでした。

18 – fanotify はサポートされていません。ファイル脅威対策用のカーネルモジュールのコンパイルに失敗しました。

19 – インストールには管理者権限が必要です。

20 – アプリケーションサービスが開始されていません。

21 – アプリケーションのアップデートがロールバックされました。

22 – EDR Agent モードまたは Light Agent モードのアプリケーションを、カスペルスキー Endpoint Detection and Response Expert（クラウド）と統合することはサポートされていません。

警告

71 – インストール中に複数の警告が発生しました。詳細は、インストールログを参照してください。

72 – 製品データベースのアップデートに失敗しました。

75 – オペレーティングシステムの再起動が必要です。

76 – KSN 設定の適用に失敗したか、KSN 声明の条項に同意していません。

77 – 更新可能なカーネルモジュールの起動に失敗しました。

79 – アプリケーションのグラフィカルインターフェイスパッケージのインストールまたはアップデートに失敗しました。

80 – 製品データベースのダウンロードに失敗しました。

81 – ネットワーク の 問題により、アプリケーションのアクティベーションが エラー で終了しました。

82 – アプリケーションはポリシーによって管理されます。

83 – アプリケーションの GUI が起動しませんでした。

84 – 管理者ロールの割り当てに失敗しました。指定されたユーザーが見つかりません。

85 – アプリケーションパッケージは、パッケージマネージャーのエラー無視モードでのみインストールまたはアップデートできました。

86 – アプリケーションのグラフィカルインターフェイスパッケージの削除に失敗しました。

87 – アプリケーションパッケージは、パッケージマネージャーのエラー無視モードでのみ削除できました。

88 – ユーザーへの管理者ロールの割り当てに失敗しました。

89 – 無効なライセンスです。

90 – アップデートタスクのスケジュールの設定に失敗しました。

kesl-control コマンドラインユーティリティの戻りコード

0 – コマンド / タスクが正常に完了しました。

1 – コマンド構文の一般エラーです。

2 – 渡された製品設定のエラー。

64 – Kaspersky Endpoint Security が動作していません。

66 – 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 問題により、アプリケーションのアクティベーションが エラー で終了しました。

68 – アプリケーションがポリシーによって管理されているため、コマンドを実行できません。

69 – アプリケーションは Amazon Paid Ami インフラストラクチャに配置されています。

70 – すでに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変更、停止中のタスクの停止、中断中のタスクの一時停止、または実行中のタスクの再開が試行されました。

71 – Kaspersky Security Network に関する声明に同意しませんでした。

72 – オブジェクトスキャンタスクまたはカスタムコンテナスキャンタスクの実行中に脅威が検知されました。

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 – Kaspersky Endpoint Security は、アップデート後に再起動する必要があります。

75 – デバイスを再起動する必要があります。

76 – root 権限を持つユーザーのみが指定されたパスに対する書き込みアクセス権を持つ必要があるため、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 – アプリケーションが Light Agent モードで使用されているため、コマンドまたはタスクを実行できません。

79 – 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ません。

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。

81 – コンポーネントは、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バージョンではサポートされていません。

128 – 不明なエラーです。

65 - その他のすべてのエラー。

補足資料 8：製品データベースを含むアーカイブの準備

Kaspersky Endpoint Security のインストールパッケージを手動で作成する場合、以前にダウンロードした製品データベースをパッケージに追加できます。統合データベースを含むインストールパッケージを使用している場合、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。

インストールパッケージに製品データベースを追加すると、パッケージのサイズが大きくなります。

保護対象デバイスのオペレーティングシステムのアーキテクチャとビット数の組み合わせごとに、個別の製品データベースのセットが必要です。インストールパッケージには、1 つまたは複数の製品データベースのセットを含むアーカイブを追加できます。製品データベースの各セットを準備するには、アーキテクチャとビット数が一致するオペレーティングシステムを搭載したデバイスに、Kaspersky Endpoint Security がすでにインストールされている必要があります。

データベースを含むアーカイブを準備するには：

1. Kaspersky Security Center を使用してまたはコマンドラインを使用して、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. デバイスの製品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* タスクを実行するか、Kaspersky Security Center で *Update* タスクを実行します。

3. 保護対象デバイスのオペレーティングシステムのアーキテクチャとビット数に応じて、データベース用のディレクトリを作成します：

   - x86_64：製品が 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場合
   - i386：製品が 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場合
   - arm64：製品が 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されている場合
   - e2k：製品が Elbrus 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されている場合

4. /var/opt/kaspersky/kesl/private/updates ディレクトリの内容を、作成したデータベース用ディレクトリにコピーします。

5. 作成したデータベース用ディレクトリを kesl-bases.tgz アーカイブに追加します。

   アーキテクチャとビット数が異なる複数のオペレーティングシステムにインストールするためのインストールパッケージを作成する場合は、データベースを含む複数のディレクトリを準備し、それらをすべて kesl-bases.tgz アーカイブに追加する必要があります。

Kaspersky Endpoint Security のインストール後、既定では、定義データベースのアップデートタスクが開始されます。データベースが組み込まれたインストールパッケージから製品をインストールする場合は、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。この設定は、作成したインストールパッケージのプロパティ、またはautoinstall.ini 設定情報ファイル（`UPDATE_EXECUTE=No`）で指定できます。

補足資料 9：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。

法律上の通知

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され、カスペルスキーに送信される情報の処理、保存、破棄に関する詳細は、使用許諾契約書、Kaspersky Security Network に関する声明、およびカスペルスキーの Web サイトに掲載されているプライバシーポリシーをお読みください。license.<言語 ID> ファイルと ksn_license.<言語 ID> ファイルには使用許諾契約書と Kaspersky Security Network に関する声明が記載されており、製品の配布パッケージに組み込まれています。

アクティベーションコードを使用する時に提供されるデータ

アクティベーションコードを使用して標準モードまたは EDR 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 EDR 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向上させ、アプリケーションの配布と使用状況に関する統計情報を提供するために、以下の情報をカスペルスキーに自動的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 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 を標準モードまたは Endpoint Detection and Response Agent モードで使用し、かつ Kaspersky Security Network を拡張モードで使用する場合、Kaspersky Security Network に関する声明の条項に同意することにより、上記の情報に加え、次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こととなります：

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）コンポーネントとの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、個人情報や機密データを含む可能性がある次の情報を保存します：

- 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）との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、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。
- Kaspersky Endpoint Detection and Response Expert（オンプレミス）との連携用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）と連携している場合、本製品は次のデータを保存し、連携サーバーに送信できます：

- EDR Expert（オンプレミス）コンポーネントへの同期リクエストに関する情報：
  - 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
- タスク実行レポート内の EDR Expert（オンプレミス）コンポーネントへのリクエストから取得された情報：
  - 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。
    - カスペルスキー 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

- ネットワーク接続の確立と終了に関する情報：
  - 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
  - 接続確立時刻
  - 接続終了時刻
  - 接続時間
  - 接続中に送信されたバイト数
  - 接続中に受信されたバイト数
- 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 Endpoint Detection and Response Expert（クラウド）コンポーネントとの連携時に提供されるデータ

Kaspersky Endpoint Security を Kaspersky Endpoint Detection and Response Expert（クラウド）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（クラウド）と連携するためのサーバーのリスト。
- Kaspersky Endpoint Detection and Response Expert（クラウド）のテレメトリおよびレスポンスサーバートンネルのアドレス。
- Kaspersky Endpoint Detection and Response Expert（クラウド）と連携するためのサーバー証明書。
- Kaspersky Endpoint Detection and Response Expert（クラウド）と連携するためのクライアント証明書。
- Kaspersky Endpoint Detection and Response Expert（クラウド）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（クラウド）との連携を処理するサーバーへの接続ステータス、クライアント証明書およびサーバー証明書のエラーに関する情報。
- Kaspersky Endpoint Detection and Response Expert（クラウド）と連携するため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（クラウド）と連携されている場合、本製品は次のデータを保存し、Integration Server に送信できます：

- EDR Expert（クラウド）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
- タスク実行レポートに含まれる EDR Expert（クラウド）コンポーネントへのリクエストの情報：
  - 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
  - サーバーからのリクエストによりデバイス上で起動されたプロセスに関する情報：
    - プロセスの終了コード
    - プロセスの標準出力ファイルの一意の ID。
    - プロセスの標準エラーファイルの一意の ID。

- サーバーからのリクエストによりデバイス上で起動または停止されたプロセスに関する情報：
  - PID（システムプロセス ID）。
  - UniquePID（プロセスの一意の識別子）
  - エラーコード
- サーバーからリクエストされたファイルのコピー、およびそのファイルのパスと ID。
- OS の再起動後にファイルを削除するかどうかを示すフラグ。
- 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返されます：
  - 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
    - 実行ファイルまたは読み込み可能なモジュールの MD5 ハッシュと SHA-256 ハッシュ。
- プロセスメモリのイメージ：
    - プロセスメモリイメージファイルの名前。
    - プロセスファイルへの完全パス
    - プロセスメモリイメージファイルの一意の ID。
    - プロセスメモリイメージファイルのサイズ。
- デバイスメモリのイメージ：
    - ダンプが開始された日時。
    - ダンプファイルへの完全パス
    - デバイスメモリイメージファイルのサイズ。
- デバイスディスクのイメージ：
    - ダンプが開始された日時。
    - ダンプファイルへの完全パスの配列

    - デバイスディスクイメージファイルのサイズ。
    - 論理ディスク。
    - 物理ディスク。
- 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。
    - カスペルスキー 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
- ネットワーク接続の確立と終了に関する情報：
  - 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
  - 接続確立時刻
  - 接続終了時刻
  - 接続時間
  - 接続中に送信されたバイト数
  - 接続中に受信されたバイト数
- 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

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。

Adobe、Acrobat、Flash、Shockwave は、米国およびその他の国における Adobe の商標または登録商標です。

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。

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。

AutoCAD は、アメリカ合衆国およびその他の国における Autodesk, Inc. およびその子会社の商標または登録商標です。

Borland は、Borland Software Corporation の商標または登録商標です。

dBase は dataBased Intelligence, Inc. の商標です。

FireWire は Apple Inc. の商標です。

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、Chromium、Google 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。

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、Microsoft Edge、Active Directory、Hyper-V、Outlook、Visual Basic、Visual FoxPro、Visual C++、PowerPoint、Excel、Internet Explorer、Windows、および Windows Server 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、Java、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 Enterprise Linux、CentOS、および 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。

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。